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

Contents

EXPOSURE DRAFT

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

The Parliament of Australia enacts:

1 Short title

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

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with

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

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	
2. Schedule 1	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 *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*. 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Note: This table relates only to the provisions of this Act as originally enacted.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.

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

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Industry assistance

Administrative Decisions (Judicial Review) Act 1977

1 After paragraph (daaa) of Schedule 1

Insert:

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

Criminal Code Act 1995

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

Insert:

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

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

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

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

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

Insert:

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

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

(vi) in compliance with a technical capability notice;

4 Dictionary in the *Criminal Code*

Insert:

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

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

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

Telecommunications Act 1997

5 Section 7

Insert:

ASIO means the Australian Security Intelligence Organisation.

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

After "this Act" (first occurring), insert "(other than section 317ZB)".

7 After Part 14

Insert:

Part 15—Industry assistance

Division 1—Introduction

317A Simplified outline of this Part

- 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

(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

(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.

317B Definitions

In this Part:

access, when used in relation to material, includes:
(a) access that is subject to a pre-condition (for example, the use of a password); and
(b) access by way of push technology; and
(c) access by way of a standing request.

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

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

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

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.

Corruption and Crime Commission (WA) means the Corruption and Crime Commission established by the *Corruption, Crime and Misconduct Act 2003* (WA).

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

electronic service has the meaning given by section 317D.

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

entrusted ASD person means a person who:

(a) is a staff member of the Australian Signals Directorate; or

(b) has entered into a contract, agreement or arrangement with the Australian Signals Directorate; or

(c) is an employee or agent of a person who has entered into a contract, agreement or arrangement with the Australian Signals Directorate.

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

entrusted ASIS person means a person who:

(a) is a staff member or agent of the Australian Secret Intelligence Service; or

(b) has entered into a contract, agreement or arrangement with the Australian Secret Intelligence Service; or

(c) is an employee or agent of a person who has entered into a contract, agreement or arrangement with the Australian Secret Intelligence Service.

giving help:

(a) when used in relation to ASIO—includes giving help to an ASIO employee or an ASIO affiliate; or

(b) when used in relation to the Australian Secret Intelligence Service—includes giving help to a staff member of the Australian Secret Intelligence Service; or

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

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

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

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

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

interception agency means:

(a) the Australian Federal Police; or

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

(c) the Australian Crime Commission; or

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

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

(f) the New South Wales Crime Commission; or

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

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

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

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

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

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

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

material means material:

(a) whether in the form of text; or

(b) whether in the form of data; or

(c) whether in the form of speech, music or other sounds; or

(d) whether in the form of visual images (moving or otherwise); or

(e) whether in any other form; or

(f) whether in any combination of forms.

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

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

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

supply:

(a) when used in relation to:

(i) a facility; or

(ii) customer equipment; or

(iii) a component;

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

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

technical assistance notice means a notice given under section 317L.

technical assistance notice information means:

(a) information about any of the following:

(i) the giving of a technical assistance notice;

(ii) the existence or non-existence of a technical assistance notice;
(iii) the variation of a technical assistance notice;
(iv) the revocation of a technical assistance notice;
(v) the requirements imposed by a technical assistance notice;
(vi) any act or thing done in compliance with a technical assistance notice; or
(b) any other information about a technical assistance notice.

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

technical assistance request information means:
(a) information about any of the following:
(i) the giving of a technical assistance request;
(ii) the existence or non-existence of a technical assistance request;
(iii) the acts or things covered by a technical assistance request;
(iv) any act or thing done in accordance with a technical assistance request; or
(b) any other information about a technical assistance request.

technical capability notice means a notice given under section 317T.

technical capability notice information means:
(a) information about any of the following:
(i) the giving of a technical capability notice;
(ii) consultation relating to the giving of a technical capability notice;
(iii) the existence or non-existence of a technical capability notice;
(iv) the variation of a technical capability notice;
(v) the revocation of a technical capability notice;
(vi) the requirements imposed by a technical capability notice;

(vii) any act or thing done in compliance with a technical capability notice; or

(b) any other information about a technical capability notice.

317C Designated communications provider etc.

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

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

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

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

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

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

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	

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

317D Electronic service

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

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

(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;

but does not include:

(c) a broadcasting service; or

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

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

(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.

(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.

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

(a) in isolation; or

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

317E Listed acts or things

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

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

(b) providing technical information; or

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

(d) ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format; or

(e) facilitating or assisting access to whichever of the following are the subject of eligible activities of the provider:

(i) a facility;

(ii) customer equipment;

(iii) a data processing device;

(iv) a listed carriage service;

(v) a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service;

(vi) an electronic service;

(vii) a service that facilitates, or is ancillary or incidental to, the provision of an electronic service;

(viii) software used, for use, or likely to be used, in connection with a listed carriage service;

(ix) software used, for use, or likely to be used, in connection with an electronic service;

(x) 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; or

(f) assisting with the testing, modification, development or maintenance of a technology or capability; or

(g) notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation; or

(h) modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider; or

(i) substituting, or facilitating the substitution of, a service provided by the designated communications provider for:

(i) another service provided by the provider; or

(ii) a service provided by another designated communications provider; or

(j) an act or thing done to conceal the fact that any thing has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

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

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

(iii) protecting the public revenue; or

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

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

(a) making a false or misleading statement; or

(b) engaging in dishonest conduct.

317F Extension to external Territories

This Part extends to every external Territory.

Division 2—Voluntary technical assistance

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

(1) If:

(a) any of the following persons:

(i) the Director-General of Security;
(ii) the Director-General of the Australian Secret Intelligence Service;
(iii) the Director-General of the Australian Signals Directorate;
(iv) the chief officer of an interception agency;

requests a designated communications provider to do one or more specified acts or things that:

(v) are in connection with any or all of the eligible activities of the provider; and
(vi) are covered by subsection (2); and

(b) the provider does an act or thing:

(i) in accordance with the request; or
(ii) in good faith purportedly in accordance with the request;

then:

(c) the provider is not subject to any civil liability for, or in relation to, the act or thing mentioned in paragraph (b); and
(d) an officer, employee or agent of the provider is not subject to any civil liability for, or in relation to, an act or thing done by the officer, employee or agent in connection with the act or thing mentioned in paragraph (b).

(2) The specified acts or things must:

(a) be directed towards ensuring that the designated communications provider is capable of giving help to:

(i) in a case where the request is made by the Director-General of Security—ASIO; or
(ii) in a case where the request is made by the Director-General of the Australian Secret Intelligence Service—the Australian Secret Intelligence Service; or
(iii) in a case where the request is made by the Director-General of the Australian Signals Directorate—the Australian Signals Directorate; or
(iv) in a case where the request is made by the chief officer of an interception agency—the agency;

in relation to:

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

(vi) a matter that facilitates, or is ancillary or incidental to, a matter covered by subparagraph (v); or

(b) be by way of giving help to:

(i) in a case where the request is made by the Director-General of Security—ASIO; or

(ii) in a case where the request is made by the Director-General of the Australian Secret Intelligence Service—the Australian Secret Intelligence Service; or

(iii) in a case where the request is made by the Director-General of the Australian Signals Directorate—the Australian Signals Directorate; or

(iv) in a case where the request is made by the chief officer of an interception agency—the agency;

in relation to:

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

(vi) a matter that facilitates, or is ancillary or incidental to, a matter covered by subparagraph (v).

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

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

Relevant objective

(5) For the purposes of this section, ***relevant objective*** means:

(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.

Listed acts or things

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

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

(b) are covered by subsection (2).

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

317H Form of technical assistance request

(1) A technical assistance request may be given:

(a) orally; or

(b) in writing.

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

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

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

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

(3) If a technical assistance request is given orally by:

(a) the Director-General of Security; or

(b) the Director-General of the Australian Secret Intelligence Service; or

(c) the Director-General of the Australian Signals Directorate; or

(d) the chief officer of an interception agency;

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, as the case requires, must:

(e) make a written record of the request; and

(f) do so within 48 hours after the request was given.

(4) If, under subsection (3):

(a) the Director-General of Security; or

(b) the Director-General of the Australian Secret Intelligence Service; or

(c) the Director-General of the Australian Signals Directorate; or

(d) the chief officer of an interception agency;

makes a written record of a technical assistance request, 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, as the case requires, must:

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

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

317HA Duration of technical assistance request

(1) A technical assistance request:

(a) comes in force:

(i) when it is given; or

(ii) if a later time is specified in the request—at that later time; and

(b) unless sooner revoked, remains in force:

(i) if an expiry date is specified in the request—until the start of the expiry date; or

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

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

317J Specified period etc.

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

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

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

317JA Variation of technical assistance requests

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

(2) If a technical assistance request has been given to a designated communications provider by the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Secret Intelligence Service may vary the request.

(3) If a technical assistance request has been given to a designated communications provider by the Director-General of the Australian Signals Directorate, the Director-General of the Australian Signals Directorate may vary the request.

(4) If a technical assistance request has been given to a designated communications provider by the chief officer of an interception agency, the chief officer may vary the request.

Form of variation

(5) A variation may be made:
  (a) orally; or
  (b) in writing.

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

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

(b) the variation is necessary for the purpose of dealing with that risk; and

(c) it is not practicable in the circumstances to make the variation in writing.

(7) If a variation is made orally by:

(a) the Director-General of Security; or

(b) the Director-General of the Australian Secret Intelligence Service; or

(c) the Director-General of the Australian Signals Directorate; or

(d) the chief officer of an interception agency;

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, as the case requires, must:

(e) make a written record of the variation; and

(f) do so within 48 hours after the variation was made.

(8) If, under subsection (7):

(a) the Director-General of Security; or

(b) the Director-General of the Australian Secret Intelligence Service; or

(c) the Director-General of the Australian Signals Directorate; or

(d) the chief officer of an interception agency;

makes a written record of a variation, 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, as the case requires, must:

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

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

Acts or things specified in a varied technical assistance request

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

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

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

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

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

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

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

317JB Revocation of technical assistance requests

(1) If a technical assistance request has been given to a person by the Director-General of Security, the Director-General of Security may, by written notice given to the person, revoke the request.

(2) If a technical assistance request has been given to a person by the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Secret Intelligence Service may, by written notice given to the person, revoke the request.

(3) If a technical assistance request has been given to a person by the Director-General of the Australian Signals Directorate, the Director-General of the Australian Signals Directorate may, by written notice given to the person, revoke the request.

(4) If a technical assistance request has been given to a person by the chief officer of an interception agency, the chief officer may, by written notice given to the person, revoke the request.

317K Contract etc.

Any of the following persons:

(a) the Director-General of Security;

(b) the Director-General of the Australian Secret Intelligence Service;

(c) the Director-General of the Australian Signals Directorate;

(d) the chief officer of an interception agency;

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

Division 3—Technical assistance notices

317L Technical assistance notices

(1) 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 one or more specified acts or things that:

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

(b) are covered by subsection (2).

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

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

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

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

in relation to:

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

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

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

(iii) protecting the public revenue; or

(iv) safeguarding national security; or

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

Listed acts or things

(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:

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

(b) are covered by subsection (2).

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

317M Form of technical assistance notice

(1) A technical assistance notice may be given:

(a) orally; or

(b) in writing.

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

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

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

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

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

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

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

(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:

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

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

317MA Duration of technical assistance notice

(1) A technical assistance notice:
  (a) comes in force:
    (i) when it is given; or
    (ii) if a later time is specified in the notice—at that later time; and
  (b) unless sooner revoked, remains in force:
    (i) if an expiry date is specified in the notice—until the start of the expiry date; or
    (ii) otherwise—at end of the 90-day period beginning when the notice was given.

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

317N Compliance period etc.

(1) A technical assistance notice may require a specified act or thing to be done within a specified period.

(2) A technical assistance notice may require a specified act or thing to be done:
  (a) in a specified manner; or
  (b) in a way that meets one or more specified conditions.

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

317P Decision-making criteria

The Director-General of Security or the chief officer of an interception agency must not give a technical assistance notice to a designated communications provider unless the Director-General of Security or the chief officer, as the case requires, is satisfied that:
  (a) the requirements imposed by the notice are reasonable and proportionate; and

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

317Q Variation of technical assistance notices

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

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

Form of variation

(3) A variation may be made:
(a) orally; or
(b) in writing.

(4) A variation must not be made orally unless:
(a) an imminent risk of serious harm to a person or substantial damage to property exists; and
(b) the variation is necessary for the purpose of dealing with that risk; and
(c) it is not practicable in the circumstances to make the variation in writing.

(5) If a variation is made orally by the 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:
(a) make a written record of the variation; and
(b) do so within 48 hours after the variation was made.

(6) If, under subsection (5), the Director-General of Security or the chief officer of an interception agency makes a written record of a variation, the Director-General of Security or the chief officer, as the case requires, must:

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

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

(7) If a variation is made in writing by the 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:

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

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

Acts or things specified in a varied technical assistance notice

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

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

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

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

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

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

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

Decision-making criteria

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

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

(b) compliance with the varied notice is:

(i) practicable; and

(ii) technically feasible.

317R Revocation of technical assistance notices

(1) If a technical assistance notice has been given to a person by the Director-General of Security, the Director-General of Security may, by written notice given to the person, revoke the notice.

(2) If a technical assistance notice has been given to a person by the Director-General of Security, and the Director-General of Security is satisfied that:

(a) the requirements imposed by the notice are not reasonable and proportionate; or

(b) compliance with the notice is not:

(i) practicable; and

(ii) technically feasible;

the Director-General of Security must, by written notice given to the person, revoke the notice.

(3) If a technical assistance notice has been given to a person by the chief officer of an interception agency, the chief officer may, by written notice given to the person, revoke the notice.

(4) If a technical assistance notice has been given to a person by the chief officer of an interception agency, and the chief officer is satisfied that:

(a) the requirements imposed by the notice are not reasonable and proportionate; or

(b) compliance with the notice is not:

(i) practicable; and

(ii) technically feasible;

the chief officer must, by written notice given to the person, revoke the notice.

Division 4—Technical capability notices

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

(1) The Attorney-General may, by writing, determine procedures and arrangements to be followed in relation to the making of requests for technical capability notices.

(2) A procedure or arrangement determined under subsection (1) may require that the agreement of a person or body must be obtained before a request is made for a technical capability notice.

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

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

317T Technical capability notices

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

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

(b) are covered by subsection (2).

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

(2) The specified acts or things must:

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

(i) the performance of a function, or the exercise of a power, conferred by or under a law of the

Commonwealth, a State or a Territory, so far as the function or power relates to a relevant objective; or

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

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

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

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

Relevant objective

(3) For the purposes of this section, ***relevant objective*** means:

(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.

Listed help

(4) For the purposes of the application of this section to a designated communications provider, if one or more acts or things done by the provider:

(a) are by way of giving help to ASIO or an interception agency; and

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

(c) consist of either or both of the following:

(i) one or more listed acts or things (other than an act or thing covered by paragraph 317E(1)(a));

(ii) one or more acts or things of a kind determined under subsection (5);

that help is ***listed help***.

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

(5) The Minister may, by legislative instrument, determine one or more kinds of acts or things for the purposes of subparagraph (4)(c)(ii).

(6) In making a determination under subsection (5), the Minister must have regard to the following matters:

(a) the interests of law enforcement;

(b) the interests of national security;

(c) the objects of this Act;

(d) the likely impact of the determination on designated communications providers;

(e) such other matters (if any) as the Minister considers relevant.

Listed acts or things

(7) The acts or things that may be specified in a technical capability notice given to a designated communications provider in accordance with paragraph (2)(b) include (but are not limited to) listed acts or things, so long as those acts or things:

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

(b) are covered by subsection (2), so far as that subsection relates to paragraph (2)(b).

Limits

(8) If:

(a) a designated communications provider supplies a particular kind of telecommunications service; and

(b) the service involves, or will involve, the use of a telecommunications system;

a technical capability notice has no effect to the extent (if any) to which it requires the provider to ensure that the kind of service, or the system:

(c) has the capability to enable a communication passing over the system to be intercepted in accordance with an interception warrant; or

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

(e) has a delivery capability.

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

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

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

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

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

(b) documents containing information of that kind;

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

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

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

Applicable costs negotiator

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

Note: See section 317ZK.

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

(a) by name; or

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

317TA Duration of technical capability notice

(1) A technical capability notice:

(a) comes in force:

(i) when it is given; or

(ii) if a later time is specified in the notice—at that later time; and

(b) unless sooner revoked, remains in force:

(i) if an expiry date is specified in the notice—until the start of the expiry date; or

(ii) otherwise—at end of the 180-day period beginning when the notice was given.

(2) If a technical capability notice expires, this Part does not prevent the giving of a fresh technical capability notice in the same terms as the expired technical capability notice.

317U Compliance period etc.

(1) A technical capability notice may require a specified act or thing to be done within a specified period.

(2) A technical capability notice may require a specified act or thing to be done:

(a) in a specified manner; or

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

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

317V Decision-making criteria

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

(a) the Attorney-General is satisfied that the requirements imposed by the notice are reasonable and proportionate; and

(b) the Attorney-General is satisfied that compliance with the notice is:

(i) practicable; and

(ii) technically feasible.

317W Consultation about a proposal to give a technical capability notice

(1) The Attorney-General must not give a technical capability notice to a person unless the Attorney-General has first:

(a) given the person a written notice:

(i) setting out a proposal to give the notice; and

(ii) inviting the person to make a submission to the Attorney-General on the proposed notice; and

(b) considered any submission that was received within the time limit specified in the notice.

(2) A time limit specified in a notice under subsection (1) must run for at least 28 days.

(3) The rule in subsection (2) does not apply to a technical capability notice given to a person if:

(a) the Attorney-General is satisfied that the notice should be given as a matter of urgency; or

(b) compliance with subsection (2) is impracticable; or

(c) the person waives compliance with subsection (2).

(4) For the purposes of paragraph (3)(c), a person may waive compliance:

(a) orally; or

(b) in writing.

(5) If compliance is waived orally by a person, the person must:

(a) make a written record of the waiver; and

(b) do so within 48 hours after the waiver was made.

(6) If, under subsection (5), a person makes a written record of the waiver, that person must:

(a) give a copy of the record to the Attorney-General; and

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

317X Variation of technical capability notices

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

Acts or things specified in a varied technical capability notice

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

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

(b) covered by subsection 317T(2).

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

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

(b) are covered by subsection 317T(2), so far as that subsection relates to paragraph 317T(2)(b).

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

Decision-making criteria

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

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

(b) compliance with the varied notice is:

(i) practicable; and

(ii) technically feasible.

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

(1) If a technical capability notice has been given to a person, the Attorney-General must not vary the notice unless the Attorney-General has first:
  (a) given the person a written notice:
    (i) setting out a proposal to vary the notice; and
    (ii) inviting the person to make a submission to the Attorney-General on the proposed variation; and
  (b) considered any submission that was received within the time limit specified in the notice.

(2) A time limit specified in a notice under subsection (1) must run for at least 28 days.

(3) If a technical capability notice has been given to a person, the rule in subsection (2) does not apply to a variation of the notice if:
  (a) the Attorney-General is satisfied that the notice should be varied as a matter of urgency; or
  (b) compliance with subsection (2) is impracticable; or
  (c) the person waives compliance with subsection (2).

(4) For the purposes of paragraph (3)(c), a person may waive compliance:
  (a) orally; or
  (b) in writing.

(5) If compliance is waived orally by a person, the person must:
  (a) make a written record of the waiver; and
  (b) do so within 48 hours after the waiver was made.

(6) If, under subsection (5), a person makes a written record of the waiver, that person must:
  (a) give a copy of the record to the Attorney-General; and
  (b) do so as soon as practicable after the record was made.

317Z Revocation of technical capability notices

(1) If a technical capability notice has been given to a person, the Attorney-General may, by written notice given to the person, revoke the notice.

(2) If a technical capability notice has been given to a person, and the Attorney-General is satisfied that:

(a) the requirements imposed by the notice are not reasonable and proportionate; or

(b) compliance with the notice is not:

(i) practicable; and

(ii) technically feasible;

the Attorney-General must, by written notice given to the person, revoke the notice.

Division 5—Compliance and enforcement

317ZA Compliance with notices—carriers and carriage service providers

(1) A carrier or carriage service provider must comply with a requirement under:

(a) a technical assistance notice; or

(b) a technical capability notice;

to the extent that the carrier or provider is capable of doing so.

(2) A person must not:

(a) aid, abet, counsel or procure a contravention of subsection (1); or

(b) induce, whether by threats or promises or otherwise, a contravention of subsection (1); or

(c) be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of subsection (1); or

(d) conspire with others to effect a contravention of subsection (1).

(3) Subsections (1) and (2) are civil penalty provisions.

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

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

(1) A designated communications provider (other than a carrier or carriage service provider) must comply with a requirement under:

(a) a technical assistance notice; or

(b) a technical capability notice;

to the extent that the provider is capable of doing so.

Civil penalty:

(a) if the provider is a body corporate—47,619 penalty units; or

(b) if the provider is not a body corporate—238 penalty units.

(2) The pecuniary penalty for a contravention by a designated communications provider of subsection (1) must not be more than:

(a) if the provider is a body corporate—47,619 penalty units; or

(b) if the provider is not a body corporate—238 penalty units.

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

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

317ZC Civil penalty provision

Enforceable civil penalty provision

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

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

Authorised applicant

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

Relevant courts

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

Extension to external Territories etc.

(4) Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*, as it applies in relation to section 317ZB of this Act, extends to:

(a) every external Territory; and

(b) acts, omissions, matters and things outside Australia.

317ZD Enforceable undertakings

Enforceable provision

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

Authorised person

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

Relevant courts

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

Extension to external Territories etc.

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

317ZE Injunctions

Enforceable provision

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

Authorised person

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

Relevant courts

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

Extension to external Territories etc.

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

Division 6—Unauthorised disclosure of information

317ZF Unauthorised disclosure of information

(1) A person commits an offence if:
(a) the person discloses information; and

(b) the person is or was:
(i) a designated communications provider; or
(ii) an employee of a designated communications provider; or
(iii) a contracted service provider of a designated communications provider; or
(iv) an employee of a contracted service provider of a designated communications provider; or
(v) an entrusted ASIO person; or
(vi) an entrusted ASIS person; or
(vii) an entrusted ASD person; or
(viii) an officer of an interception agency; or
(ix) an officer or employee of the Commonwealth, a State or a Territory; or
(x) an arbitrator appointed under section 317ZK; and

(c) the information:
(i) is technical assistance notice information; or
(ii) is technical capability notice information; or
(iii) is technical assistance request information; or
(iv) was obtained in accordance with a technical assistance notice; or
(v) was obtained in accordance with a technical capability notice; or
(vi) was obtained in accordance with a technical assistance request; and

(d) if the information is covered by subparagraph (c)(i), (ii) or (iii)—the information has come to the person's knowledge, or into the person's possession:
(i) if the person is or was a designated communications provider—in connection with the person's capacity as such a provider; or
(ii) if the person is or was an employee of a designated communications provider—because the person is or was employed by the provider in connection with its business as such a provider; or

(iii) if the person is or was a contracted service provider of a designated communications provider—in connection with the person's business as such a contracted service provider; or

(iv) if the person is or was an employee of a contracted service provider of a designated communications provider—because the person is or was employed by the contractor in connection with its business as such a contracted service provider; or

(v) if the person is or was an entrusted ASIO person—in the person's capacity as such an entrusted ASIO person; or

(vi) if the person is or was an entrusted ASIS person—in the person's capacity as such an entrusted ASIS person; or

(vii) if the person is or was an entrusted ASD person—in the person's capacity as such an entrusted ASD person; or

(viii) if the person is or was an officer of an interception agency—in the person's capacity as such an officer; or

(ix) if the person is or was an officer or employee of the Commonwealth, a State or a Territory—in the person's capacity as such an officer or employee; or

(x) if the person is or was an arbitrator appointed under section 317ZK—in the person's capacity as such an arbitrator; and

(e) if the information is covered by subparagraph (c)(iv), (v) or (vi)—the information has come to the person's knowledge, or into the person's possession:

(i) if the person is or was an entrusted ASIO person—in the person's capacity as such an entrusted ASIO person; or

(ii) if the person is or was an entrusted ASIS person—in the person's capacity as such an entrusted ASIS person; or

(iii) if the person is or was an entrusted ASD person—in the person's capacity as such an entrusted ASD person; or

(iv) if the person is or was an officer of an interception agency—in the person's capacity as such an officer; or

(v) if the person is or was an officer or employee of the Commonwealth, a State or a Territory—in the person's capacity as such an officer or employee; or

(vi) if the person is or was an arbitrator appointed under section 317ZK—in the person's capacity as such an arbitrator.

Penalty: Imprisonment for 5 years.

Exceptions

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

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

Authorised disclosures—general

(3) A person covered by paragraph (1)(b) may disclose technical assistance notice information, technical capability notice information or technical assistance request information:

(a) in connection with the administration or execution of this Part; or

(b) for the purposes of any legal proceedings arising out of or otherwise related to this Part or of any report of any such proceedings; or

(c) in accordance with any requirement imposed by law; or

(d) in connection with the performance of functions, or the exercise of powers, by:

(i) ASIO; or

(ii) the Australian Secret Intelligence Service; or

(iii) the Australian Signals Directorate; or

(iv) an interception agency; or

(e) for the purpose of obtaining legal advice in relation to this Part; or

(f) to an IGIS official for the purpose of exercising powers, or performing functions or duties, as an IGIS official.

(4) For the purposes of subsection (3), ***this Part*** includes:

(a) any other provision of this Act, so far as that other provision relates to this Part; and

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

Authorised disclosures—IGIS official

(5) An IGIS official may disclose:

(a) technical assistance notice information; or

(b) technical capability notice information; or

(c) technical assistance request information;

in connection with the IGIS official exercising powers, or performing functions or duties, as an IGIS official.

Authorised disclosures—information sharing

(6) The Director-General of Security or the Communications Access Co-ordinator may disclose information that is:

(a) technical assistance notice information; or

(b) technical capability notice information; or

(c) technical assistance request information;

to the chief officer of an interception agency for purposes relating to the performance of functions, or the exercise of powers, by the interception agency.

(7) The chief officer of an interception agency may disclose information that is:

(a) technical assistance notice information; or

(b) technical capability notice information; or

(c) technical assistance request information;

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

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

(a) technical assistance notice information; or

(b) technical capability notice information; or

(c) technical assistance request information;

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

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

(a) technical assistance notice information; or

(b) technical capability notice information; or

(c) technical assistance request information;

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

(10) The Communications Access Co-ordinator, 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 disclose information that is:

(a) technical assistance notice information; or

(b) technical capability notice information; or

(c) technical assistance request information;

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

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

(a) technical assistance notice information; or

(b) technical capability notice information; or

(c) technical assistance request information;

to the Communications Access Co-ordinator for purposes relating to the performance of functions, or the exercise of powers, by the Communications Access Co-ordinator.

(12) Before disclosing information under subsection (6), (7), (8), (9) or (10), 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, as the case requires, must notify the Communications Access Co-ordinator of the proposed disclosure.

Authorised disclosures—statistics

(13) A person who is:

(a) a designated communications provider; or

(b) an employee of a designated communications provider; or

(c) a contracted service provider of a designated communications provider; or

(d) an employee of a contracted service provider of a designated communications provider;

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

(e) the total number of technical assistance notices given to the provider during a period of at least 6 months; or

(f) the total number of technical capability notices given to the provider during a period of at least 6 months; or

(g) the total number of technical assistance requests given to the provider during a period of at least 6 months.

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

(a) by agency; or

(b) in any other way.

Division 7—Limitations

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

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

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

(b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.

(2) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection includes a reference to implement or build a new decryption capability in relation to a form of electronic protection.

(3) The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection includes a reference to one or more actions that would render systemic methods of authentication or encryption less effective.

(4) Subsections (2) and (3) are enacted for the avoidance of doubt.

(5) A technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).

317ZH General limits on technical assistance notices and technical capability notices

(1) A technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would require a designated communications provider to do an act or thing for which a warrant or authorisation under any of the following laws is required:

(a) the *Telecommunications (Interception and Access) Act 1979*;

(b) the *Surveillance Devices Act 2004*;

(c) the *Crimes Act 1914*;

(d) the *Australian Security Intelligence Organisation Act 1979*;

(e) the *Intelligence Services Act 2001*.

(2) For the purposes of subsection (1):

(a) assume that each law mentioned in that subsection applied both within and outside Australia; and

(b) assume that each reference in Part 13 to a carriage service provider included a reference to a designated communications provider.

(3) A technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would require a designated communications provider to:

(a) use a surveillance device (within the meaning of the *Surveillance Devices Act 2004*); or

(b) access data held in a computer (within the meaning of the *Surveillance Devices Act 2004*);

if a law of a State or Territory requires a warrant or authorisation for that use or access.

(4) To avoid doubt, subsection (1) or (3) does not prevent a technical assistance notice or technical capability notice from requiring a designated communications provider to do an act or thing by way of giving help to:

(a) ASIO; or

(b) an interception agency;

in relation to:

(c) in the case of a technical assistance notice—a matter covered by paragraph 317L(2)(c) or (d); or

(d) in the case of a technical capability notice—a matter covered by subparagraph 317T(2)(b)(i) or (ii);

if the doing of the act or thing would:

(e) assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(f) give effect to a warrant or authorisation under a law of the Commonwealth.

(5) To avoid doubt, subsection (1) or (3) does not prevent a technical capability notice from requiring a designated communications provider to do an act or thing directed towards ensuring that the provider is capable of giving listed help (within the meaning of section 317T) to:

(a) ASIO; or

(b) an interception agency;

in relation to a matter covered by subparagraph 317T(2)(a)(i) or (ii), if the doing of the act or thing would:

(c) assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(d) give effect to a warrant or authorisation under a law of the Commonwealth.

Division 8—General provisions

317ZJ Immunity

(1) A designated communications provider is not subject to any civil liability for, or in relation to, an act or thing done by the provider:

(a) in compliance; or

(b) in good faith in purported compliance;

with:

(c) a technical assistance notice; or

(d) a technical capability notice.

(2) Paragraph (1)(b) does not apply to an act or thing done by a designated communications provider unless the act or thing is in connection with any or all of the eligible activities of the provider.

(3) An officer, employee or agent of a designated communications provider is not subject to any civil liability for, or in relation to, an act or thing done by the officer, employee or agent in connection with an act or thing done by the provider:

(a) in compliance; or

(b) in good faith in purported compliance;

with:

(c) a technical assistance notice; or

(d) a technical capability notice.

(4) Paragraph (3)(b) does not apply to an act or thing done by a designated communications provider unless the act or thing is in connection with any or all of the eligible activities of the provider.

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

Scope

(1) This section applies if a designated communications provider is subject to a requirement under:

(a) a technical assistance notice; or

(b) a technical capability notice;

unless:

(c) in the case of a requirement under a technical assistance notice given by the Director-General of Security—the Director-General of Security is satisfied that it would be contrary to the public interest for this section to apply to the requirement; or

(d) in the case of a requirement under a technical assistance notice given by the chief officer of an interception agency—the chief officer is satisfied that it would be contrary to the public interest for this section to apply to the requirement; or

(e) in the case of a requirement under a technical capability notice—the Attorney-General is satisfied that it would be contrary to the public interest for this section to apply to the requirement.

(2) In deciding whether it would be contrary to the public interest for this section to apply to a requirement, the Director-General of Security, the chief officer or the Attorney-General, as the case may be, must have regard to the following matters:

(a) the interests of law enforcement;

(b) the interests of national security;

(c) the objects of this Act;

(d) the extent to which compliance with the requirement will impose a regulatory burden on the provider;

(e) the reasons for the giving of the technical assistance notice or technical capability notice, as the case requires;

(f) such other matters (if any) as the Director-General of Security, the chief officer or the Attorney-General, as the case may be, considers relevant.

Basis of compliance

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

(a) profits from complying with the requirement; nor

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

unless the provider and the applicable costs negotiator otherwise agree.

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

Terms and conditions

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

(a) agreed between the following parties:

(i) the provider;

(ii) the applicable costs negotiator; or

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

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

(5) If:

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

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

the ACMA is to appoint the arbitrator.

(6) If:

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

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

the Attorney-General is to appoint the arbitrator.

Arbitration

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

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

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

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

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

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

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

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

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

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

Acquisition of property

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

Applicable costs negotiator

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

(a) in the case of a requirement under a technical assistance notice given by the Director-General of Security—the Director-General of Security; or

(b) in the case of a requirement under a technical assistance notice given by the chief officer of an interception agency—the chief officer; or

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

317ZL Service of notices etc.

Scope

(1) This section applies to:

(a) a summons or process in any proceedings under, or connected with, this Part; or

(b) a summons or process in any proceedings under, or connected with, the *Regulatory Powers (Standard Provisions) Act 2014*, so far as that Act relates to this Part; or

(c) a technical assistance notice or any other notice under this Part; or

(d) a notice under the *Regulatory Powers (Standard Provisions) Act 2014*, so far as that Act relates to this Part; or

(e) a technical capability notice.

Address for service of summons, process or notice

(2) If:

(a) the summons, process or notice, as the case may be, is required to be served on, or given to, a designated communications provider; and

(b) the designated communications provider has nominated an address for service in a document given by the provider to:

(i) the Attorney-General; or

(ii) the Communications Access Co-ordinator; or

(iii) the Director-General of Security; or

(iv) the chief officer of an interception agency;

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

(3) If:

(a) the summons, process or notice, as the case may be, is required to be served on, or given to, a designated communications provider; and

(b) the designated communications provider has nominated an electronic address for service in a document given by the provider to:

(i) the Attorney-General; or

(ii) the Communications Access Co-ordinator; or

(iii) the Director-General of Security; or

(iv) the chief officer of an interception agency;

the summons, process or notice, as the case may be, is taken to have been served on, or given to, the provider if it is sent to the nominated electronic address for service.

Service of summons, process or notice on agent etc.

(4) If:

(a) the summons, process or notice, as the case may be, is required to be served on, or given to, a body corporate incorporated outside Australia; and

(b) the body corporate does not have a registered office or a principal office in Australia; and

(c) the body corporate has an agent in Australia;

the summons, process or notice, as the case may be, is taken to have been served on, or given to, the body corporate if it is served on, or given to, the agent.

(5) If:

(a) the summons, process or notice, as the case may be, is required to be served on, or given to, a body corporate incorporated outside Australia; and

(b) the body corporate does not have a registered office or a principal office in Australia; and

(c) the body corporate carries on business, or conducts activities, at an address in Australia;

the summons, process or notice, as the case may be, is taken to have been served on, or given to, the body corporate if it is left at, or sent by pre-paid post to, that address.

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 *Australian Federal Police Act 1979*)	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 *Law Enforcement Integrity Commissioner Act 2006*)	(a) the Integrity Commissioner (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*); or (b) a staff member of ACLEI (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*)
3	Australian Crime Commission	Chief Executive Officer of the Australian Crime	(a) the Chief Executive Officer of the Australian Crime

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 *Australian Crime Commission Act 2002*); or (c) a member of the staff of the ACC (within the meaning of the *Australian Crime Commission Act 2002*)
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 *Independent Commission Against Corruption Act 1988* (NSW))	an officer of the Commission (within the meaning of the *Independent Commission Against Corruption Act 1988* (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 *Crime Commission Act 2012* (NSW))	an officer of the Commission (within the meaning of the *Crime Commission Act 2012* (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

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 *Law Enforcement Conduct Commission Act 2016* (NSW))	of the *Law Enforcement Conduct Commission Act 2016* (NSW)); or (b) the Commissioner for Integrity (within the meaning of the *Law Enforcement Conduct Commission Act 2016* (NSW)); or (c) a member of the staff of the Commission (within the meaning of the *Law Enforcement Conduct Commission Act 2016* (NSW))
8	Independent Broad-based Anti-corruption Commission of Victoria	the Commissioner (within the meaning of the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic.))	a sworn IBAC Officer (within the meaning of the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic.))
9	Crime and Corruption Commission of Queensland	the chairperson (within the meaning of the *Crime and Corruption Act 2001* (Qld))	a commission officer (as defined by paragraph (a) of the definition of ***commission officer*** in the Dictionary to the *Crime and Corruption Act 2001* (Qld)) other than a person engaged

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 *Independent Commissioner Against Corruption Act 2012* (SA))	(a) the Commissioner (within the meaning of the *Independent Commissioner Against Corruption Act 2012* (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 *Corruption, Crime and Misconduct Act 2003* (WA))	an officer of the Commission (within the meaning of the *Corruption, Crime and Misconduct Act 2003* (WA)) other than a person engaged under section 182 of that Act

317ZN Delegation by Director-General of Security

(1) The Director-General of Security may, by writing, delegate any or all of the functions or powers of the Director-General of Security under Division 2, 3 or 6 to a senior position-holder (within the meaning of the *Australian Security Intelligence Organisation Act 1979*).

(2) A delegate must comply with any written directions of the Director-General of Security.

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

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

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

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

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

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

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

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

(b) who:

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

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

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

317ZR Delegation by the chief officer of an interception agency

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

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

Potential delegates

Item	Column 1 Interception agency	Column 2 Potential delegates
1	Australian Federal Police	(a) a Deputy Commissioner (within the meaning of the *Australian Federal Police Act 1979*); or (b) a senior executive AFP employee (within the meaning of the *Australian Federal Police Act 1979*)
2	Australian Commission for Law Enforcement Integrity	(a) an Assistant Integrity Commissioner (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*); or (b) a staff member of ACLEI (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*) 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 *Australian Crime Commission Act 2002*) 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 *Independent Commission Against Corruption Act 1988* (NSW)); or (b) an Assistant Commissioner (within the meaning of the *Independent Commission Against Corruption Act 1988* (NSW)); or (c) an officer of the Commission (within the meaning of the *Independent Commission Against Corruption Act 1988* (NSW)) (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 *Crime Commission Act 2012* (NSW)) (other than a person engaged under subsection 74(2) of that Act) who is at executive level

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 *Law Enforcement Conduct Commission Act 2016* (NSW)); or (b) a member of the staff of the Commission (within the meaning of the *Law Enforcement Conduct Commission Act 2016* (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 *Independent Broad-based Anti-corruption Commission Act 2011* (Vic.)) who is at executive level
9	Crime and Corruption Commission of Queensland	a senior executive officer (within the meaning of the *Crime and Corruption Act 2001* (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

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

Executive level

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

(4) For the purposes of this section, a person is at ***executive level***, in relation to an interception agency of Victoria, if the person

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

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

317ZS Annual reports

(1) The Minister must, as soon as practicable after each 30 June, cause to be prepared a written report that sets out:

(a) the number of technical assistance notices that were given during the year ending on that 30 June by the chief officers of interception agencies; and

(b) the number of technical capability notices that were:

(i) given during the year ending on that 30 June; and

(ii) directed towards ensuring that designated communications providers are capable of giving help to interception agencies.

(2) A report under subsection (1) must be included in the report prepared under subsection 186(2) of the *Telecommunications (Interception and Access) Act 1979* relating to the year ending on that 30 June.

317ZT Alternative constitutional basis

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

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

Schedule 2—Computer access warrants etc.

Part 1—Amendments

Australian Security Intelligence Organisation Act 1979

1 Section 4

Insert:

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

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

After "subsection", insert "25A(8),".

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

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

4 Paragraph 25A(4)(ab)

Repeal the paragraph, substitute:

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

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

5 After paragraph 25A(4)(ab)

Insert:

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

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

6 After paragraph 25A(4)(b)

Insert:

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

7 At the end of section 25A

Add:

Concealment of access etc.

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

(a) the warrant; or

(b) this subsection;

the Organisation is authorised to do any of the following:

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

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

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

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

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

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

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

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

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

at the following time:

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

(k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).

8 After subsection 27A(3B)

Insert:

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

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

(b) this subsection;

the Organisation is authorised to do any of the following:

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

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

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

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

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

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

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

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

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

at the following time:

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

(k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).

9 Paragraph 27E(2)(d)

Repeal the paragraph, substitute:

(d) 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) use any other computer or a communication in transit for the purpose referred to in paragraph (c); and

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

10 After paragraph 27E(2)(d)

Insert:

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

11 After paragraph 27E(2)(e)

Insert:

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

12 At the end of section 27E

Add:

Concealment of access etc.

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

(a) a subsection (2) authorisation; or

(b) under this subsection;

the Organisation is authorised to do any of the following:

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

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

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

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

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

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

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

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

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

at the following time:

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

(k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).

13 Subsection 33(1)

Repeal the subsection.

14 Paragraph 34(2)(b)

After "25A(4)", insert "or (8) or 27A(3C)".

15 Paragraph 34(2)(b)

After "27E(2)", insert "or (6)".

16 At the end of section 34

Add:

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

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

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

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

Before "26B(5)", insert "25A(8),".

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

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

Mutual Assistance in Criminal Matters Act 1987

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

After "44(1)(a),", insert "(aa),".

26 After Part IIIBA

Insert:

Part IIIBB—Assistance in relation to data held in computers

15CB Simplified outline of this Part

- 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.

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

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

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

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

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

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

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

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

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

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

(a) a particular computer;

(b) a computer on particular premises;

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

(3) In this section:

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

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

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

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

Surveillance Devices Act 2004

27 Title

After "**devices**", insert "**and access to data held in computers**".

28 After paragraph 3(a)

Insert:

(aaa) to establish procedures for law enforcement officers to obtain warrants and emergency authorisations that:

(i) are for access to data held in computers; and

(ii) relate to criminal investigations and the location and safe recovery of children to whom recovery orders relate; and

29 After paragraph 3(aa)

Insert:

(aaaa) to establish procedures for law enforcement officers to obtain warrants for access to data held in computers in cases where a control order is in force, and access to the data 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

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

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

30 After paragraph 3(b)

Insert:

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

31 Paragraph 3(c)

After "surveillance device operations", insert "and computer data access operations".

32 Subsection 4(1)

Omit all the words after "Territory,", substitute:

that:

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

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

33 After subsection 4(4)

Insert:

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

(a) for access to data held in a computer; and

(b) in relation to a relevant offence or a recovery order.

34 After subsection 4(5)

Insert:

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

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

(b) preventing the provision of support for, or the facilitation of, a terrorist act; or

(c) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(d) determining whether the control order, or any succeeding control order, has been, or is being, complied with.

35 Subsection 6(1)

Insert:

carrier means:

(a) a carrier within the meaning of the *Telecommunications Act 1997*; or

(b) a carriage service provider within the meaning of that Act.

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

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

Repeal the definition, substitute:

computer means all or part of:

(a) one or more computers; or

(b) one or more computer systems; or

(c) one or more computer networks; or

(d) any combination of the above.

37 Subsection 6(1)

Insert:

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

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

data includes:

(a) information in any form; and

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

data held in a computer includes:

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

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

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

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

Omit "a computer", substitute "an electronic device for storing or processing information".

39 Subsection 6(1)

Insert:

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

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

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

Repeal the definition, substitute:

mutual assistance application means:

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

(b) an application for a computer access warrant;

made under a mutual assistance authorisation.

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

Omit "subsection 15CA(1)", substitute, "subsection 15CA(1) or 15CC(1)".

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

After "warrant,", insert "a computer access warrant,".

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

Omit "or 23", substitute, ", 23 or 27B".

44 Subsection 6(1)

Insert:

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

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

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

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

Repeal the definition, substitute:

> ***warrant*** means:
> (a) a surveillance device warrant; or
> (b) a retrieval warrant; or
> (c) a computer access warrant.

47 At the end of subsection 10(1)

Add:

; (c) a computer access warrant.

48 Subsection 10(2)

Before "warrant", insert "surveillance device warrant or a retrieval".

49 At the end of Part 2

Add:

Division 4—Computer access warrants

27A Application for computer access warrant

Warrants sought for offence investigations

(1) 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 suspects on reasonable grounds that:

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

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

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

(i) the commission of those offences; or

(ii) the identity or location of the offenders.

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

Warrants sought for recovery orders

(3) 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:

(a) a recovery order is in force; and

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

Warrants sought for mutual assistance investigations

(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:

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

(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:

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

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

Warrants sought for integrity operations

(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:

(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

(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.

Control order access warrants

(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:

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

(b) the law enforcement officer suspects on reasonable grounds that access to data held in a computer (the ***target computer***) to obtain information relating to the person 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

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with.

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

Procedure for making applications

(7) An application under subsection (1), (3), (4), (5) or (6) may be made to an eligible Judge or to a nominated AAT member.

(8) An application:

(a) must specify:

(i) the name of the applicant; and

(ii) the nature and duration of the warrant sought; and

(b) subject to this section, must be supported by an affidavit setting out the grounds on which the warrant is sought.

Unsworn applications—warrants sought for offence investigations

(9) If a law enforcement officer believes that:

(a) immediate access to data held in the target computer referred to in subsection (1) is necessary as described in paragraph (1)(c); and

(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made;

an application for a warrant under subsection (1) may be made before an affidavit is prepared or sworn.

(10) If subsection (9) applies, the applicant must:

(a) provide as much information as the eligible Judge or nominated AAT member considers is reasonably practicable in the circumstances; and

(b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or nominated AAT member, whether or not a warrant has been issued.

Unsworn applications—warrants sought for recovery orders

(11) If a law enforcement officer believes that:

(a) immediate access to data held in the target computer referred to in subsection (3) may assist as described in paragraph (3)(b); and

(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made;

an application for a warrant under subsection (3) may be made before an affidavit is prepared or sworn.

(12) If subsection (11) applies, the applicant must:

(a) provide as much information as the eligible Judge or nominated AAT member considers is reasonably practicable in the circumstances; and

(b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or nominated AAT member, whether or not a warrant has been issued.

Unsworn applications—control order access warrants

(13) If a law enforcement officer believes that:

(a) immediate access to data held in the target computer referred to in subsection (6) would be likely to substantially assist as described in paragraph (6)(b); and

(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made;

an application for a warrant under subsection (6) may be made before an affidavit is prepared or sworn.

(14) If subsection (13) applies, the applicant must:

(a) provide as much information as the eligible Judge or nominated AAT member considers is reasonably practicable in the circumstances; and

(b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or nominated AAT member, whether or not a warrant has been issued.

Target computer

(15) The target computer referred to in subsection (1), (3), (4), (5) or (6) may be any one or more of the following:

(a) a particular computer;

(b) a computer on particular premises;

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

27B Remote application

(1) If a law enforcement officer believes that it is impracticable for an application for a computer access warrant to be made in person, the application may be made under section 27A by telephone, fax, email or any other means of communication.

(2) If transmission by fax is available and an affidavit has been prepared, the person applying must transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or to the nominated AAT member who is to determine the application.

27C Determining the application

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

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

(b) in the case of a warrant sought in relation to a recovery order—that such an order is in force and that there are

reasonable grounds for the suspicion founding the application for the warrant; and

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

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

(e) in the case of a control order access warrant—that a control order is in force in relation to a person, and that access to data held in the relevant target computer to obtain information relating to the person 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

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

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

(f) in the case of an unsworn application—that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and

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

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

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

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

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

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

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

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

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

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

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

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

(h) in the case of a control order access warrant issued on the basis of a control order that is in force in relation to a

person—whether the access to data held in the relevant target computer in accordance with the warrant would be the means of obtaining the evidence or information sought to be obtained, that is likely to have the least interference with any person's privacy; and

(i) in the case of a control order access warrant issued on the basis of a control order that is in force in relation to a person—the possibility that the person:

(i) has engaged, is engaging, or will engage, in a terrorist act; or

(ii) has provided, is providing, or will provide, support for a terrorist act; or

(iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or

(iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or

(v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; or

(vi) has contravened, is contravening, or will contravene, the control order; or

(vii) will contravene a succeeding control order; and

(j) in the case of a warrant sought in relation to a relevant offence or a recovery order—any previous warrant sought or issued under this Division in connection with the same alleged offence or the same recovery order; and

(k) in the case of a control order access warrant issued on the basis of a control order that is in force in relation to a person—any previous control order access warrant sought or issued on the basis of a control order relating to the person.

27D What must a computer access warrant contain?

(1) A computer access warrant must:

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

(b) specify:

(i) the name of the applicant; and

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

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

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

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

(vi) the date the warrant is issued; and

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

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

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

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

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

(2) If a control order access warrant is issued on the basis of a control order that is in force in relation to a person, the warrant must also specify the following details in relation to the control order:

(a) the name of the person;

(b) the date the control order was made;

(c) whether the control order is an interim control order or a confirmed control order.

(3) A warrant may only be issued:

(a) for a period of no more than 90 days; or

(b) if the warrant is issued for the purposes of an integrity operation—for a period of no more than 21 days.

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

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

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

(6) As soon as practicable after completing and signing a warrant issued on a remote application, the person issuing it must:

(a) inform the applicant of:

(i) the terms of the warrant; and

(ii) the date on which, and the time at which, the warrant was issued; and

(b) give the warrant to the applicant while retaining a copy of the warrant for the person's own record.

27E What a computer access warrant authorises

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

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

(a) entering specified premises for the purposes of doing the things mentioned in this subsection;

(b) entering any premises for the purposes of gaining entry to, or exiting, the specified premises;

(c) using:

(i) the target computer; 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 target computer at any time while the warrant is in force, in order to determine whether the relevant data is covered by the warrant;

(d) if necessary to achieve the purpose mentioned in paragraph (c)—adding, copying, deleting or altering other data in the target computer;

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

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

(f) removing a computer or other thing from premises for the purposes of doing any thing specified in the warrant in accordance with this subsection, and returning the computer or other thing to the premises;

(g) copying any data to which access has been obtained, and that:

(i) appears to be relevant for the purposes of determining whether the relevant data is covered by the warrant; or

(ii) is covered by the warrant;

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

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

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

(3) For the purposes of paragraph (2)(g), if:

(a) access has been obtained to data; and

(b) the data is subject to a form of electronic protection;

the data is taken to be relevant for the purposes of determining whether the relevant data is covered by the warrant.

When data is covered by a warrant

(4) For the purposes of this section, data is ***covered by*** a warrant if:

(a) in the case of a warrant sought in relation to a relevant offence—access to the data is necessary as described in paragraph 27A(1)(c); or

(b) in the case of a warrant sought in relation to a recovery order—access to the data may assist as described in paragraph 27A(3)(b); or

(c) in the case of a warrant sought in relation to a mutual assistance authorisation—access to the data is necessary as described in paragraph 27A(4)(b); or

(d) in the case of a warrant sought for the purposes of an integrity operation—access to the data will assist as described in paragraph 27A(5)(b); or

(e) in the case of a control order access warrant—access to the data would be likely to substantially assist as described in paragraph 27A(6)(b).

Certain acts not authorised

(5) Subsection (2) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

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

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

Warrant must provide for certain matters

(6) A computer access warrant must:

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

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

Concealment of access etc.

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

(a) a computer access warrant; or

(b) this subsection;

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

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

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

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

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

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

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

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

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

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

at the following time:

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

(k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).

27F Extension and variation of computer access warrant

(1) A law enforcement officer to whom a computer access warrant has been issued (or another person on the law enforcement officer's behalf) may apply, at any time before the expiry of the warrant:

(a) for an extension of the warrant for a period of no more than:

(i) 90 days after the day the warrant would otherwise expire; or

(ii) if the warrant is issued for the purposes of an integrity operation—21 days after the day the warrant would otherwise expire; or

(b) for a variation of any of the other terms of the warrant.

(2) The application is to be made to an eligible Judge or to a nominated AAT member and must be accompanied by the original warrant.

(3) Sections 27A and 27B apply, with any necessary changes, to an application under this section as if it were an application for the warrant.

(4) The eligible Judge or nominated AAT member may grant an application if satisfied that the matters referred to in subsection 27C(1) still exist, having regard to the matters in subsection 27C(2).

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

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

27G Revocation of computer access warrant

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

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

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

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

(5) If:

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

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

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

27H Discontinuance of access under warrant

Scope

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

Discontinuance of access

(2) If:

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

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

(i) the commission of the relevant offence; or

(ii) the identity or location of the offender;

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

(3) If:

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

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

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

(4) If:

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

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

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

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

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

(5) If:

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

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

(i) access to data under the warrant is no longer necessary for the purposes of the integrity operation; or

(ii) the integrity authority for the integrity operation is no longer in effect;

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

(6) If:

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

(b) the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded is satisfied that access to data under the warrant to obtain information

relating to the person is no longer required for any of the following purposes:

(i) protecting the public from a terrorist act;

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

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country;

(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;

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

(7) If:

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

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

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

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

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

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

(b) if the warrant was issued in relation to a recovery order—of enabling the location and safe recovery of the child to whom the order relates; or

(c) if the warrant was issued in relation to a mutual assistance authorisation—of enabling evidence to be obtained of:

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

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

the law enforcement officer must immediately inform the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded.

(10) In the case of a warrant issued for the purposes of an integrity operation, if the law enforcement officer to whom the warrant is issued, or who is primarily responsible for executing the warrant, believes that:

(a) access to data under the warrant is no longer necessary for those purposes; or

(b) the integrity authority for the integrity operation is no longer in effect;

the law enforcement officer must immediately inform the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded.

50 After subsection 28(1)

Insert:

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

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

(b) access to data held in the target computer is immediately necessary for the purpose of dealing with that risk; and

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

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

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

(a) a particular computer;

(b) a computer on particular premises;

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

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

After "application", insert "mentioned in subsection (1) or (1A)".

52 After subsection 29(1)

Insert:

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

(a) a recovery order is in force; and

(b) the law enforcement officer reasonably suspects that:

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

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

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

(a) a particular computer;

(b) a computer on particular premises;

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

53 Subsections 29(2) and (3)

After "application", insert "mentioned in subsection (1) or (1A)".

54 After subsection 30(1)

Insert:

(1A) If:

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

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

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

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

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

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

or more than one offence; and

(b) the law enforcement officer reasonably suspects that:

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

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

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

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

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

(a) a particular computer;

(b) a computer on particular premises;

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

55 Subsection 30(2)

After "application", insert "mentioned in subsection (1) or (1A)".

56 Subsection 30(3)

Omit "The", substitute "In the case of an application mentioned in subsection (1), the".

57 At the end of section 30

Add:

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

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

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

58 Subsections 32(1) and (2)

After "authorisation", insert "for the use of a surveillance device".

59 After subsection 32(2)

Insert:

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

60 After subsection 32(3)

Insert:

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

61 Subsection 33(2)

Omit "The", substitute "In the case of an application for an emergency authorisation for the use of a surveillance device, the".

62 After subsection 33(2)

Insert:

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

(a) must specify:

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

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

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

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

63 Subsection 34(1)

Omit "section 28", substitute "subsection 28(1)".

64 After subsection 34(1)

Insert:

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

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

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

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

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

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

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

65 Subsection 34(2)

Omit "section 29", substitute "subsection 29(1)".

66 After subsection 34(2)

Insert:

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

(a) the urgency of enforcing the recovery order;

(b) the extent to which access to data held in the target computer mentioned in that subsection would assist in the location and safe recovery of the child to whom the recovery order relates;

(c) the extent to which law enforcement officers could have used alternative methods to assist in the location and safe recovery of the child;

(d) how much the use of alternative methods to assist in the location and safe recovery of the child might have prejudiced the effective enforcement of the recovery order;

(e) whether or not it was practicable in the circumstances to apply for a computer access warrant.

67 Subsection 34(3)

Omit "section 30", substitute "subsection 30(1)".

68 At the end of section 34

Add:

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

(a) the nature of the risk of the loss of evidence;

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

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

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

(e) whether or not it was practicable in the circumstances to apply for a computer access warrant.

69 Section 35 (heading)

Repeal the heading, substitute:

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

70 Subsection 35(1)

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

71 Subsection 35(1)

Omit "approve the application", substitute "give the approval".

72 Subsection 35(2)

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

73 Subsection 35(2)

Omit "approve the application", substitute "give the approval".

74 Subsection 35(3)

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

75 Subsection 35(3)

Omit "approve the application", substitute "give the approval".

76 After section 35

Insert:

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

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

(a) there was a risk of serious violence to a person or substantial damage to property; and

(b) accessing data held in the target computer mentioned in that subsection may have helped reduce the risk; and

(c) it was not practicable in the circumstances to apply for a computer access warrant.

(2) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 29(1A) in relation to a recovery order, the eligible Judge or nominated AAT member may give the approval if satisfied that:

(a) the recovery order was in force at the time the emergency authorisation was given; and

(b) there were reasonable grounds to suspect that:

(i) the enforcement of the recovery order was urgent; and

(ii) accessing data held in the target computer mentioned in that subsection may have assisted in the prompt location

and safe recovery of the child to whom the order relates; and

(iii) it was not practicable in the circumstances to apply for a computer access warrant.

(3) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 30(1A), the eligible Judge or nominated AAT member may give the approval if satisfied that:

(a) there were reasonable grounds to suspect that:

(i) there was a risk of loss of evidence; and

(ii) accessing data held in the target computer mentioned in that subsection may have helped reduce the risk; and

(b) it was not practicable in the circumstances to apply for a computer access warrant.

(4) If, under subsection (1), (2) or (3), the eligible Judge or nominated AAT member approves the giving of an emergency authorisation, the eligible Judge or nominated AAT member may:

(a) unless paragraph (b) applies—issue a computer access warrant relating to the continued access to data held in the relevant target computer as if the application for the approval were an application for a computer access warrant under Division 4 of Part 2; or

(b) if the eligible Judge or nominated AAT member is satisfied that, since the application for the emergency authorisation, the activity that required access to data held in the relevant target computer has ceased—order that access to data held in that computer cease.

(5) If, under subsection (1), (2) or (3), the eligible Judge or nominated AAT member does not approve the giving of an emergency authorisation, the eligible Judge or nominated AAT member may:

(a) order that access to data held in the relevant target computer cease; or

(b) if the eligible Judge or nominated AAT member is of the view that, although the situation did not warrant the emergency authorisation at the time that authorisation was given, the use of a computer access warrant under Division 4

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

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

77 Section 36

After "section 35", insert "or 35A".

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

Repeal the definition, substitute:

appropriate consenting official, in relation to a foreign country:

(a) when used in section 42 or 43—means an official of that country having authority in that country to give consent to the use of surveillance devices in that country or on a vessel or aircraft registered under the laws of that country; or

(b) when used in section 43A or 43B—means an official of that country having authority in that country to give consent to access to data held in computers in that country or on a vessel or aircraft registered under the laws of that country.

79 Section 42 (heading)

Repeal the heading, substitute:

42 Extraterritorial operation of surveillance device warrants

80 Subsection 42(1)

Before "warrant" (first occurring), insert "surveillance device".

81 After paragraph 42(2)(a)

Insert:

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

82 Paragraph 42(2)(b)

After "of that", insert "section 33".

83 Subsection 42(2)

After "whom the", insert "section 33".

84 Subsection 42(2)

After "consideration of that", insert "section 33".

85 Paragraph 42(3)(a)

Before "warrant", insert "surveillance device".

86 Subsections 42(6) and (9)

Before "warrant" (first occurring), insert "surveillance device".

87 At the end of Part 5

Add:

43A Extraterritorial operation of computer access warrants

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

(a) in a foreign country; or

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

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

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

(2) If:

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

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

(c) before the completion of consideration of that section 33 application, it becomes apparent to the applicant that there will be a need for access to data held in a computer:

(i) in a foreign country; or

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

to assist in the investigation to which the emergency authorisation related;

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

(3) If:

(a) a computer access warrant has been issued in relation to the investigation of a relevant offence in response to an application by or on behalf of a federal law enforcement officer; and

(b) after the issue of the warrant, it becomes apparent to the law enforcement officer primarily responsible for executing the warrant that there will be a need for access to data held in a computer that is:

(i) in a foreign country; or

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

to assist in that investigation;

the warrant is taken to permit that access if, and only if, the access has been agreed to by an appropriate consenting official of the foreign country.

(4) Subsections (1), (2) and (3) do not apply to a computer access warrant authorising access to data if:

(a) the person, or each of the persons, responsible for executing the warrant will be physically present in Australia; and

(b) the location where the data is held is unknown or cannot reasonably be determined.

(5) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the contiguous zone of Australia; and

(b) the relevant offence in respect of which it becomes apparent that access to data held in a computer on the vessel will be required is an offence relating to the customs, fiscal, immigration or sanitary laws of Australia;

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 such waters.

(6) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the Australian fishing zone; and

(b) the relevant offence in respect of which it becomes apparent that access to data held in a computer on the vessel will be required is an offence against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991* or section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait Fisheries Act 1984*;

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

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

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

Insert:

(aa) any information (other than general computer access intercept information) obtained from access to data under:

(i) a computer access warrant; or

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

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

Add "or".

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

Insert:

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

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

Add:

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

92 Section 46 (heading)

Repeal the heading, substitute:

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

93 Paragraph 46(1)(a)

After "protected information", insert "or general computer access intercept information".

94 Subsection 46(2)

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

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

(aa) using a surveillance device; or

(ab) accessing data held in a computer;

the officer in charge of the agency:

95 After subsection 46A(1)

Insert:

(1A) If:

(a) a record or report is in the possession of a law enforcement agency; and

(b) the record or report comprises information obtained from access to data under a control order access warrant issued on the basis of a control order made in relation to a person; and

(c) the warrant was issued for the purpose, or for purposes that include the purpose, of obtaining information that would be likely to substantially assist in connection with determining whether the control order, or any succeeding control order, has been, or is being, complied with; and

(d) access to the data occurred when the control order had been made, but had not come into force because it had not been served on the person; and

(e) the chief officer of the agency is satisfied that none of the information obtained from accessing the data is likely to assist in connection with:

(i) the protection of the public from a terrorist act; or

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

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country;

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

96 Subsection 46A(2)

After "subsection (1)", insert "or (1A)".

97 After section 47

Insert:

47A Protection of computer access technologies and methods

(1) In a proceeding, a person may object to the disclosure of information on the ground that the information, if disclosed, could reasonably be expected to reveal details of computer access technologies or methods.

(2) If the person conducting or presiding over the proceeding is satisfied that the ground of objection is made out, the person may order that the person who has the information not be required to disclose it in the proceeding.

(3) In determining whether or not to make an order under subsection (2), the person conducting or presiding over the proceeding must take into account whether disclosure of the information:

(a) is necessary for the fair trial of the defendant; or

(b) is in the public interest.

(4) Subsection (2) does not affect a provision of another law under which a law enforcement officer cannot be compelled to disclose information or make statements in relation to the information.

(5) If the person conducting or presiding over a proceeding is satisfied that publication of any information disclosed in the proceeding could reasonably be expected to reveal details of computer access technologies or methods, the person must make any orders prohibiting or restricting publication of the information that the person considers necessary to ensure that those details are not revealed.

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

(7) In this section:

computer access technologies or methods means:

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

(i) a computer; 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 held in the computer; or

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

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

(c) a computer access warrant; or

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

proceeding includes a proceeding before a court, tribunal or Royal Commission.

98 Subsection 49(2)

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

99 After subsection 49(2A)

Insert:

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

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

(b) if so:

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

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

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

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

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

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

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

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

the general use made, or to be made, of any evidence or information obtained by the access to data; and

(ix) if the warrant is a control order access warrant—give the details specified in subsection (2C); and

(x) give details of the communication of evidence or information obtained by access to data held in the computer to persons other than officers of the agency; and

(xi) give details of the compliance with the conditions (if any) to which the warrant or authorisation was subject; and

(c) if the warrant or authorisation was extended or varied, state:

(i) the number of extensions or variations; and

(ii) the reasons for them.

(2C) For the purposes of subparagraph (2B)(b)(ix), the details are:

(a) the benefit of obtaining access to data held in the computer 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

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether a control order has been, or is being, complied with; and

(b) the general use to be made of any evidence or information obtained by access to data held in the computer.

100 Subsection 49A(1)

After "control order warrant", insert "or control order access warrant".

101 Paragraph 49A(2)(a)

After "control order warrant", insert "or control order access warrant".

102 After paragraph 49A(2)(b)

Insert:

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

103 After paragraph 49A(2)(c)

Insert:

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

104 Subsection 49A(3)

After "control order warrant", insert "or control order access warrant".

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

Repeal the paragraphs, substitute:

(g) the number of arrests made by law enforcement officers of the agency during that year on the basis (wholly or partly) of information obtained by:

(i) the use of a surveillance device under a warrant; or

(ii) access under a warrant to data held in a computer; or

(iii) an emergency authorisation for the use of a surveillance device; or

(iv) an emergency authorisation for access to data held in a computer; or

(v) a tracking device authorisation; and

(h) the number of instances during that year in which the location and safe recovery of children to whom recovery orders related was assisted (wholly or partly) by information obtained by:

(i) the use of a surveillance device under a warrant; or

(ii) access under a warrant to data held in a computer; or

(iii) an emergency authorisation for the use of a surveillance device; or

(iv) an emergency authorisation for access to data held in a computer; or

(v) a tracking device authorisation; and

(i) the number of prosecutions for relevant offences that were commenced during that year in which information obtained by:

(i) the use of a surveillance device under a warrant; or

(ii) access under a warrant to data held in a computer; or

(iii) an emergency authorisation for the use of a surveillance device; or

(iv) an emergency authorisation for access to data held in a computer; or

(v) a tracking device authorisation;

was given in evidence and the number of those prosecutions in which a person was found guilty; and

106 Paragraph 50(1)(j)

After "surveillance devices", insert ", access to data held in computers".

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

Repeal the definition, substitute:

control order information means:

(a) information that, if made public, could reasonably be expected to enable a reasonable person to conclude that a control order warrant authorising:

(i) the use of a surveillance device on particular premises; or

(ii) the use of a surveillance device in or on a particular object or class of object; or

(iii) the use of a surveillance device in respect of the conversations, activities or location of a particular person;

is likely to be, or is not likely to be, in force; or

(b) information that, if made public, could reasonably be expected to enable a reasonable person to conclude that a control order access warrant authorising:

(i) access to data held in a particular computer; or

(ii) access to data held in a computer on particular premises; or

(iii) access to data held in a computer associated with, used by or likely to be used by, a particular person;

is likely to be, or is not likely to be, in force.

108 Paragraph 51(b)

Omit "or 27(4)", substitute ", 27(4) or 27G(4)".

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

Repeal the paragraphs, substitute:

(e) details of each use by the agency, or by a law enforcement officer of the agency, of information obtained by:

(i) the use of a surveillance device by a law enforcement officer of the agency; or

(ii) access, by a law enforcement officer of the agency, to data held in a computer;

(f) details of each communication by a law enforcement officer of the agency to a person other than a law enforcement officer of the agency of information obtained by:

(i) the use of a surveillance device by a law enforcement officer of the agency; or

(ii) access, by a law enforcement officer of the agency, to data held in a computer;

(g) details of each occasion when, to the knowledge of a law enforcement officer of the agency, information obtained by:

(i) the use of a surveillance device by a law enforcement officer of the agency; or

(ii) access, by a law enforcement officer of the agency, to data held in a computer;

was given in evidence in a relevant proceeding;

(h) details of each occasion when, to the knowledge of a law enforcement officer of the agency, information obtained by:

(i) the use of a surveillance device by a law enforcement officer of the agency; or

(ii) access, by a law enforcement officer of the agency, to data held in a computer;

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

110 Paragraph 52(1)(j)

After "subsection 46A(1)", insert "or (1A)".

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

Insert:

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

112 At the end of subsection 62(1)

Add:

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

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

(ii) the making use of; or

(iii) the making of a record of; or

(iv) the custody of a record of;

information obtained from access to data under:

(v) a computer access warrant; or

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

113 Subsection 62(3)

After "section 35", insert "or 35A".

114 After section 64

Insert:

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

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

person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to do one or more of the following:

(a) access data held in a computer that is the subject of:

(i) a computer access warrant; or

(ii) an emergency authorisation given in response to an application under subsection 28(1A), 29(1A) or 30(1A);

(b) copy data held in the computer described in paragraph (a) to a data storage device;

(c) convert into documentary form or another form intelligible to a law enforcement officer:

(i) data held in the computer described in paragraph (a); or

(ii) data held in a data storage device to which the data was copied as described in paragraph (b).

Warrants and emergency authorisations relating to relevant offences

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

(a) a computer access warrant issued in relation to a relevant offence; or

(b) an emergency authorisation given in response to an application under subsection 28(1A);

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

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

(i) the commission of those offences; or

(ii) the identity or location of the offenders; and

(d) the specified person is:

(i) reasonably suspected of having committed any of the offences to which the warrant or emergency authorisation relates; or

(ii) the owner or lessee of the computer or device; or

(iii) an employee of the owner or lessee of the computer or device; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or

(v) a person who uses or has used the computer or device; or

(vi) a person who is or was a system administrator for the system including the computer or device; and

(e) the specified person has relevant knowledge of:

(i) the computer or device or a computer network of which the computer or device forms or formed a part; or

(ii) measures applied to protect data held in the computer or device.

Warrants and emergency authorisations relating to recovery orders

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

(a) a computer access warrant issued in relation to a recovery order; or

(b) an emergency authorisation given in response to an application under subsection 29(1A);

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

(c) there are reasonable grounds for suspecting that access to data held in the computer may assist in the location and safe recovery of the child to whom the recovery order relates; and

(d) the specified person is:

(i) the owner or lessee of the computer or

(ii) an employee of the owner or lessee of the computer; or

(iii) a person engaged under a contract for services by the owner or lessee of the computer; or

(iv) a person who uses or has used the computer; or

(v) a person who is or was a system administrator for the system including the computer; and

(e) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

Warrants relating to mutual assistance authorisations

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

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

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

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

(b) the specified person is:

(i) reasonably suspected of committing the offence to which the authorisation relates; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer; or

(v) a person who uses or has used the computer; or

(vi) a person who is or was a system administrator for the system including the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

Warrants relating to integrity operations

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

(a) there are reasonable grounds for suspecting that access to data held in the computer will assist the conduct of the 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.

Warrants relating to control orders

(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

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

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

(b) the specified person is:

(i) the subject of the control order; 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.

Emergency authorisations relating to risk of loss of evidence

(7) In the case of a computer that is the subject of an emergency authorisation given in response to an application under subsection 30(1A), the eligible Judge or nominated AAT member may grant the assistance order if the eligible Judge or nominated AAT member is satisfied that:

(a) there are reasonable grounds for suspecting that access to data held in the computer is necessary to prevent the loss of any evidence relevant to the investigation to which the subsection 30(1A) application relates; and

(b) the specified person is:

(i) reasonably suspected of having committed any of the offences to which the emergency authorisation relates; or

(ii) the owner or lessee of the computer or device; or

(iii) an employee of the owner or lessee of the computer or device; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or

(v) a person who uses or has used the computer or device; or

(vi) a person who is or was a system administrator for the system including the computer or device; and

(c) the specified person has relevant knowledge of:

(i) the computer or device or a computer network of which the computer or device forms or formed a part; or

(ii) measures applied to protect data held in the computer or device.

Offence

(8) A person commits an offence if:

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

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

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

(d) the omission contravenes the requirement.

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

115 After subsection 65(1)

Insert:

(1A) If:

(a) information or a record is purportedly obtained through accessing, under a computer access warrant or emergency authorisation, particular data held in a computer; and

(b) there is a defect or irregularity in relation to the warrant or emergency authorisation; and

(c) but for that defect or irregularity, the warrant or emergency authorisation would be a sufficient authority for accessing the data;

then:

(d) access to the data is taken to be as valid; and

(e) the information or record obtained through accessing the data may be dealt with, or given in evidence in any proceeding;

as if the warrant or emergency authorisation did not have that defect or irregularity.

116 Subsection 65(2)

After "subsection (1)", insert "or (1A)".

117 After subsection 65A(2)

Insert:

Control order access warrant

(2A) If:

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

(b) a court subsequently declares the interim control order to be void;

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

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

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

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

118 Section 65B (heading)

Repeal the heading, substitute:

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

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

Insert:

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

Telecommunications Act 1997

119A After paragraph 313(7)(c)

Insert:

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

Telecommunications (Interception and Access) Act 1979

120 Subsection 5(1)

Insert:

ASIO computer access intercept information means information obtained under:

(a) an ASIO computer access warrant; or

(b) subsection 25A(8) of the *Australian Security Intelligence Organisation Act 1979*; or

(c) subsection 27A(3C) of the *Australian Security Intelligence Organisation Act 1979*; or

(d) an authorisation under section 27E of the *Australian Security Intelligence Organisation Act 1979*; or

(e) subsection 27E(6) of the *Australian Security Intelligence Organisation Act 1979*;

by intercepting a communication passing over a telecommunications system.

ASIO computer access warrant means:

(a) a warrant issued under section 25A of the *Australian Security Intelligence Organisation Act 1979*; or

(b) a warrant issued under section 27A of the *Australian Security Intelligence Organisation Act 1979* that authorises the Organisation to do any of the acts or things referred to in subsection 25A(4) or (8) of that Act; or

(c) an authorisation under section 27E of the *Australian Security Intelligence Organisation Act 1979*.

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

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

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

Add ", but does not include a record of general computer access intercept information".

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

After "definition)", insert ", a general computer access warrant or an ASIO computer access warrant".

123 After paragraph 7(2)(b)

Insert:

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

(bb) the interception of a communication under subsection 27E(7) of the *Surveillance Devices Act 2004*; or

123A Subsection 31(1)

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

system:

(a) if one or more carriers are specified in the request for the purposes of this paragraph—by:

(i) employees of the security authority authorised under section 31B; and

(ii) employees of those carriers; or

(b) if no carriers are specified in the request for the purposes of paragraph (a)—by employees of the security authority authorised under section 31B.

123B Subsection 31A(1)

Omit "system by employees of the security authority authorised under section 31B.", substitute:

system:

(a) if one or more carriers are specified in the request for the purposes of paragraph 31(1)(a)—by:

(i) employees of the security authority authorised under section 31B; and

(ii) employees of those carriers; or

(b) if no carriers are specified in the request for the purposes of paragraph 31(1)(a)—by employees of the security authority authorised under section 31B.

123BA After subsection 31A(4)

Insert:

(4A) If paragraph (1)(a) applies to the authorisation, this Part does not require that an authorised interception must involve:

(a) one or more employees of the security authority referred to in that paragraph; and

(b) one or more employees of a carrier referred to in that paragraph;

acting together or in the presence of each other.

123C After section 31A

Insert:

31AA Carrier to be notified of authorisation etc.

(1) If:

(a) the Attorney-General gives a section 31A authorisation in response to an application made by:

(i) the head (however described) of a security authority; or

(ii) a person acting as that head; and

(b) the authorisation covers the employees of a carrier;

the head (however described) of the security authority, or a person acting as that head, must cause a copy of the authorisation to be given to the authorised representative of the carrier as soon as practicable.

(2) If:

(a) the Attorney-General has given a section 31A authorisation in response to an application made by:

(i) the head (however described) of a security authority; or

(ii) a person acting as that head; and

(b) the authorisation is varied or revoked; and

(c) the authorisation covers the employees of a carrier;

the head (however described) of the security authority, or a person acting as that head, must cause:

(d) an authorised representative of the carrier to be immediately informed of the variation or revocation; and

(e) a copy of the variation or revocation to be given to the authorised representative as soon as practicable.

123D At the end of Part 2-4

Add:

31E Employees of security authorities

(1) For the purposes of this Part:

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

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

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

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

(b) the agency is a security authority;

the person is taken to be an employee of the security authority.

124 After section 63AA

Insert:

63AB Dealing in general computer access intercept information

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

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

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

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

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

(2) A person may:

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

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

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

if the information relates, or appears to relate, to the involvement, or likely involvement, of a person in one or more of the following activities:

(d) activities that present a significant risk to a person's safety;

(e) acting for, or on behalf of, a foreign power (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);

(f) activities that are, or are likely to be, a threat to security;

(g) activities that pose a risk, or are likely to pose a risk, to the operational security (within the meaning of the *Intelligence Services Act 2001*) of the Organisation or of ASIS, AGO or ASD (within the meanings of that Act);

(h) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);

(i) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).

63AC Dealing in ASIO computer access intercept information

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

(a) communicate ASIO computer access intercept information to another person; or

(b) make use of ASIO computer access intercept information; or

(c) make a record of ASIO computer access intercept information; or

(d) give ASIO computer access intercept information in evidence in a proceeding.

(2) A person may:

(a) communicate ASIO computer access intercept information to another person; or

(b) make use of ASIO computer access intercept information; or

(c) make a record of ASIO computer access intercept information;

if the information relates, or appears to relate, to the involvement, or likely involvement, of a person in one or more of the following activities:

(d) activities that present a significant risk to a person's safety;

(e) acting for, or on behalf of, a foreign power (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);

(f) activities that are, or are likely to be, a threat to security;

(g) activities that pose a risk, or are likely to pose a risk, to the operational security (within the meaning of the *Intelligence Services Act 2001*) of the Organisation or of ASIS, AGO or ASD (within the meanings of that Act);

(h) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);

(i) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).

124A At the end of section 63B

Add:

(5) If an employee of a carrier has obtained lawfully intercepted information under a section 31A authorisation that was given in response to an application made by the head (however described) of a security authority or a person acting as that head, the employee may:

(a) communicate the information to:

(i) an employee of the security authority; or

(ii) another employee of the carrier; or

(iii) if the authorisation covers the employees of one or more other carriers—an employee of any of those other carriers; or

(b) make use of the information; or

(c) make a record of the information;

if:

(d) the employee does so for the purposes of the development or testing of technologies, or interception capabilities, to which the authorisation relates; and

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

125 Paragraph 64(1)(a)

After "foreign intelligence information", insert "or ASIO computer access intercept information".

126 Paragraph 65(1)(a)

After "information", insert "other than ASIO computer access intercept information".

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

Add:

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

(a) a staff member of an authority of the Commonwealth; or

(b) a staff member of an authority of a State;

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

(c) that authority; or

(d) the Organisation.

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

(a) ASIS, ASD or AGO, as the case requires; or

(b) the Organisation.

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

(a) that body; or

(b) the Organisation.

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

126A Paragraph 65A(1)(a)

After "foreign intelligence information", insert "or information obtained under a section 31A authorisation".

127 Paragraph 67(1)(a)

After "foreign intelligence information", insert "or general computer access intercept information".

128 Section 68

After "communicate lawfully intercepted information", insert "(other than general computer access intercept information)".

129 Subsection 74(1)

After "foreign intelligence information", insert ", general computer access intercept information or ASIO computer access intercept information".

130 Subsection 75(1)

After "other than", insert "a general computer access warrant or".

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

After "63A,", insert "63AB, 63AC,".

131A After paragraph 108(2)(ca)

Insert:

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

Part 2—Application provisions

132 Application—computer access warrants

(1) The amendments of sections 25A and 27A of the *Australian Security Intelligence Organisation Act 1979* made by this Schedule apply in relation to a warrant issued after the commencement of this item.

(2) The amendments of section 27E of the *Australian Security Intelligence Organisation Act 1979* made by this Schedule apply in relation to an authorisation given after the commencement of this item.

(3) The amendments of sections 50 and 50A of the *Surveillance Devices Act 2004* made by this Schedule apply in relation to a report in respect of:

(a) the financial year in which this item commences; or

(b) a later financial year.

(4) The amendment of section 31 of the *Telecommunications (Interception and Access) Act 1979* made by this Schedule applies in relation to a request made after the commencement of this item.

(5) The amendments of section 31A of the *Telecommunications (Interception and Access) Act 1979* made by this Schedule apply in relation to an authorisation given in response to a request made after the commencement of this item.

Part 3—Amendments contingent on the commencement of the Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018

International Criminal Court Act 2002

133 After Division 12A of Part 4

Insert:

Division 12B—Requests for access to data held in computers

79B Authorising applications for computer access warrants

(1) The Attorney-General may authorise, in writing, an eligible law enforcement officer to apply for a computer access warrant under section 27A of the *Surveillance Devices Act 2004* if:

(a) the ICC has requested the Attorney-General to arrange for the access to data held in a computer (the ***target computer***); and

(b) the Attorney-General is satisfied that an investigation is being conducted by the Prosecutor, or a proceeding is before the ICC; and

(c) the Attorney-General is satisfied that the ICC has given appropriate undertakings for:

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

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

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

Note: The eligible law enforcement officer can only apply for the warrant if the officer reasonably suspects that the access to data held in the target

computer is necessary for the investigation or proceeding (see subsection 27A(4) of the *Surveillance Devices Act 2004*).

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

(a) a particular computer;

(b) a computer on particular premises;

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

(3) In this section:

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

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

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

eligible law enforcement officer means a person mentioned in column 3 of table item 5 in subsection 6A(6), or column 3 of table 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

Insert:

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

32B Authorising applications for computer access warrants

(1) The Attorney-General may authorise, in writing, an eligible law enforcement officer to apply for a computer access warrant under section 27A of the *Surveillance Devices Act 2004* if:

(a) a Tribunal has requested the Attorney-General to arrange for access to data held in a computer (the ***target computer***); and

(b) the Attorney-General is satisfied that a proceeding is before, or an investigation is being conducted by, the Tribunal; and

(c) the Attorney-General is satisfied that the Tribunal has given appropriate undertakings for:

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

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

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

Note: The eligible law enforcement officer can only apply for the warrant if the officer reasonably suspects that the access to data held in the target computer is necessary for the investigation or proceeding (see subsection 27A(4) of the *Surveillance Devices Act 2004*).

(2) In this section:

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

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

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

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

Surveillance Devices Act 2004

135 Subsection 6(1) (definition of *international assistance application*)

Repeal the definition, substitute:

international assistance application means:

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

(b) an application for a computer access warrant;

made under an international assistance authorisation.

136 Subsection 6(1) (paragraph (a) of the definition of *international assistance authorisation*)

After "15CA(1)", insert "or 15CC(1)".

137 Subsection 27A(4)

Repeal the subsection, substitute:

Warrants sought for international assistance investigations

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

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

(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:

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

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

138 Paragraphs 27C(1)(c) and (2)(a)

Omit "a mutual assistance authorisation", substitute "an international assistance authorisation".

139 Paragraph 27C(2)(f)

Repeal the paragraph, substitute:

(f) in the case of a warrant sought in relation to an international assistance authorisation—the likely evidentiary or intelligence value of any evidence or information sought to be obtained, to the extent that this is possible to determine from information obtained from the international entity to which the authorisation relates; and

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

Repeal the paragraph, substitute:

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

141 Paragraph 27E(3)(c)

Omit "a mutual assistance authorisation", substitute "an international assistance authorisation".

142 Paragraph 27H(4)(a)

Omit "a mutual assistance authorisation", substitute "an international assistance authorisation".

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

Repeal the subparagraph, substitute:

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

144 Paragraph 27H(9)(c)

Repeal the paragraph, substitute:

(c) if the warrant was issued in relation to an international assistance authorisation—of enabling evidence to be obtained of:

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

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

145 Subsection 64A(4)

Repeal the subsection, substitute:

Warrants relating to international assistance authorisations

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

grant the assistance order if the eligible Judge or nominated AAT member is satisfied that:

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

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

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

(b) the specified person is:

(i) reasonably suspected of committing an offence to which the authorisation relates; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer; or

(v) a person who uses or has used the computer; or

(vi) a person who is or was a system administrator for the system including the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

146 Application of amendments

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

(a) at or after the commencement of this item; or

(b) before the commencement of this item, if, immediately before that commencement, the Attorney-General had yet to make a decision on the request;

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

Schedule 3—Search warrants issued under the Crimes Act 1914

Crimes Act 1914

1 Subsection 3C(1)

Insert:

account-based data has the meaning given by section 3CAA.

carrier means:

(a) a carrier within the meaning of the *Telecommunications Act 1997*; or

(b) a carriage service provider within the meaning of that Act.

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

electronic service has the same meaning as in the *Enhancing Online Safety Act 2015*.

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

2 After section 3C

Insert:

3CAA Account-based data

(1) For the purposes of this Part, if:

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

(b) either:

(i) a person holds an account with the electronic service; or

(ii) a person is, or is likely to be, a user of an account with the electronic service; and

(c) the person can (with the use of appropriate equipment) access particular data provided by the service;

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

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

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

(b) either:

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

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

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

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

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

3 After subsection 3F(2)

Insert:

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

(a) to use:

(i) a computer, or data storage device, found in the course of a search authorised under the warrant; 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 computer or device mentioned in subparagraph (i) at any time when the warrant is in force, in order to determine whether the relevant data is evidential material of a kind specified in the warrant; and

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

(i) appears to be relevant for the purposes of determining whether the relevant data is evidential material of a kind specified in the warrant; or

(ii) is evidential material of a kind specified in the warrant; and

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

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

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

(a) to use:

(i) a computer found in the course of a search authorised under the warrant; or

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

(iii) any other electronic equipment;

for the purpose of obtaining access to data (the ***relevant account-based data***) that is account-based data in relation to:

(iv) a person who is the owner or lessee of the computer mentioned in subparagraph (i); or

(v) a person who uses or has used the computer mentioned in subparagraph (i); or

(vi) a deceased person who, before the person's death, was the owner or lessee of the computer mentioned in subparagraph (i); or

(vii) a deceased person who, before the person's death, used the computer mentioned in subparagraph (i);

in order to determine whether the relevant account-based data is evidential material of a kind specified in the warrant; and

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

(c) if, having regard to other methods (if any) of obtaining access to the relevant account-based 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 account-based 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:

(i) appears to be relevant for the purposes of determining whether the relevant account-based data is evidential material of a kind specified in the warrant; or

(ii) is evidential material of a kind specified in the warrant; and

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

(2C) Subsections (2A) and (2B) do not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

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

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

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

(a) at the premises; or

(b) at any other place.

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

(a) in the presence of the person; or

(b) at any other place.

4 Subsection 3K(3A)

Omit "14 days.", substitute:

whichever of the following is applicable:

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

(b) otherwise—14 days.

5 Subsection 3K(3B)

Omit "14 days", substitute "the time applicable under subsection (3A)".

6 Subsection 3K(3D)

Omit "7 days.", substitute:

whichever of the following is applicable:

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

(b) otherwise—7 days.

6A At the end of section 3K

Add:

Extended powers of examination and processing

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

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

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

(iii) any other electronic equipment;

for the purpose of obtaining access to data (the ***relevant account-based data***) that is account-based data in relation to:

(iv) a person who is the owner or lessee of the relevant computer; or

(v) a person who uses or has used the relevant computer; or

(vi) a deceased person who, before the person's death, was the owner or lessee of the relevant computer; or

(vii) a deceased person who, before the person's death, used the relevant computer;

in order to determine whether the relevant computer 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; and

(c) if, having regard to other methods (if any) of obtaining access to the relevant account-based 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 account-based 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 is a thing that may be seized under the warrant; and

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

(7) Subsections (5) and (6) do not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

unless the addition, deletion or alteration, or the doing of the thing, is necessary to determine:

(iii) in the case of subsection (5)—whether the relevant computer or device is a thing that may be seized under the warrant referred to in that subsection; or

(iv) in the case of subsection (6)—whether the relevant computer is a thing that may be seized under the warrant referred to in that subsection; or

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

(8) In the case of a warrant that was in force in relation to premises, it is immaterial whether a thing mentioned in subsection (5) or (6) is done:

(a) at the premises; or

(b) at any other place.

(9) In the case of a warrant that was in force in relation to a person, it is immaterial whether a thing mentioned in subsection (5) or (6) is done:

(a) in the presence of the person; or

(b) at any other place.

7 Subsection 3LAA(1)

Omit "to access data (including data held at another place).", substitute:

to:

(a) access data (including data held at another place); or

(b) access account-based data.

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

Insert:

(ia) is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by a warrant under section 3E; or

9 Subsection 3LA(5)

Repeal the subsection, substitute:

Offences

(5) A person commits an offence if:
(a) the person is subject to an order under this section; and
(b) the person is capable of complying with a requirement in the order; and
(c) the person omits to do an act; and
(d) the omission contravenes the requirement.

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

(6) A person commits an offence if:
(a) the person is subject to an order under this section; and
(b) the person is capable of complying with a requirement in the order; and
(c) the person omits to do an act; and
(d) the omission contravenes the requirement; and
(e) the offence to which the relevant warrant relates is:
(i) a serious offence; or
(ii) a serious terrorism offence.

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

10 After paragraph 3N(2)(a)

Insert:

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

11 After subsection 3ZQV(3)

Insert:

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

12 Application of amendments

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

Schedule 4—Search warrants issued under the Customs Act 1901

Customs Act 1901

1 Subsection 183UA(1)

Insert:

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

recently used conveyance, in relation to a search of a person, means a conveyance that the person had operated or occupied at any time within 24 hours before the search commenced.

1A Subsection 183UA(1) (definition of *search warrant*)

After "section 198", insert "or 199A".

2 Subsection 183UA(1)

Insert:

serious offence has the same meaning as in Part IAA of the *Crimes Act 1914.*

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

3 Section 198 (heading)

Repeal the heading, substitute:

198 When search warrants relating to premises can be issued

4 Section 199 (heading)

Repeal the heading, substitute:

199 The things that are authorised by a search warrant relating to premises

4A After subsection 199(4)

Insert:

(4A) A warrant that is in force in relation to premises authorises the executing officer or a person assisting:

(a) to use:

(i) a computer, or data storage device, found in the course of a search authorised under the warrant; 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 computer or device mentioned in subparagraph (i) at any time when the warrant is in force, in order to determine whether the relevant data is evidential material of a kind specified in the warrant; and

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

(i) appears to be relevant for the purposes of determining whether the relevant data is evidential material of a kind specified in the warrant; or

(ii) is evidential material of a kind specified in the warrant; and

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

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

(4B) Subsection (4A) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

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

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

(4C) It is immaterial whether a thing mentioned in subsection (4A) is done:

(a) at the warrant premises; or

(b) at any other place.

5 After section 199

Insert:

199A When search warrants relating to persons can be issued

(1) A judicial officer may issue a warrant authorising an ordinary search or a frisk search of a person if the judicial officer is satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that the person has in the person's possession, or will within the next 72 hours have in the person's possession, any computer, or data storage device, that is evidential material.

(2) If the person applying for the warrant has, at any time previously, applied for a warrant under this section relating to the same person,

the person applying for the warrant must state particulars of those applications, and their outcome, in the information.

(3) If a judicial officer issues a warrant, the judicial officer is to state in the warrant:

(a) the offence to which the warrant relates; and

(b) the name or description of the person to whom the warrant relates; and

(c) the name of the authorised person who, unless the authorised person inserts the name of another authorised person in the warrant, is to be responsible for executing the warrant; and

(d) the time at which the warrant expires (see subsection (4)); and

(e) whether the warrant may be executed at any time or only during particular hours.

(4) The time stated in the warrant under paragraph (3)(d) as the time at which the warrant expires must be a time that is not later than the end of the seventh day after the day on which the warrant is issued.

Example: If a warrant is issued at 3 pm on a Monday, the expiry time specified must not be later than midnight on Monday in the following week.

(5) The judicial officer is also to state, in a warrant in relation to a person:

(a) that the warrant authorises the seizure of a computer or data storage device found, in the course of the search, on or in the possession of the person or in a recently used conveyance, if the executing officer or a person assisting believes on reasonable grounds that:

(i) the computer or device is evidential material in relation to an offence to which the warrant relates; and

(ii) the seizure of the computer or device is necessary to prevent its concealment, loss or destruction or its use in committing an offence; and

(b) the kind of search of a person that the warrant authorises.

(6) Paragraph (3)(d) and subsection (4) do not prevent the issue of successive warrants in relation to the same person.

199B The things that are authorised by a search warrant relating to a person

(1) A warrant that is in force in relation to a person (the ***target person***) authorises the executing officer or person assisting:

(a) to search:

(i) the target person as specified in the warrant; and

(ii) any recently used conveyance;

for computers or data storage devices of the kind specified in the warrant; and

(b) to:

(i) seize computers or data storage devices of that kind; or

(ii) record fingerprints from computers or data storage devices; or

(iii) to take samples for forensic purposes from computers or data storage devices;

found in the course of the search; and

(c) to seize other things found on or in the possession of the target person or in the conveyance in the course of the search that the executing officer or person assisting believes on reasonable grounds to be:

(i) prohibited goods that are unlawfully carried by the target person; or

(ii) seizable items.

(2) A warrant that is in force in relation to a person (the ***target person***) authorises the executing officer or a person assisting:

(a) to use:

(i) a computer, or data storage device, found in the course of a search authorised under the warrant; 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 computer or device mentioned in subparagraph (i) at any time when the warrant is in force, in

order to determine whether the relevant data is evidential material of a kind specified in the warrant; and

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

(i) appears to be relevant for the purposes of determining whether the relevant data is evidential material of a kind specified in the warrant; or

(ii) is evidential material of a kind specified in the warrant; and

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

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

(3) Subsection (2) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

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

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

(4) It is immaterial whether a thing mentioned in subsection (2) is done:

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

(b) at any other place.

(5) If the warrant states that it may be executed only during particular hours, the warrant must not be executed outside those hours.

(6) If the warrant authorises an ordinary search or a frisk search of the target person, a search of the target person different from that so authorised must not be done under the warrant.

5A Subsection 200(1)

Omit "executing officer or a person assisting", substitute "executing officer of a warrant in relation to premises, or a person assisting,".

5AA Subsection 200(2)

Omit "thing found at the premises", substitute "thing found at warrant premises, or a thing found during a search under a warrant that is in force in relation to a person,".

5B Paragraph 200(2)(b)

Repeal the paragraph, substitute:

(b) for a thing found at warrant premises—the occupier of the premises consents in writing; or

(c) for a thing found during a search under a warrant that is in force in relation to a person—the person consents in writing.

5C Paragraph 200(3)(a)

Omit "occupier", substitute "person referred to in paragraph (2)(b) or (c) (as the case requires)".

5D Paragraph 200(3)(b)

Omit "the occupier", substitute "that person".

6 Subsection 200(3A)

Omit "72 hours.", substitute:

whichever of the following is applicable:

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

(b) otherwise—72 hours.

7 Subsection 200(3B)

Omit "72 hours", substitute "the time applicable under subsection (3A)".

7A Subsection 200(3C)

Omit "occupier of the premises, and the occupier", substitute "person referred to in paragraph (2)(b) or (c) (as the case requires), and that person".

8 After subsection 200(3C)

Insert:

(3D) If the thing is a computer or data storage device, a single extension cannot exceed 14 days.

8AA Subsection 200(4)

Omit "executing officer or a person assisting", substitute "executing officer of a warrant in relation to premises, or a person assisting,".

8A After section 201

Insert:

201AA Use of electronic equipment at other place

(1) If electronic equipment is moved to another place under subsection 200(2), the executing officer or a person assisting may operate the equipment to access data (including data held at another place).

(2) If the executing officer or person assisting suspects on reasonable grounds that any data accessed by operating the electronic equipment constitutes evidential material, the executing officer or person assisting may copy any or all of the data accessed by

operating the electronic equipment to a disk, tape or other associated device.

(3) If the Comptroller-General of Customs is satisfied that the data is not required (or is no longer required) for:

(a) investigating an offence against a law of the Commonwealth, a State or a Territory; or

(b) judicial proceedings or administrative review proceedings; or

(c) investigating or resolving a complaint under the *Ombudsman Act 1976* or the *Privacy Act 1988*;

the Comptroller-General of Customs must arrange for:

(d) the removal of the data from any device subject to customs control; and

(e) the destruction of any other reproduction of the data subject to customs control.

(4) If the executing officer or a person assisting, after operating the equipment, finds that evidential material is accessible by doing so, the executing officer or person assisting may:

(a) seize the equipment and any disk, tape or other associated device; or

(b) if the material can be put in documentary form—put the material in that form and seize the documents so produced.

(5) The executing officer or a person assisting may seize equipment under paragraph (4)(a) only if:

(a) it is not practicable to copy the data as mentioned in subsection (2) or to put the material in documentary form as mentioned in paragraph (4)(b); or

(b) possession of the equipment by the person referred to in paragraph 200(2)(b) or (c) (as the case requires) could constitute an offence.

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

Repeal the paragraphs, substitute:

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

(i) is on warrant premises; or

(ii) has been seized under this Subdivision; or

(iii) is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by a search warrant;

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

(c) convert into documentary form or another form intelligible to an executing officer:

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

(ii) data held in a data storage device to which the data was copied as described in paragraph (b).

10 Paragraph 201A(2)(a)

After "the computer", insert "or data storage device".

11 Subparagraph 201A(2)(b)(ii)

After "the computer", insert "or device".

12 Subparagraph 201A(2)(b)(iii)

Omit "; and", substitute "or device; or".

13 At the end of paragraph 201A(2)(b)

Add:

(iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or

(v) a person who uses or has used the computer or device; or

(vi) a person who is or was a system administrator for the system including the computer or device; and

14 Subparagraph 201A(2)(c)(i)

After "the computer or", insert "device or".

15 Subparagraph 201A(2)(c)(i)

After "which the computer", insert "or device".

16 Subparagraph 201A(2)(c)(i)

After "forms", insert "or formed".

17 Subparagraph 201A(2)(c)(ii)

After "the computer", insert "or device".

18 Subsection 201A(3)

Repeal the subsection, substitute:

Offences

(3) A person commits an offence if:

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

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

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

(d) the omission contravenes the requirement.

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

(4) A person commits an offence if:

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

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

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

(d) the omission contravenes the requirement; and

(e) the offence to which the relevant warrant relates is a serious offence.

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

18A Paragraph 201B(1)(a)

After "201(1)", insert "or 201AA(1)".

18B Paragraph 201B(1)(d)

After "or (2)", insert "or 201AA(2) or (4)".

18C Paragraph 202(1)(a)

Omit "or 201", substitute ", 201 or 201AA".

18D Paragraph 202A(2)(a)

After "201(2)(b)", insert "or 201AA(4)(a)".

19 Subsection 203K(5)

After "198(1),", insert "199A(1),".

20 Subsection 203M(4)

After "198,", insert "199A,".

21 Application of amendments

(1) The amendments of sections 199, 200 and 201A of the *Customs Act 1901* made by this Schedule apply in relation to a warrant issued after the commencement of this item.

(2) Section 201AA of the *Customs Act 1901* (as amended by this Schedule) applies in relation to a warrant issued after the commencement of this item.

Schedule 5—Australian Security Intelligence Organisation

Australian Security Intelligence Organisation Act 1979

1 After subsection 16(1)

Insert:

(1A) The Director-General may, by writing, delegate any or all of the Director-General's functions or powers under section 21A to a senior position-holder.

2 At the end of Division 1 of Part III

Add:

21A Voluntary assistance provided to the Organisation

Assistance provided in accordance with a request by the Director-General

(1) If:

(a) the Director-General requests a person or body to engage in conduct; and

(b) the Director-General is satisfied, on reasonable grounds, that the conduct is likely to assist the Organisation in the performance of its functions; and

(c) the person engages in the conduct in accordance with the request; and

(d) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and

(e) the conduct does not result in significant loss of, or serious damage to, property;

the person or body is not subject to any civil liability for, or in relation to, the conduct.

(2) A request under paragraph (1)(a) may be made:

(a) orally; or
(b) in writing.

(3) If a request under paragraph (1)(a) is made orally, the Director-General must:
(a) make a written record of the request; and
(b) do so within 48 hours after the request was made.

(4) The Director-General may enter into a contract, agreement or arrangement with a person or body in relation to conduct engaged in by the person or body in accordance with a request under paragraph (1)(a).

Unsolicited disclosure of information etc.

(5) If:
(a) a person or body engages in conduct that consists of, or is connected with:
(i) giving information to the Organisation; or
(ii) giving or producing a document to the Organisation; or
(iii) making one or more copies of a document and giving those copies to the Organisation; and
(b) the person reasonably believes that the conduct is likely to assist the Organisation in the performance of its functions; and
(c) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and
(d) the conduct does not result in significant loss of, or serious damage to, property; and
(e) subsection (1) does not apply to the conduct;
the person or body is not subject to any civil liability for, or in relation to, the conduct.

Copies of, or extracts from, documents

(6) The Organisation may make and retain copies of, or take and retain extracts from, a document given or produced to the Organisation:
(a) in accordance with a request under paragraph (1)(a); or

(b) under paragraph (5)(a).

Subsections (1) and (5) have effect despite other laws

(7) Subsections (1) and (5) have effect despite anything in a law of the Commonwealth, a State or a Territory (whether passed or made before or after the commencement of this section) unless the law expressly provides otherwise.

Certificate

(8) The Director-General may give a certificate in writing certifying one or more facts relevant to the question of whether the Director-General was satisfied, on reasonable grounds, that particular conduct was likely to assist the Organisation in the performance of its functions.

(9) In any proceedings that involve determining whether subsection (1) or (5) applies to particular conduct, a certificate given under subsection (8) is prima facie evidence of the facts certified.

Compensation for acquisition of property

(10) If the operation of this section would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from a person otherwise than on just terms (within the meaning of that paragraph), the Commonwealth is liable to pay a reasonable amount of compensation to the person.

(11) If the Commonwealth and the person do not agree on the amount of the compensation, the person may institute proceedings in the Federal Court of Australia for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

3 At the end of Division 2 of Part III

Add:

Subdivision J—Assistance relating to access to data

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

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

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

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

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

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

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

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

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

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

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

(ix) has been seized under section 34ZB;

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

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

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

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

(iii) data held in a computer or data storage device removed from premises under a warrant under section 25, 26 or 27A; or

(iv) data held in a computer or data storage device removed from premises under section 27D.

(2) The Attorney-General may make the order if:

(a) in a case where the computer or data storage device:

(i) is the subject of a warrant under section 27A; or

(ii) is on premises in relation to which a warrant under section 27A is in force; or

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

(iv) has been removed from premises under a warrant under section 27A;

the Attorney-General is satisfied, on reasonable grounds, that:

(v) access by the Organisation to data held in, or accessible from, the computer or data storage device will be for the purpose of obtaining foreign intelligence relating to a matter specified in the relevant notice under subsection 27A(1); and

(vi) on the basis of advice received from the Defence Minister or the Foreign Affairs Minister, the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being; and

(b) in a case where paragraph (a) does not apply—the Attorney-General is satisfied that there are reasonable grounds for suspecting that access by the Organisation to data held in, or accessible from, the computer or data storage device will substantially assist the collection of intelligence in accordance with this Act in respect of a matter that is important in relation to security; and

(c) the Attorney-General is satisfied, on reasonable grounds, that the specified person is:
  (i) reasonably suspected of being involved in activities that are prejudicial to security; or
  (ii) the owner or lessee of the computer or device; or
  (iii) an employee of the owner or lessee of the computer or device; or
  (iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or
  (v) a person who uses or has used the computer or device; or
  (vi) a person who is or was a system administrator for the system including the computer or device; and
(d) the Attorney-General is satisfied, on reasonable grounds, that the specified person has relevant knowledge of:
  (i) the computer or device or a computer network of which the computer or device forms or formed a part; or
  (ii) measures applied to protect data held in, or accessible from, the computer or device.

(3) If the computer or data storage device is not on premises in relation to which a warrant is in force, the order must:
(a) specify the period within which the person must provide the information or assistance; and
(b) specify the place at which the person must provide the information or assistance; and
(c) specify the conditions (if any) determined by the Attorney-General as the conditions to which the requirement on the person to provide the information or assistance is subject.

(4) A person commits an offence if:
(a) the person is subject to an order under this section; and
(b) the person is capable of complying with a requirement in the order; and
(c) the person omits to do an act; and
(d) the omission contravenes the requirement.

Penalty for contravention of this subsection: Imprisonment for 5 years or 300 penalty units, or both.