

**Cybercrime legislation – country profile**

**AUSTRALIA**

*This profile has been prepared within the framework of the Council of Europe’s capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.*

Comments may be sent to:

Economic Crime Division  
 Directorate General of Human Rights and Legal Affairs  
 Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506  
 Fax: +33-3-9021-5650  
 Email: [alexander.seger@coe.int](mailto:alexander.seger@coe.int)  
[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

<b>Country:</b>	<b>Australia</b>
Signature of Convention:	No
Ratification/accession:	No
<b>Provisions of the Convention</b>	<b>Corresponding provisions/solutions in national legislation</b> <i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i>
<b>Chapter I – Use of terms</b>	
<b>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</b> For the purposes of this Convention: a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;	<b>Art. 476.1 of Criminal Code Act 1995 (Act n°12 of 1995) of Australia</b>  <b>Definitions</b> (1) In this Part: <b>access to data held in a computer</b> means:

<p>b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service</p>	<p>(a) the display of the data by the computer or any other output of the data from the computer; or</p> <p>(b) the copying or moving of the data to any other place in the computer or to a data storage device; or</p> <p>(c) in the case of a program—the execution of the program.</p> <p><b>Commonwealth computer</b> means a computer owned, leased or operated by a Commonwealth entity.</p> <p><b>data</b> includes:</p> <p>(a) information in any form; or</p> <p>(b) any program (or part of a program).</p> <p><b>data held in a computer</b> includes:</p> <p>(a) data held in any removable data storage device for the time being held in a computer; or</p> <p>(b) data held in a data storage device on a computer network of which the computer forms a part.</p> <p><b>data storage device</b> means a thing (for example, a disk or file server) containing, or designed to contain, data for use by a computer.</p> <p><b>electronic communication</b> means a communication of information in any form by means of guided or unguided electromagnetic energy.</p> <p><b>unauthorised access, modification or impairment</b> has the meaning given in section 476.2.</p> <p>(2) In this Part, a reference to:</p> <p>(a) access to data held in a computer; or</p> <p>(b) modification of data held in a computer; or</p> <p>(c) the impairment of electronic communication to or from a computer; is limited to such access, modification or impairment caused, whether directly or indirectly, by the execution of a function of a computer.</p>
--	--

**Chapter II – Measures to be taken at the national level**  
**Section 1 – Substantive criminal law**

*Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems*

<p><b>Article 2 – Illegal access</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by</p>	<p><b>Art. 476.2 of Criminal Code Act 1995 (Act n°12 of 1995) of Australia</b>  <b>Meaning of unauthorised access, modification or impairment</b></p> <p>(1) In this Part:</p> <p>(a) access to data held in a computer; or</p>
---	---

infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

(b) modification of data held in a computer; or  
(c) the impairment of electronic communication to or from a computer; or  
(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means; by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

(2) Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

(3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification or impairment if the person's conduct substantially contributes to it.

(4) For the purposes of subsection (1), if:

- (a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and
- (b) the person does so under a warrant issued under the law of the Commonwealth, a State or a Territory; the person is entitled to cause that access, modification or impairment.

**Art. 477.1(1/i of Criminal Code Act 1995 (Act n°12 of 1995) of Australia)**

**Unauthorised access, modification or impairment with intent to commit a serious offence**

*Intention to commit a serious Commonwealth, State or Territory offence*

(1) A person is guilty of an offence if:

- (a) the person causes:
  - (i) any unauthorised access to data held in a computer; or

**Art. 478.1 of Criminal Code Act 1995 (Act n°12 of 1995) of Australia**

**Unauthorised access to, or modification of, restricted data**

(1) A person is guilty of an offence if:

- (a) the person causes any unauthorised access to, or modification of, restricted data; and

- (b) the person intends to cause the access or modification; and
- (c) the person knows that the access or modification is unauthorised; and
- (d) one or more of the following applies:

- (i) the restricted data is held in a Commonwealth computer;
- (ii) the restricted data is held on behalf of the Commonwealth;
- (iii) the access to, or modification of, the restricted data is caused by means of a telecommunications service.

*Penalty:* 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) In this section:

**restricted data** means data:

- (a) held in a computer; and
- (b) to which access is restricted by an access control system associated with a function of the computer.

**Part VIA, Section 76B of Crimes Act 1914 of Australia.**

1. A person who intentionally and without authority obtains access to:

- a. data stored in a Commonwealth computer; or
- b. data stored on behalf of the Commonwealth in a computer that is not Commonwealth computer;

is guilty of an offence.

***Penalty: Imprisonment for 6 months***

2. A person who:

- a. with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
- b. with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
  - i. the security, defence or international relations of Australia;
  - ii. the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or

	<p>Territory;</p> <p>iii.the enforcement of a law of the Commonwealth or of a State or Territory;</p> <p>iv.the protection of public safety;</p> <p>v.the personal affairs of any person;</p> <p>vi.trade secrets;</p> <p>vii.records of a financial institution; or</p> <p>viii.commercial Information the disclosure of which could cause advantage or disadvantage to any person</p> <p>is guilty of an offence</p> <p><b>Penalty: Imprisonment for 2 years</b></p> <p>3. A person who:</p> <p>a. has intentionally and without authority obtained access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;</p> <p>b. after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2) (b); and</p> <p>c. continues to examine that data;</p> <p>is guilty of an offence.</p> <p>Penalty for a contravention of this subsection: <b>Imprisonment for 2 years</b></p>
<p><b>Article 3 – Illegal interception</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Section 7 of TIA Act</b></p> <p>Telecommunications not to be intercepted</p> <p>(1) A person shall not:</p> <p>(a) intercept;</p> <p>(b) authorize, suffer or permit another person to intercept; or</p> <p>(c) do any act or thing that will enable him or her or another person to intercept; a communication passing over a telecommunications system.</p> <p>(2) Subsection (1) does not apply to or in relation to:</p> <p>(a) an act or thing done by an employee of a carrier in the course of his or her duties for or in connection with:</p>

- (i) the installation of any line, or the installation of any equipment, used or intended for use in connection with a telecommunications service; or
- (ii) the operation or maintenance of a telecommunications system; or
- (iii) the identifying or tracing of any person who has contravened, or is suspected of having contravened or being likely to contravene, a provision of Part 10.6 of the *Criminal Code*;

where it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively; or

(aa) the interception of a communication by another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line, where it is reasonably necessary for the person to intercept the communication in order to perform those duties effectively; or

(aaa) the interception of a communication by a person if:

(i) the person is authorised, in writing, by a responsible person for a computer network to engage in network protection duties in relation to the network; and

(ii) it is reasonably necessary for the person to intercept the communication in order to perform those duties effectively; or

(ab) the interception of a communication by a person lawfully engaged in duties relating to the installation, connection or maintenance of equipment used, or to be used, for the interception of communications under warrants; or

(ac) the interception of a communication where the interception results from, or is incidental to, action taken by an officer of the Organisation, in the lawful performance of his or her duties, for the purpose of:

(i) discovering whether a listening device is being used at, or in relation to, a particular place; or

(ii) determining the location of a listening device; or

(b) the interception of a communication under a warrant; or

(c) the interception of a communication pursuant to a request made, or purporting to be made, under subsection 30(1) or (2); or

(d) the interception of a communication under an authorisation under section 31A.

(2A) For the purposes of paragraphs (2)(a), (aa) and (aaa), in determining whether an act or thing done by a person was reasonably necessary in order for

the person to perform his or her duties effectively, a court is to have regard to such matters (if any) as are specified in, or ascertained in accordance with, the regulations.

(3) Paragraph (2)(aaa) does not apply to a voice communication in the form of speech (including a communication that involves a recorded or synthetic voice).

(4) Subsection (1) does not apply to, or in relation to, an act done by an officer of an agency in relation to a communication if the following conditions are satisfied:

- (a) the officer or another officer of the agency is a party to the communication; and
- (b) there are reasonable grounds for suspecting that another party to the communication has:
  - (i) done an act that has resulted, or may result, in loss of life or the infliction of serious personal injury; or
  - (ii) threatened to kill or seriously injure another person or to cause serious damage to property; or
  - (iii) threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety; and
- (c) because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a Part 2-5 warrant to be made.

(5) Subsection (1) does not apply to, or in relation to, an act done by an officer of an agency in relation to a communication if the following conditions are satisfied:

- (a) the person to whom the communication is directed has consented to the doing of the act; and
- (b) there are reasonable grounds for believing that that person is likely to receive a communication from a person who has:
  - (i) done an act that has resulted, or may result, in loss of life or the infliction of serious personal injury; or
  - (ii) threatened to kill or seriously injure another person or to cause serious damage to property; or
  - (iii) threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or

	<p>safety; and</p> <p>(c) because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a Part 2-5 warrant to be made.</p> <p>(6) As soon as practicable after the doing of an act in relation to a communication under the provisions of subsection (4) or (5), an officer of the agency which is concerned with the communication shall cause an application for a Part 2-5 warrant to be made in relation to the matter.</p> <p>(6A) Subsection (6) does not apply if action has been taken under subsection (4) or (5) to intercept a communication, or cause it to be intercepted, and the action has ceased before it is practicable for an application for a Part 2-5 warrant to be made.</p> <p>(7) Where after considering an application made in relation to a matter arising under subsections (4) or (5) and (6) a Judge or nominated AAT member does not issue a warrant in relation to the application, the chief officer of the agency concerned shall ensure that no further action is taken by the agency to intercept the communication or to cause it to be intercepted.</p> <p>(8) Subsections (4), (5), (6) and (7) only apply where the agency concerned is:</p> <p>(a) the Australian Federal Police; or</p> <p>(b) the Police Force of a State.</p> <p>(9) The doing of an act mentioned in subparagraph (4)(b)(ii) or (iii) or (5)(b)(ii) or (iii) in a particular case is taken to constitute a serious offence, even if it would not constitute a serious offence apart from this subsection.</p> <p>Note: See subsection (6). A Part 2-5 warrant can only be issued for the purposes of an investigation relating to the commission of a serious offence.</p> <p>(10) Subsection (9) has effect only to the extent necessary:</p> <p>(a) to enable an application to be made for the purposes of subsection (6); and</p> <p>(b) to enable a decision to be made on such an application and, if a Judge so decides, a Part 2-5 warrant to be issued; and</p> <p>(c) to enable this Act to operate in relation to a Part 2-5 warrant issued on such an application.</p>
<b>Article 4 – Data interference</b>	<b>Art. 477.1 (1/ii) of Criminal Code Act 1995 (Act n°12 of 1995) of</b>



1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.  
2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

**Australia - Unauthorised access, modification or impairment with intent to commit a serious offence**

*Intention to commit a serious Commonwealth, State or Territory offence*

- (1) A person is guilty of an offence if:
- (a) the person causes:
  - (ii) any unauthorised modification of data held in a computer; or

**Art. 477.2 of Criminal Code Act 1995 (Act n°12 of 1995) of Australia  
Unauthorised modification of data to cause impairment**

- (1) A person is guilty of an offence if:
- (a) the person causes any unauthorised modification of data held in a computer; and
  - (b) the person knows the modification is unauthorised; and
  - (c) the person is reckless as to whether the modification impairs or will impair:
    - (i) access to that or any other data held in any computer; or
    - (ii) the reliability, security or operation, of any such data; and
  - (d) one or more of the following applies:
    - (i) the data that is modified is held in a Commonwealth computer;
    - (ii) the data that is modified is held on behalf of the Commonwealth in a computer;
    - (iii) the modification of the data is caused by means of a telecommunications service;
    - (iv) the modification of the data is caused by means of a Commonwealth computer;
    - (v) the modification of the data impairs access to, or the reliability, security or operation of, other data held in a Commonwealth computer;
    - (vi) the modification of the data impairs access to, or the reliability, security or operation of, other data held on behalf of the Commonwealth in a computer;
    - (vii) the modification of the data impairs access to, or the reliability, security or operation of, other data by means of a telecommunications service.

*Penalty:* 10 years imprisonment.

- (2) Absolute liability applies to paragraph (1)(d).

(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:

- (a) access to data held in a computer; or
- (b) the reliability, security or operation, of any such data.

(4) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.3 (unauthorized impairment of electronic communication).

**Art. 478.1 of Criminal Code Act 1995 (Act n°12 of 1995) of Australia.  
Unauthorised access to, or modification of, restricted data**

(1) A person is guilty of an offence if:

- (a) the person causes any unauthorised access to, or modification of, restricted data; and
- (b) the person intends to cause the access or modification; and
- (c) the person knows that the access or modification is unauthorised; and
- (d) one or more of the following applies:
  - (i) the restricted data is held in a Commonwealth computer;
  - (ii) the restricted data is held on behalf of the Commonwealth;
  - (iii) the access to, or modification of, the restricted data is caused by means of a telecommunications service.

*Penalty:* 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) In this section:

**restricted data** means data:

- (a) held in a computer; and
- (b) to which access is restricted by an access control system associated with a function of the computer.

**Part VIA, Section 76C (a,c) of Crimes Act 1914 of Australia.**

A person who intentionally and without authority or lawful excuse:

- a. destroys, erases or alters data stored in, or inserts data into a Commonwealth computer;
- c. destroys, erases, alters or adds data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

	<p>is guilty of an offence.</p> <p><b>Section 76D of Crimes Act 1914 of Australia</b></p> <p>1.A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority obtains access to data stored in a computer, is guilty of an offence.</p> <p><b>Section 76E(a) of Crimes Act 1914 of Australia</b></p> <p>A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority or lawful excuse:</p> <p>a.destroys, erases or alters data stored in, or inserts data into a computer;</p> <p>is guilty of an offence</p>
<p><b>Article 5 – System interference</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p><b>Part VIA, Section 76C(b) of Crimes Act 1914 of Australia</b></p> <p>A person who intentionally and without authority or lawful excuse:</p> <p>b.interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer;</p> <p>is guilty of an offence.</p> <p><b>Section 76E (b) of Crimes Act 1914 of Australia</b></p> <p>A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority or lawful excuse:</p> <p>b.destroys, erases or alters data stored in, or inserts data into a computer;</p> <p>is guilty of an offence.</p>
<p><b>Article 6 – Misuse of devices</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p>	<p><b>For Art. 6(1/a/ii)- Art. 478.3(1) of Criminal Code Act 1995 (Act n°12 of 1995) of Australia.</b></p> <p><b>Possession or control of data with intent to commit a computer offence</b></p> <p>(1) A person is guilty of an offence if:</p> <p>(a) the person has possession or control of data; and</p> <p>(b) the person has that possession or control with the intention that the data be used, by the person or another person, in:</p> <p>(i) committing an offence against Division 477; or</p>

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

(ii) facilitating the commission of such an offence.

**For Art. 6(1)- Art. 478.4(1-2) of Criminal Code Act 1995  
Producing, supplying or obtaining data with intent to commit  
a computer offence**

(1) A person is guilty of an offence if:

- (a) the person produces, supplies or obtains data; and
- (b) the person does so with the intention that the data be used, by the person or another person, in:
  - (i) committing an offence against Division 477; or
  - (ii) facilitating the commission of such an offence.

*Penalty:* 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

**Section 132 APD of the Copyright Act 1968**

**Manufacturing etc. a circumvention device for a technological protection measure**

(1) A person commits an offence if:

- (a) the person does any of the following acts with a device:
  - (i) manufactures it with the intention of providing it to another person;
  - (ii) imports it into Australia with the intention of providing it to another person;
  - (iii) distributes it to another person;
  - (iv) offers it to the public;
  - (v) provides it to another person;
  - (vi) communicates it to another person; and
- (b) the person does the act with the intention of obtaining a commercial advantage or profit; and
- (c) the device is a circumvention device for a technological protection measure.

*Penalty:* 550 penalty units or imprisonment for 5 years, or both.

*Defence*--no promotion, advertising etc.

(2) Subsection (1) does not apply to the person if:

- (a) the device is a circumvention device for the technological protection measure only because it was promoted, advertised or marketed as having the purpose of circumventing the technological protection measure; and
- (b) both of the following apply:
  - (i) the person did not do such promoting, advertising or marketing;
  - (ii) the person did not direct or request (expressly or impliedly) another person to do such promoting, advertising or marketing.

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

#### Defence--interoperability

(3) Subsection (1) does not apply to the person if:

- (a) the circumvention device will be used to circumvent the technological protection measure to enable the doing of an act; and
- (b) the act:
  - (i) relates to a copy of a computer program (the **original program** ) that is not an infringing copy and that was lawfully obtained; and
  - (ii) will not infringe the copyright in the original program; and
  - (iia) relates to elements of the original program that will not be readily available to the person doing the act when the circumvention occurs; and
  - (iii) will be done for the sole purpose of achieving interoperability of an independently created computer program with the original program or any other program.

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

#### Defence--encryption research

(4) Subsection (1) does not apply to the person if:

- (a) the technological protection measure is an access control technological protection measure; and
- (b) the circumvention device will be used to circumvent the access control technological protection measure to enable a person (the **researcher** ) to do an act; and
- (c) the act:
  - (i) relates to a copy of a work or other subject-matter that is not an infringing copy and that was lawfully obtained; and

(ii) will not infringe the copyright in the work or other subject-matter; and  
(iii) will be done for the sole purpose of identifying and analysing flaws and vulnerabilities of encryption technology; and  
(d) the researcher is:  
(i) engaged in a course of study at an educational institution in the field of encryption technology; or  
(ii) employed, trained or experienced in the field of encryption technology; and  
(e) the researcher:  
(i) has obtained permission from the owner or exclusive licensee of the copyright to do the act; or  
(ii) has made, or will make, a good faith effort to obtain such permission.  
In this subsection, **encryption technology** means the scrambling and descrambling of information using mathematical formulas or algorithms.  
Note: A defendant bears an evidential burden in relation to the matter in subsection (4) (see subsection 13.3(3) of the *Criminal Code* ).  
Defence--computer security testing

(5) Subsection (1) does not apply to the person if:  
(a) the technological protection measure is an access control technological protection measure; and  
(b) the circumvention device will be used to circumvent the access control technological protection measure to enable the doing of an act; and  
(c) the act:  
(i) relates to a copy of a computer program that is not an infringing copy; and  
(ii) will not infringe the copyright in the computer program; and  
(iii) will be done for the sole purpose of testing, investigating or correcting the security of a computer, computer system or computer network; and  
(iv) will be done with the permission of the owner of the computer, computer system or computer network.  
Note: A defendant bears an evidential burden in relation to the matter in subsection (5) (see subsection 13.3(3) of the *Criminal Code* ).  
Defence--law enforcement and national security

(6) Subsection (1) does not apply in relation to anything lawfully done for the purposes of:

- (a) law enforcement; or
  - (b) national security; or
  - (c) performing a statutory function, power or duty;
- by or on behalf of the Commonwealth, a State or a Territory, or an authority of one of those bodies.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code* ).

Defence--libraries etc.

(7) Subsection (1) does not apply in respect of anything lawfully done by the following bodies in performing their functions:

(a) a library (other than a library that is conducted for the profit, direct or indirect, of an individual or individuals);

(b) a body mentioned in:

- (i) paragraph (a) of the definition of **archives** in subsection 10(1); or
- (ii) subsection 10(4);

(c) an educational institution;

(d) a public non-commercial broadcaster (including a body that provides a national broadcasting service, within the meaning of the *Broadcasting Services Act 1992*, and a body that holds a community broadcasting licence within the meaning of that Act).

Note 1: A library that is owned by a person conducting a business for profit might not itself be conducted for profit (see section 18).

Note 2: A defendant bears an evidential burden in relation to the matter in subsection (7) (see subsection 13.3(3) of the *Criminal Code* ).

(8) This section does not apply in respect of anything lawfully done by a person in connection with a work or other subject-matter if:

a) the person has custody of the work or other subject-matter under an arrangement referred to in section 64 of the *Archives Act 1983* ; and

(b) under subsection (7), it would be lawful for the National Archives of Australia to do that thing.

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

*Title 2 – Computer-related offences*

**Article 7 – Computer-related forgery**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

**Part 7.7—Forgery and related offences of the Criminal Code****Division 143—Preliminary****143.1 Definitions**

(1) In this Part:

*document* includes:

- (a) any paper or other material on which there is writing; or
- (b) any paper or other material on which there are marks, figures, symbols or perforations that are:
  - i) capable of being given a meaning by persons qualified to interpret them; or
  - or
  - (ii) capable of being responded to by a computer, a machine or an electronic device; or
- (c) any article or material (for example, a disk or a tape) from which information is capable of being reproduced with or without the aid of any other article or device.

*false Commonwealth document* has the meaning given by section 143.3.

*false document* has the meaning given by section 143.2.

*information* means information, whether in the form of data, text, sounds, images or in any other form.

(2) The following are examples of things covered by the definition of *document* in subsection (1):

- (a) a credit card;
- (b) a debit card;
- (c) a card by means of which property can be obtained.

**143.2 False documents**

(1) For the purposes of this Part, a document is a *false document* if, and only if:

- (a) the document, or any part of the document:
  - (i) purports to have been made in the form in which it is made by a person who did not make it in that form; or
  - (ii) purports to have been made in the form in which it is made on the authority of a person who did not authorise its making in that form; or



- (b) the document, or any part of the document:
  - (i) purports to have been made in the terms in which it is made by a person who did not make it in those terms; or
  - (ii) purports to have been made in the terms in which it is made on the authority of a person who did not authorise its making in those terms; or
- (c) the document, or any part of the document:
  - (i) purports to have been altered in any respect by a person who did not alter it in that respect; or
  - (ii) purports to have been altered in any respect on the authority of a person who did not authorise its alteration in that respect; or
- (d) the document, or any part of the document:
  - (i) purports to have been made or altered by a person who did not exist; or
  - (ii) purports to have been made or altered on the authority of a person who did not exist; or
- (e) the document, or any part of the document, purports to have been made or altered on a date on which, at a time at which, at a place at which, or otherwise in circumstances in which, it was not made or altered.

(2) For the purposes of this Part, a person is taken to *make* a false document if the person alters a document so as to make it a false document (whether or not it was already a false document before the alteration).

(3) This section has effect as if a document that purports to be a true copy of another document were the original document.

### **143.3 False Commonwealth documents**

(1) For the purposes of this Part, a document is a *false Commonwealth document* if, and only if:

- (a) the document, or any part of the document:
  - (i) purports to have been made in the form in which it is made by a Commonwealth entity, or a Commonwealth public official, who did not make it in that form; or
  - (ii) purports to have been made in the form in which it is made on the authority of a Commonwealth entity, or a Commonwealth public official, who did not authorise its making in that form; or
- (b) the document, or any part of the document:

- (i) purports to have been made in the terms in which it is made by a Commonwealth entity, or a Commonwealth public official, who did not make it in those terms; or
  - (ii) purports to have been made in the terms in which it is made on the authority of a Commonwealth entity, or a Commonwealth public official, who did not authorise its making in those terms; or
- (c) the document, or any part of the document:
- (i) purports to have been altered in any respect by a Commonwealth entity, or a Commonwealth public official, who did not alter it in that respect; or
  - (ii) purports to have been altered in any respect on the authority of a Commonwealth entity, or a Commonwealth public official, who did not authorise its alteration in that respect; or
- (d) the document, or any part of the document:
- (i) purports to have been made or altered by a Commonwealth entity, or a Commonwealth public official, who did not exist; or
  - (ii) purports to have been made or altered on the authority of a Commonwealth entity, or a Commonwealth public official, who did not exist; or
- (e) the document, or any part of the document, purports to have been made or altered by a Commonwealth entity, or a Commonwealth public official, on a date on which, at a time at which, at a place at which, or otherwise in circumstances in which, it was not made or altered.
- (2) For the purposes of this Part, a person is taken to *make* a false Commonwealth document if the person alters a document so as to make it a false Commonwealth document (whether or not it was already a false Commonwealth document before the alteration).
- (3) This section has effect as if a document that purports to be a true copy of another document were the original document.
- (4) A reference in this section to a *Commonwealth public official* is a reference to a person in the person's capacity as a Commonwealth public official.
- 143.4 Inducing acceptance of false documents**  
If it is necessary for the purposes of this Part to prove an intent to induce a

person in the person's capacity as a public official to accept a false document as genuine, it is not necessary to prove that the defendant intended so to induce a particular person in the person's capacity as a public official.

**Division 144—Forgery**

(1) A person is guilty of an offence if:

- (a) the person makes a false document with the intention that the person or another will use it:
  - (i) to dishonestly induce a third person in the third person's capacity as a public official to accept it as genuine; and
  - (ii) if it is so accepted, to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function;
- (b) the capacity is a capacity as a Commonwealth public official.

Penalty: Imprisonment for 10 years.

(2) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the capacity was a capacity as a Commonwealth public official.

(3) A person is guilty of an offence if:

- (a) the person makes a false document with the intention that the person or another will use it:
  - (i) to dishonestly cause a computer, a machine or an electronic device to respond to the document as if the document were genuine; and
  - (ii) if it is so responded to, to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function;
- (b) the response is in connection with the operations of a Commonwealth entity.

Penalty: Imprisonment for 10 years.

(4) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the response was in connection with the operations of a Commonwealth entity.

(5) A person is guilty of an offence if:

- (a) the person makes a false document with the intention that the person or another will use it:
- (i) to dishonestly induce a third person to accept it as genuine; and
  - (ii) if it is so accepted, to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function; and
- (b) the false document is a false Commonwealth document.

Penalty: Imprisonment for 10 years.

(6) In a prosecution for an offence against subsection (5), it is not necessary to prove that the defendant knew that the false document was a false Commonwealth document.

(7) A person is guilty of an offence if:

- (a) the person makes a false document with the intention that the person or another will use it:
- (i) to dishonestly cause a computer, a machine or an electronic device to respond to the document as if the document were genuine; and
  - (ii) if it is so responded to, to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function; and
- (b) the false document is a false Commonwealth document.

Penalty: Imprisonment for 10 years.

(8) In a prosecution for an offence against subsection (7), it is not necessary to prove that the defendant knew that the false document was a false Commonwealth document.

(9) Section 15.4 (extended geographical jurisdiction—category D) applies to an offence against subsection (1), (3), (5) or (7).

#### **Division 145—Offences relating to forgery**

##### **145.1 Using forged document**

(1) A person is guilty of an offence if:

- (a) the person knows that a document is a false document and uses it with the

	<p>intention of:</p> <ul style="list-style-type: none"><li>(i) dishonestly inducing another person in the other person's capacity as a public official to accept it as genuine; and</li><li>(ii) if it is so accepted, dishonestly obtaining a gain, dishonestly causing a loss, or dishonestly influencing the exercise of a public duty or function; and</li></ul> <p>(b) the capacity is a capacity as a Commonwealth public official.</p> <p>Penalty: Imprisonment for 10 years.</p> <p>(2) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the capacity was a capacity as a Commonwealth public official.</p> <p>(3) A person is guilty of an offence if:</p> <ul style="list-style-type: none"><li>(a) the person knows that a document is a false document and uses it with the intention of:<ul style="list-style-type: none"><li>(i) dishonestly causing a computer, a machine or an electronic device to respond to the document as if the document were genuine; and</li><li>(ii) if it is so responded to, dishonestly obtaining a gain, dishonestly causing a loss, or dishonestly influencing the exercise of a public duty or function; and</li></ul></li><li>(b) the response is in connection with the operations of a Commonwealth entity.</li></ul> <p>Penalty: Imprisonment for 10 years.</p> <p>(4) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the response was in connection with the operations of a Commonwealth entity.</p> <p>(5) A person is guilty of an offence if:</p> <ul style="list-style-type: none"><li>(a) the person knows that a document is a false document and uses it with the intention of:<ul style="list-style-type: none"><li>(i) dishonestly inducing another person to accept it as genuine; and</li><li>(ii) if it is so accepted, dishonestly obtaining a gain, dishonestly causing a loss, or dishonestly influencing the exercise of a public duty or function; and</li></ul></li><li>(b) the false document is a false Commonwealth document.</li></ul> <p>Penalty: Imprisonment for 10 years.</p>
--	--

(6) In a prosecution for an offence against subsection (5), it is not necessary to prove that the defendant knew that the false document was a false Commonwealth document.

(7) A person is guilty of an offence if:

(a) the person knows that a document is a false document and uses it with the intention of:

(i) dishonestly causing a computer, a machine or an electronic device to respond to the document as if the document were genuine; and

(ii) if it is so responded to, dishonestly obtaining a gain, dishonestly causing a loss, or dishonestly influencing the exercise of a public duty or function; and

(b) the false document is a false Commonwealth document.

Penalty: Imprisonment for 10 years.

(8) In a prosecution for an offence against subsection (7), it is not necessary to prove that the defendant knew that the false document was a false Commonwealth document.

#### **145.2 Possession of forged document**

(1) A person is guilty of an offence if:

(a) the person knows that a document is a false document and has it in his or her possession with the intention that the person or another will use it:

(i) to dishonestly induce a third person in the third person's capacity as a public official to accept it as genuine; and

(ii) if it is so accepted, to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function; and

(b) the capacity is a capacity as a Commonwealth public official.

Penalty: Imprisonment for 10 years.

(2) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the capacity was a capacity as a Commonwealth public official.

	<p>(3) A person is guilty of an offence if:</p> <p>(a) the person knows that a document is a false document and has it in his or her possession with the intention that the person or another will use it:</p> <ul style="list-style-type: none"><li>(i) to dishonestly cause a computer, a machine or an electronic device to respond to the document as if the document were genuine; and</li><li>gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function; and</li></ul> <p>(b) the response is in connection with the operations of a Commonwealth entity. Penalty: Imprisonment for 10 years.</p> <p>(4) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the response was in connection with the operations of a Commonwealth entity.</p> <p>(5) A person is guilty of an offence if:</p> <p>(a) the person knows that a document is a false document and has it in his or her possession with the intention that the person or another will use it:</p> <ul style="list-style-type: none"><li>(i) to dishonestly induce a third person to accept it as genuine; and</li><li>(ii) if it is so accepted, to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function; and</li></ul> <p>(b) the false document is a false Commonwealth document. Penalty: Imprisonment for 10 years.</p> <p>(6) In a prosecution for an offence against subsection (5), it is not necessary to prove that the defendant knew that the false document was a false Commonwealth document.</p> <p>(7) A person is guilty of an offence if:</p> <p>(a) the person knows that a document is a false document and has it in his or her possession with the intention that the person or another will use it:</p> <ul style="list-style-type: none"><li>(i) to dishonestly cause a computer, a machine or an electronic device to respond to the document as if the document were genuine; and</li><li>(ii) if it is so responded to, to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function; and</li></ul> <p>(b) the false document is a false Commonwealth document.</p>
--	--

Penalty: Imprisonment for 10 years.

(8) In a prosecution for an offence against subsection (7), it is not necessary to prove that the defendant knew that the false document was a false Commonwealth document.

**145.3 Possession, making or adaptation of devices etc. for making forgeries**

(1) A person is guilty of an offence if:

- (a) the person knows that a device, material or other thing is designed or adapted for the making of a false document (whether or not the device, material or thing is designed or adapted for another purpose); and
- (b) the person has the device, material or thing in his or her possession with the intention that the person or another person will use it to commit an offence against section 144.1.

Penalty: Imprisonment for 10 years.

(2) A person is guilty of an offence if:

- (a) the person makes or adapts a device, material or other thing; and
- (b) the person knows that the device, material or other thing is designed or adapted for the making of a false document (whether or not the device, material or thing is designed or adapted for another purpose); and
- (c) the person makes or adapts the device, material or thing with the intention that the person or another person will use it to commit an offence against section 144.1.

Penalty: Imprisonment for 10 years.

(3) A person is guilty of an offence if:

- (a) the person knows that a device, material or other thing is designed or adapted for the making of a false Commonwealth document (whether or not the device, material or thing is designed or adapted for another purpose); and
- (b) the person has the device, material or thing in his or her possession; and
- (c) the person does not have a reasonable excuse for having the device,



material or thing in his or her possession.

Penalty: Imprisonment for 2 years.

Note: A defendant bears an evidential burden in relation to the matter in

(4) A person is guilty of an offence if:

- (a) the person makes or adapts a device, material or other thing; and
- (b) the person knows that the device, material or other thing is designed or adapted for the making of a false Commonwealth document (whether or not the device, material or thing is designed or adapted for another purpose).

Penalty: Imprisonment for 2 years.

Note: See also section 10.5 (lawful authority).

**145.4 Falsification of documents etc.**

(1) A person is guilty of an offence if:

- (a) the person dishonestly damages, destroys, alters, conceals or falsifies a document; and
- (b) the document is:
  - (i) kept, retained or issued for the purposes of a law of the Commonwealth; or
  - (ii) made by a Commonwealth entity or a person in the capacity of a Commonwealth public official; or
  - (iii) held by a Commonwealth entity or a person in the capacity of a Commonwealth public official; and
- (c) the first-mentioned person does so with the intention of:
  - (i) obtaining a gain; or
  - (ii) causing a loss.

Penalty: Imprisonment for 7 years.

(1A) Absolute liability applies to the paragraph (1)(b) element of the offence.

(2) A person is guilty of an offence if:

- (a) the person dishonestly damages, destroys, alters, conceals or falsifies a document; and
- (b) the person does so with the intention of:

- (i) obtaining a gain from another person; or
- (ii) causing a loss to another person; and
- (c) the other person is a Commonwealth entity.

Penalty: Imprisonment for 7 years.

(3) In a prosecution for an offence against subsection (2), it is not necessary to prove that the defendant knew that the other person was a Commonwealth entity.

#### **145.5 Giving information derived from false or misleading documents**

(1) A person is guilty of an offence if:

- (a) the person dishonestly gives information to another person; and
- (b) the information was derived, directly or indirectly, from a document that, to the knowledge of the first-mentioned person, is false or misleading in a material particular; and
- (c) the document is:
  - (i) kept, retained or issued for the purposes of a law of the Commonwealth; or
  - (ii) made by a Commonwealth entity or a person in the capacity of a Commonwealth public official; or
  - (iii) held by a Commonwealth entity or a person in the capacity of a Commonwealth public official; and
- (d) the first-mentioned person does so with the intention of:
  - (i) obtaining a gain; or
  - (ii) causing a loss.

Penalty: Imprisonment for 7 years.

(1A) Absolute liability applies to the paragraph (1)(c) element of the offence.

(2) A person is guilty of an offence if:

- (a) the person dishonestly gives information to another person; and
- (b) the information was derived, directly or indirectly, from a document that, to

	<p>the knowledge of the first-mentioned person, is false or misleading in a material particular; and</p> <p>(c) the first-mentioned person does so with the intention of:</p> <ul style="list-style-type: none"> <li>(i) obtaining a gain from another person; or</li> <li>(ii) causing a loss to another person; and</li> </ul> <p>(d) the other person is a Commonwealth entity.</p> <p>Penalty: Imprisonment for 7 years.</p> <p>(3) In a prosecution for an offence against subsection (2), it is not necessary to prove that the defendant knew that the other person was a Commonwealth entity.</p> <p><b>145.6 Geographical jurisdiction</b> Section 15.4 (extended geographical jurisdiction—category D) applies to each offence against this Division.</p>
<p><b>Article 8 – Computer-related fraud</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <ul style="list-style-type: none"> <li>a any input, alteration, deletion or suppression of computer data;</li> <li>b any interference with the functioning of a computer system,</li> </ul> <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p><b>Part 7.3—Fraudulent conduct</b></p> <p><b>Division 133—Preliminary</b></p> <p><b>133.1 Definitions</b></p> <p>In this Part:</p> <p><b>account</b> means an account (including a loan account, a credit card account or a similar account) with a bank or other financial institution.</p> <p><b>deception</b> means an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes:</p> <ul style="list-style-type: none"> <li>(a) a deception as to the intentions of the person using the deception or any other person; and</li> <li>(b) conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.</li> </ul> <p><b>Division 134—Obtaining property or a financial advantage by deception</b></p> <p><b>134.1 Obtaining property by deception</b></p> <p>(1) A person is guilty of an offence if:</p>

- (a) the person, by a deception, dishonestly obtains property belonging to another with the intention of permanently depriving the other of the property; and
  - (b) the property belongs to a Commonwealth entity.
- Penalty: Imprisonment for 10 years.

(2) Absolute liability applies to the paragraph (1)(b) element of the offence.  
Obtaining property

(3) For the purposes of this section (and for the purposes of the application of section 132.1 to this section), a person (the **first person**) is taken to have **obtained** property if, and only if:

- (a) the first person obtains ownership, possession or control of it for himself or herself or for another person; or
- (b) the first person enables ownership, possession or control of it to be retained by himself or herself; or
- (c) the first person induces a third person to pass ownership, possession or control of it to another person; or
- (d) the first person induces a third person to enable another person to retain ownership, possession or control of it; or
- (e) subsection (9) or (10) applies.

(4) The definition of **obtaining** in section 130.1 does not apply for the purposes of this section (or for the purposes of the application of section 132.1 to this section).

(5) For the purposes of this section, a person's obtaining of property belonging to another may be dishonest even if the person or another person is willing to pay for the property.

Intention of permanently depriving a person of property

(6) For the purposes of this section, if:

- (a) a person obtains property belonging to another without meaning the other permanently to lose the thing itself; and
  - (b) the person's intention is to treat the thing as the person's own to dispose of regardless of the other's rights;
- the person has the intention of permanently depriving the other of it.

(7) For the purposes of subsection (6), a borrowing or lending of a thing amounts to treating the thing as the borrower's or lender's own to dispose of regardless of another's rights if, and only if, the borrowing or lending is for a period and in circumstances making it equivalent to an outright taking or disposal.

(8) For the purposes of subsection (6), if:

- (a) a person has possession or control (lawfully or not) of property belonging to another; and
- (b) the person parts with the property under a condition as to its return that the person may not be able to perform; and
- (c) the parting is done for purposes of the person's own and without the other's authority;

the parting is taken to amount to treating the property as the person's own to dispose of regardless of the other's rights.

Money transfers

(9) For the purposes of this section (and for the purposes of the application of section 132.1 to this section), if a person (the **first person**) causes an amount to be transferred from an account held by another person (the **second person**) to an account held by the first person:

- (a) the amount is taken to have been property that belonged to the second person; and
- (b) the first person is taken to have obtained the property for himself or herself with the intention of permanently depriving the second person of the property.

(10) For the purposes of this section (and for the purposes of the application of section 132.1 to this section), if a person (the **first person**) causes an amount to be transferred from an account held by another person (the **second person**) to an account held by a third person:

- (a) the amount is taken to have been property that belonged to the second person; and
- (b) the first person is taken to have obtained the property for the third person with the intention of permanently depriving the second person of the property.

(11) For the purposes of this section (and for the purposes of the application of section 132.1 to this section), if:

- (a) a credit is made to an account (the **credited account**); and
- (b) a debit is made to another account (the **debited account**); and
- (c) either:

- (i) the credit results from the debit; or
- (ii) the debit results from the credit;

the amount of the credit is taken to be transferred from the debited account to the credited account.

(12) For the purposes of this section (and for the purposes of the application of section 132.1 to this section), a person is taken to cause an amount to be transferred from an account if the person induces another person to transfer the amount from the account (whether or not the other person is the holder of the account).

General deficiency

(13) A person may be convicted of an offence against this section involving all or any part of a general deficiency in money even though the deficiency is made up of any number of particular sums of money that were obtained over a period of time.

(14) A person may be convicted of an offence against this section involving all or any part of a general deficiency in property other than money even though the deficiency is made up of any number of particular items of property that were obtained over a period of time.

Alternative verdicts

(15) If, in a prosecution for an offence of theft, the trier of fact is not satisfied that the defendant is guilty of the offence, but is satisfied beyond reasonable doubt that the defendant is guilty of an offence against this section, the trier of fact may find the defendant not guilty of the offence of theft but guilty of the offence against this section, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

(16) If, in a prosecution for an offence against this section, the trier of fact is not satisfied that the defendant is guilty of the offence, but is satisfied beyond

reasonable doubt that the defendant is guilty of an offence of theft, the trier of fact may find the defendant not guilty of the offence against this section but guilty of the offence of theft, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

#### **134.2 Obtaining a financial advantage by deception**

(1) A person is guilty of an offence if:

- (a) the person, by a deception, dishonestly obtains a financial advantage from another person; and
- (b) the other person is a Commonwealth entity.

Penalty: Imprisonment for 10 years.

(2) Absolute liability applies to the paragraph (1)(b) element of the offence.

#### **134.3 Geographical jurisdiction**

Section 15.4 (extended geographical jurisdiction—category D) applies to each offence against this Division.

### **Division 135—Other offences involving fraudulent conduct**

#### **135.1 General dishonesty**

##### **135.2**

Obtaining a gain

(1) A person is guilty of an offence if:

- (a) the person does anything with the intention of dishonestly obtaining a gain from another person; and
- (b) the other person is a Commonwealth entity.

Penalty: Imprisonment for 5 years.

(2) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the other person was a Commonwealth entity.

Causing a loss

(3) A person is guilty of an offence if:

- (a) the person does anything with the intention of dishonestly causing a loss to another person; and

	<p>(b) the other person is a Commonwealth entity. Penalty: Imprisonment for 5 years.</p> <p>(4) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the other person was a Commonwealth entity.</p> <p>(5) A person is guilty of an offence if:</p> <ul style="list-style-type: none"> <li>(a) the person dishonestly causes a loss, or dishonestly causes a risk of loss, to another person; and</li> <li>(b) the first-mentioned person knows or believes that the loss will occur or that there is a substantial risk of the loss occurring; and</li> <li>(c) the other person is a Commonwealth entity.</li> </ul> <p>Penalty: Imprisonment for 5 years.</p> <p>(6) Absolute liability applies to the paragraph (5)(c) element of the offence. Influencing a Commonwealth public official</p> <p>(7) A person is guilty of an offence if:</p> <ul style="list-style-type: none"> <li>(a) the person does anything with the intention of dishonestly influencing a public official in the exercise of the official's duties as a public official; and</li> <li>(b) the public official is a Commonwealth public official; and</li> <li>(c) the duties are duties as a Commonwealth public official.</li> </ul> <p>Penalty: Imprisonment for 5 years.</p> <p>(8) In a prosecution for an offence against subsection (7), it is not necessary to prove that the defendant knew:</p> <ul style="list-style-type: none"> <li>(a) that the official was a Commonwealth public official; or</li> <li>(b) that the duties were duties as a Commonwealth public official.</li> </ul> <p><b>135.2 Obtaining financial advantage</b></p> <p>(1) A person is guilty of an offence if:</p> <ul style="list-style-type: none"> <li>(a) the person engages in conduct; and</li> <li>(aa) as a result of that conduct, the person obtains a financial advantage for himself or herself from another person; and</li> <li>(ab) the person knows or believes that he or she is not eligible to receive that financial advantage; and</li> </ul>
--	---



(b) the other person is a Commonwealth entity.

Penalty: Imprisonment for 12 months.

(1A) Absolute liability applies to the paragraph (1)(b) element of the offence.

(2) A person is guilty of an offence if:

(a) the person engages in conduct; and

(aa) as a result of that conduct, the person obtains a financial advantage for another person from a third person; and

(ab) the person knows or believes that the other person is not eligible to receive that financial advantage; and

(b) the third person is a Commonwealth entity.

Penalty: Imprisonment for 12 months.

(2A) Absolute liability applies to the paragraph (2)(b) element of the offence.

(3) For the purposes of subsection (2), a person is taken to have obtained a financial advantage for another person from a Commonwealth entity if the first-mentioned person induces the Commonwealth entity to do something that results in the other person obtaining the financial advantage.

(4) The definition of **obtaining** in section 130.1 does not apply to this section.

### **135.3 Conspiracy to defraud**

Obtaining a gain

(1) A person is guilty of an offence if:

(a) the person conspires with another person with the intention of dishonestly obtaining a gain from a third person; and

(b) the third person is a Commonwealth entity.

Penalty: Imprisonment for 10 years.

(2) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the third person was a Commonwealth entity.

Causing a loss

(3) A person is guilty of an offence if:

- (a) the person conspires with another person with the intention of dishonestly causing a loss to a third person; and
- (b) the third person is a Commonwealth entity.

Penalty: Imprisonment for 10 years.

(4) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the third person was a Commonwealth entity.

(5) A person is guilty of an offence if:

- (a) the person conspires with another person to dishonestly cause a loss, or to dishonestly cause a risk of loss, to a third person; and
- (b) the first-mentioned person knows or believes that the loss will occur or that there is a substantial risk of the loss occurring; and
- (c) the third person is a Commonwealth entity.

Penalty: Imprisonment for 10 years.

(6) In a prosecution for an offence against subsection (5), it is not necessary to prove that the defendant knew that the third person was a Commonwealth entity.

(7) A person is guilty of an offence if:

- (a) the person conspires with another person with the intention of dishonestly influencing a public official in the exercise of the official's duties as a public official; and
- (b) the public official is a Commonwealth public official; and
- (c) the duties are duties as a Commonwealth public official.

Penalty: Imprisonment for 10 years.

(8) In a prosecution for an offence against subsection (7), it is not necessary to prove that the defendant knew:

- (a) that the official was a Commonwealth public official; or
- (b) that the duties were duties as a Commonwealth public official.

General provisions

(9) For a person to be guilty of an offence against this section:

- (a) the person must have entered into an agreement with one or more other persons; and
- (b) the person and at least one other party to the agreement must have intended to do the thing pursuant to the agreement; and
- (c) the person or at least one other party to the agreement must have committed an overt act pursuant to the agreement.

(10) A person may be found guilty of an offence against this section even if:

- (a) obtaining the gain, causing the loss, causing the risk of loss, or influencing the Commonwealth public official, as the case may be, is impossible; or
- (b) the only other party to the agreement is a body corporate; or
- (c) each other party to the agreement is a person who is not criminally responsible; or
- (d) subject to subsection (11), all other parties to the agreement have been acquitted of the offence.

(11) A person cannot be found guilty of an offence against this section if:

- (a) all other parties to the agreement have been acquitted of such an offence; and
- (b) a finding of guilt would be inconsistent with their acquittal.

(12) A person cannot be found guilty of an offence against this section if, before the commission of an overt act pursuant to the agreement, the person:

- (a) withdrew from the agreement; and
- (b) took all reasonable steps to prevent the doing of the thing.

(13) A court may dismiss a charge of an offence against this section if the court thinks that the interests of justice require the court to do so.

(14) Proceedings for an offence against this section must not be commenced without the consent of the Director of Public Prosecutions. However, before the necessary consent has been given, a person may be:

- (a) arrested for an offence against this section; or
- (b) charged with an offence against this section; or
- (c) remanded in custody or released on bail in connection with an offence against this section.

	<p><b>135.5 Geographical jurisdiction</b> Section 15.4 (extended geographical jurisdiction—category D) applies to each offence against this Division.</p>
<p><i>Title 3 – Content-related offences</i></p>	
<p><b>Article 9 – Offences related to child pornography</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <ul style="list-style-type: none"> <li>a producing child pornography for the purpose of its distribution through a computer system;</li> <li>b offering or making available child pornography through a computer system;</li> <li>c distributing or transmitting child pornography through a computer system;</li> <li>d procuring child pornography through a computer system for oneself or for another person;</li> <li>e possessing child pornography in a computer system or on a computer-data storage medium.</li> </ul> <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <ul style="list-style-type: none"> <li>a a minor engaged in sexually explicit conduct;</li> <li>b a person appearing to be a minor engaged in sexually explicit conduct;</li> <li>c realistic images representing a minor engaged in sexually explicit conduct</li> </ul> <p>3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.</p>	<p><b>For. Art. 9(1)-</b></p> <p><b>Sect. 474.19 of Criminal Code Act 1995 of Australia.</b> <b>Using a carriage service for child pornography material</b></p> <p>(1) A person is guilty of an offence if:</p> <ul style="list-style-type: none"> <li>(a) the person: <ul style="list-style-type: none"> <li>(i) uses a carriage service to access material; or</li> <li>(ii) uses a carriage service to cause material to be transmitted to the person; or</li> <li>(iii) uses a carriage service to transmit material; or</li> <li>(iv) uses a carriage service to make material available; or</li> <li>(v) uses a carriage service to publish or otherwise distribute material; and</li> </ul> </li> <li>(b) the material is child pornography material.</li> </ul> <p><i>Penalty:</i> Imprisonment for 10 years.</p> <p>(2) To avoid doubt, the following are the fault elements for the physical elements of an offence against subsection (1):</p> <ul style="list-style-type: none"> <li>(a) intention is the fault element for the conduct referred to in paragraph (1)(a);</li> <li>(b) recklessness is the fault element for the circumstances referred to in paragraph (1)(b).</li> </ul> <p>Note: For the meaning of <i>intention</i> and <i>recklessness</i> see sections 5.2 and 5.4.</p> <p>(3) As well as the general defences provided for in Part 2.3, defences are provided for under section 474.21 in relation to this section.</p> <p><b>Sect. 474.20 of Criminal Code Act 1995 of Australia.</b> <b>Possessing, controlling, producing, supplying or obtaining child</b></p>

**pornography material for use through a carriage service**

(1) A person is guilty of an offence if:

(a) the person:

(i) has possession or control of material; or

(ii) produces, supplies or obtains material; and

(b) the material is child pornography material; and

(c) the person has that possession or control, or engages in that production, supply or obtaining, with the intention that the material be used:

(i) by that person; or

(ii) by another person;

in committing an offence against section 474.19 (using a carriage service for child pornography material).

*Penalty:* Imprisonment for 10 years.

(2) A person may be found guilty of an offence against subsection (1) even if committing the offence against section 474.19 (using a carriage service for child pornography material) is impossible.

(3) It is not an offence to attempt to commit an offence against subsection (1).

**For Art. 9(2)**

**The Definitions in the Criminal Code Act 1995 "child pornography material" of the Australian Federal Legislation (as amended in 2005)**  
***child pornography material*** means:

(a) material that depicts a person, or a representation of a person, who is, or appears to be, under 18 years of age and who:

(i) is engaged in, or appears to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or

(ii) is in the presence of a person who is engaged in, or appears to be engaged in, a sexual pose or sexual activity; and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive; or

(b) material the dominant characteristic of which is the depiction, for a sexual purpose, of:

(i) a sexual organ or the anal region of a person who is, or appears to be, under

18 years of age; or  
(ii) a representation of such a sexual organ or anal region; or  
(iii) the breasts, or a representation of the breasts, of a female person who is, or appears to be, under 18 years of age; in a way that reasonable persons would regard as being, in all the circumstances, offensive; or  
(c) material that describes a person who is, or is implied to be, under 18 years of age and who:  
(i) is engaged in, or is implied to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or  
(ii) is in the presence of a person who is engaged in, or is implied to be engaged in, a sexual pose or sexual activity; and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive; or  
(d) material that describes:  
(i) a sexual organ or the anal region of a person who is, or is implied to be, under 18 years of age; or  
(ii) the breasts of a female person who is, or is implied to be, under 18 years of age; and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive.

**For Art. 9(3)- The Definitions in the Criminal Code Act 1995, "child abuse material" (a/i) of the Australian Federal Legislation (as amended in 2005).**

*child abuse material* means:

(a) material that depicts a person, or a representation of a person, who:  
(i) is, or appears to be, under 18 years of age; and

**For Art. 9(4)- Sect. 474.21 of Criminal Code Act 1995 of Australia Defences in respect of child pornography material**

(1)A person is not criminally responsible for an offence against section 474.19 (using a carriage service for child pornography material) or 474.20 (possessing etc. child pornography material for use through a carriage service) because of engaging in particular conduct if the conduct:  
(a) is of public benefit; and  
(b) does not extend beyond what is of public benefit.

In determining whether the person is, under this subsection, not criminally responsible for the offence, the question whether the conduct is of public benefit is a question of fact and the person's motives in engaging in the conduct are irrelevant.

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

(2) For the purposes of subsection (1), conduct is of public benefit if, and only if, the conduct is necessary for or of assistance in:

- (a) enforcing a law of the Commonwealth, a State or a Territory; or
- (b) monitoring compliance with, or investigating a contravention of, a law of the Commonwealth, a State or a Territory; or
- (c) the administration of justice; or
- (d) conducting scientific, medical or educational research that has been approved by the Minister in writing for the purposes of this section.

(3) A person is not criminally responsible for an offence against section 474.19 (using a carriage service for child pornography material) or 474.20 (possessing etc. child pornography material for use through a carriage service) if:

- (a) the person is, at the time of the offence, a law enforcement officer, or an intelligence or security officer, acting in the course of his or her duties; and
- (b) the conduct of the person is reasonable in the circumstances for the purpose of performing that duty.

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

(4) A person is not criminally responsible for an offence against section 474.19 (using a carriage service for child pornography material) or 474.20 (possessing etc. child pornography material for use through a carriage service) if the person engages in the conduct in good faith for the sole purpose of:

- (a) assisting the Australian Communications and Media Authority to detect:
  - (i) prohibited content (within the meaning of Schedule 5 to the *Broadcasting Services Act 1992*); or

	<p>(ii) potential prohibited content (within the meaning of that Schedule); in the performance of the Authority's functions under that Schedule; or</p> <p>(b) manufacturing or developing, or updating, content filtering technology (including software) in accordance with:</p> <p>(i) a recognised alternative access-prevention arrangement (within the meaning of clause 40 of Schedule 5 to the <i>Broadcasting Services Act 1992</i>); or</p> <p>(ii) a designated alternative access-prevention arrangement (within the meaning of clause 60 of that Schedule).</p> <p>Note: A defendant bears an evidential burden in relation to the matter in this subsection, see subsection 13.3(3).</p>
<p><i>Title 4 – Offences related to infringements of copyright and related rights</i></p>	
<p><b>Article 10 – Offences related to infringements of copyright and related rights</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that</p>	<p><b>For Art. 10(1)- Sec. 47G of Copyright Act 1968 of Australia. Unauthorised use of copies or information</b></p> <p>(1) If:</p> <p>(a) a reproduction or adaptation of a literary work that is a computer program is made under a prescribed provision; and</p> <p>(b) the reproduction or adaptation, or any information derived from it, is, without the consent of the owner of the copyright in the computer program, used, or sold or otherwise supplied to a person, for a purpose other than a purpose specified in the prescribed provision;</p> <p>the prescribed provision does not apply, and is taken never to have applied, to the making of the reproduction or adaptation.</p> <p>(2) For the purposes of this section, sections 47B, 47C, 47D, 47E and 47F are prescribed provisions.</p> <p><b>For Art. 1(2)- Sec. 91 of Copyright Act 1968 of Australia. Television broadcasts and sound broadcasts in which copyright subsists</b></p> <p>Subject to this Act, copyright subsists in a television broadcast or sound broadcast made from a place in Australia:</p> <p>(a) under the authority of a licence or a class licence under the <i>Broadcasting Services Act 1992</i> ; or</p> <p>(b) by the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.</p>



other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

**See also Sec. 116B Removal or alteration of electronic rights management information**

(1) This section applies if:

(a) either:

(i) a person removes, from a copy of a work or other subject-matter in which copyright subsists, any electronic rights management information that relates to the work or other subject-matter; or

(ii) a person alters any electronic rights management information that relates to a work or other subject-matter in which copyright subsists; and

(b) the person does so without the permission of the owner or exclusive licensee of the copyright; and

(c) the person knew, or ought reasonably to have known, that the removal or alteration would induce, enable, facilitate or conceal an infringement of the copyright in the work or other subject-matter.

(2) If this section applies, the owner or exclusive licensee of the copyright may bring an action against the person.

(3) In an action under subsection (2), it must be presumed that the defendant knew, or ought reasonably to have known, that the removal or alteration to which the action relates would have the effect referred to in paragraph (1)(c) unless the defendant proves otherwise.

**Sec. 116C Distribution to the public etc. of works whose electronic rights management information has been removed or altered**

(1) This section applies if:

(a) a person does any of the following acts in relation to a work or other subject-matter in which copyright subsists without the permission of the owner or exclusive licensee of the copyright:

(i) distributes a copy of the work or other subject-matter to the public;

(ii) imports into Australia a copy of the work or other subject-matter for distribution to the public;

(iii) communicates a copy of the work or other subject-matter to the public; and

(b) either:

- (i) any electronic rights management information that relates to the work or other subject-matter has been removed from the copy of the work or subject-matter; or
- (ii) any electronic rights management information that relates to the work or other subject-matter has been altered; and
- (c) the person knew that the electronic rights management information had been so removed or altered without the permission of the owner or exclusive licensee of the copyright; and
- (d) the person knew, or ought reasonably to have known, that the act referred to in paragraph (a) that was done by the person would induce, enable, facilitate or conceal an infringement of the copyright in the work or other subject-matter.

(2) If this section applies, the owner or exclusive licensee of the copyright may bring an action against the person.

- (3) In an action under subsection (2), it must be presumed that the defendant:
- (a) had the knowledge referred to in paragraph (1)(c); and
  - (b) knew, or ought reasonably to have known, that the doing of the act to which the action relates would have the effect referred to in paragraph (1)(d); unless the defendant proves otherwise.

**Sec. 132AC(1/d) Commercial-scale infringement prejudicing copyright owner**

Indictable offence

- (1) A person commits an offence if:
- (d) the infringement or infringements occur on a commercial scale.

**Sec. 132AD(1/a/iii) of Copyright Act 1968 of Australia. Making infringing copy commercially**

Indictable offence

- (1) A person commits an offence if:
- (a) the person makes an article, with the intention of:
    - (iii) obtaining a commercial advantage or profit; and

**Sec.132AD(2 Note 2) of Copyright Act 1968 of Australia. Commercial-scale infringement prejudicing copyright owner**

	<p>Indictable offence</p> <p>(2) An offence against subsection (1) is punishable on conviction by a fine of not more than 550 penalty units or imprisonment for not more than 5 years, or both.</p> <p>Note 2: If the infringing copy was made by converting the work or other subject-matter from a hard copy or analog form into a digital or other electronic machine-readable form, there is an aggravated offence with a higher maximum penalty under section 132AK.</p> <p><b>Section 132 AM Copyright Act 1968 of Australia, Advertising supply of infringing copy</b></p> <p>Summary offence</p> <p>(1) A person commits an offence if:</p> <p>(a) the person, by any means, publishes, or causes to be published, an advertisement for the supply in Australia of a copy (whether from within or outside Australia) of a work or other subject-matter; and</p> <p>(b) the copy is, or will be, an infringing copy.</p> <p>Penalty: 30 penalty units or imprisonment for 6 months, or both.</p> <p>Location of supply of copy by communication resulting in creation of copy</p> <p>(2) For the purposes of this section, a communication of a work or other subject-matter that, when received and recorded, will result in the creation of a copy of the work or other subject-matter is taken to constitute the supply of a copy of the work or other subject-matter at the place where the copy will be created.</p> <p><b>Section 132 AN Copyright Act 1968 of Australia, Causing work to be performed publicly</b></p> <p>Indictable offence</p> <p>(1) A person commits an offence if:</p> <p>(a) the person causes a literary, dramatic or musical work to be performed; and</p> <p>(b) the performance is in public at a place of public entertainment; and</p> <p>(c) the performance infringes copyright in the work.</p>
--	--

(2) An offence against subsection (1) is punishable on conviction by a fine of not more than 550 penalty units or imprisonment for not more than 5 years, or both.

Note: A corporation may be fined up to 5 times the amount of the maximum fine (see subsection 4B(3) of the *Crimes Act 1914* ).

#### Summary offence

(3) A person commits an offence if:

- (a) the person causes a literary, dramatic or musical work to be performed; and
- (b) the performance is in public at a place of public entertainment; and
- (c) the performance infringes copyright in the work and the person is negligent as to that fact.

Penalty: 120 penalty units or imprisonment for 2 years, or both.

(4) An offence against subsection (3) is a summary offence, despite section 4G of the *Crimes Act 1914* .

### **Section 132AO of the Copyright Act 1968 of Australia, Causing recording or film to be heard or seen in public**

#### Indictable offence

(1) A person commits an offence if:

- (a) the person causes:
  - (i) a sound recording to be heard; or
  - (ii) images from a cinematograph film to be seen; or
  - (iii) sound from a cinematograph film to be heard; and
- (b) the hearing or seeing occurs in public at a place of public entertainment; and
- (c) causing the hearing or seeing infringes copyright in the recording or film.

(2) An offence against subsection (1) is punishable on conviction by a fine of not more than 550 penalty units or imprisonment for not more than 5 years, or both.

Note: A corporation may be fined up to 5 times the amount of the maximum fine (see subsection 4B(3) of the *Crimes Act 1914* ).

Summary offence

(3) A person commits an offence if:

(a) the person causes:

- (i) a sound recording to be heard; or
- (ii) images from a cinematograph film to be seen; or
- (iii) sound from a cinematograph film to be heard; and

(b) the hearing or seeing occurs in public at a place of public entertainment; and

(c) causing the hearing or seeing infringes copyright in the recording or film and the person is negligent as to that fact.

Penalty: 120 penalty units or imprisonment for 2 years, or both.

(4) An offence against subsection (3) is a summary offence, despite section 4G of the *Crimes Act 1914* .

Strict liability offence

5) A person commits an offence if:

(a) the person causes:

- (ii) images from a cinematograph film to be seen; or
- (iii) sound from a cinematograph film to be heard; and

(b) the hearing or seeing occurs in public at a place of public entertainment; and

(c) causing the hearing or seeing infringes copyright in the recording or film.

Penalty: 60 penalty units.

6) Subsection (5) is an offence of strict liability.

Note: For strict liability, see section 6.1 of the *Criminal Code*

**Section 132 APA of the Copyright Act 1968 of Australia**

Definitions

In this Subdivision, *computer program* has the same meaning as in section 47AB.

**Section 132APB of the Copyright Act 1968 of Australia**

Interaction of this Subdivision with Part VAA

This Subdivision does not apply to encoded broadcasts (within the meaning of Part VAA).

**Section 132APC of the Copyright Act 1968 of Australia**

Circumventing an access control technological protection measure

(1) A person commits an offence if:

- (a) the person engages in conduct; and
- (b) the conduct results in the circumvention of a technological protection measure; and
- (c) the technological protection measure is an access control technological protection measure; and
- (d) the person engages in the conduct with the intention of obtaining a commercial advantage or profit.

Penalty: 60 penalty units.

Defence--permission

(2) Subsection (1) does not apply to the person if the person has the permission of the copyright owner or exclusive licensee to circumvent the access control technological protection measure.

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

Defence--interoperability

(3) Subsection (1) does not apply to the person if:

- (a) the person circumvents the access control technological protection measure to enable the person to do an act; and
- (b) the act:
  - (i) relates to a copy of a computer program (the *original program* ) that is not an infringing copy and that was lawfully obtained; and
  - (ii) will not infringe the copyright in the original program; and
  - (iia) relates to elements of the original program that will not be readily available to the person when the circumvention occurs; and
  - (iii) will be done for the sole purpose of achieving interoperability of an independently created computer program with the original program or any other program.

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

	<p>Defence--encryption research</p> <p>(4) Subsection (1) does not apply to the person if:</p> <p>(a) the person circumvents the access control technological protection measure to enable:</p> <ul style="list-style-type: none"> <li>(i) the person; or</li> <li>(ii) if the person is a body corporate--an employee of the person; to do an act; and</li> </ul> <p>(b) the act:</p> <ul style="list-style-type: none"> <li>(i) relates to a copy of a work or other subject-matter that is not an infringing copy and that was lawfully obtained; and</li> <li>(ii) will not infringe the copyright in the work or other subject-matter; and</li> <li>(iii) will be done for the sole purpose of identifying and analysing flaws and vulnerabilities of encryption technology; and</li> </ul> <p>(c) the person or employee is:</p> <ul style="list-style-type: none"> <li>(i) engaged in a course of study at an educational institution in the field of encryption technology; or</li> <li>(ii) employed, trained or experienced in the field of encryption technology; and</li> </ul> <p>(d) the person or employee:</p> <ul style="list-style-type: none"> <li>(i) has obtained permission from the owner or exclusive licensee of the copyright to do the act; or</li> <li>(ii) has made, or will make, a good faith effort to obtain such permission.</li> </ul> <p>In this subsection, <i>encryption technology</i> means the scrambling and descrambling of information using mathematical formulas or algorithms.</p> <p>Note: A defendant bears an evidential burden in relation to the matter in subsection (4) (see subsection 13.3(3) of the <i>Criminal Code</i> ).</p> <p>Defence--computer security testing</p> <p>(5) Subsection (1) does not apply to the person if:</p> <p>(a) the person circumvents the access control technological protection measure to enable the person to do an act; and</p> <p>b) the act:</p> <ul style="list-style-type: none"> <li>(i) relates to a copy of a computer program that is not an infringing copy; and</li> <li>(ii) will not infringe the copyright in the computer program; and</li> <li>(iii) will be done for the sole purpose of testing, investigating or correcting the security of a computer, computer system or computer network; and</li> </ul>
--	--

(iv) will be done with the permission of the owner of the computer, computer system or computer network.

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

Defence--online privacy

(6) Subsection (1) does not apply to the person if:

(a) the person circumvents the access control technological protection measure to enable the person to do an act; and

(b) the act:

(i) relates to a copy of a work or other subject-matter that is not an infringing copy; and

(ii) will not infringe the copyright in the work or other subject-matter; and

(iii) will be done for the sole purpose of identifying and disabling an undisclosed capability to collect or disseminate personally identifying information about the online activities of a natural person; and

(iv) will not affect the ability of the person or any other person to gain access to the work or other subject-matter or any other work or subject-matter.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code* ).

Defence--law enforcement and national security

(7) Subsection (1) does not apply in relation to anything lawfully done for the purposes of:

(a) law enforcement; or

(b) national security; or

(c) performing a statutory function, power or duty;

by or on behalf of the Commonwealth, a State or a Territory, or an authority of one of those bodies.

Note: A defendant bears an evidential burden in relation to the matter in subsection (7) (see subsection 13.3(3) of the *Criminal Code* ).

Defence--libraries etc.

(8) Subsection (1) does not apply in respect of anything lawfully done by the following bodies in performing their functions:



- (a) a library (other than a library that is conducted for the profit, direct or indirect, of an individual or individuals);
- (b) a body mentioned in:
  - (i) paragraph (a) of the definition of *archives* in subsection 10(1); or
  - (ii) subsection 10(4);
- (c) an educational institution;
- d) a public non-commercial broadcaster (including a body that provides a national broadcasting service, within the meaning of the *Broadcasting Services Act 1992*, and a body that holds a community broadcasting licence within the meaning of that Act).

Note 1: A library that is owned by a person conducting a business for profit might not itself be conducted for profit (see section 18).

Note 2: A defendant bears an evidential burden in relation to the matter in subsection (8) (see subsection 13.3(3) of the *Criminal Code* ).

(8A) This section does not apply in respect of anything lawfully done by a person in connection with a work or other subject-matter if:

- (a) the person has custody of the work or other subject-matter under an arrangement referred to in section 64 of the *Archives Act 1983* ; and
- (b) under subsection (8), it would be lawful for the National Archives of Australia to do that thing.

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

Defence--prescribed acts

(9) Subsection (1) does not apply to the person if:

- (a) the person circumvents the access control technological protection measure to enable the person to do an act; and
- (b) the act will not infringe the copyright in a work or other subject-matter; and
- (c) the doing of the act by the person is prescribed by the regulations.

Note 1: A defendant bears an evidential burden in relation to the matter in subsection (9) (see subsection 13.3(3) of the *Criminal Code* ).

Note 2: For the making of regulations prescribing the doing of an act by a person, see section 249.

**Section 132 APD of the Copyright Act 1968, Manufacturing etc. a circumvention device for a technological p Section rotection measure**

- (1) A person commits an offence if:
- (a) the person does any of the following acts with a device:
    - (i) manufactures it with the intention of providing it to another person;
    - (ii) imports it into Australia with the intention of providing it to another person;
    - (iii) distributes it to another person;
    - (iv) offers it to the public;
    - (v) provides it to another person;
    - (vi) communicates it to another person; and
  - (b) the person does the act with the intention of obtaining a commercial advantage or profit; and
  - (c) the device is a circumvention device for a technological protection measure.
- Penalty: 550 penalty units or imprisonment for 5 years, or both.  
 Defence--no promotion, advertising etc.
- (2) Subsection (1) does not apply to the person if:
- (a) the device is a circumvention device for the technological protection measure only because it was promoted, advertised or marketed as having the purpose of circumventing the technological protection measure; and
  - (b) both of the following apply:
    - (i) the person did not do such promoting, advertising or marketing;
    - (ii) the person did not direct or request (expressly or impliedly) another person to do such promoting, advertising or marketing.
- Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code* ).  
 Defence--interoperability
- (3) Subsection (1) does not apply to the person if:
- (a) the circumvention device will be used to circumvent the technological protection measure to enable the doing of an act; and
  - (b) the act:
    - (i) relates to a copy of a computer program (the **original program** ) that is not an infringing copy and that was lawfully obtained; and
    - (ii) will not infringe the copyright in the original program; and
    - (iia) relates to elements of the original program that will not be readily available to the person doing the act when the circumvention occurs; and

(iii) will be done for the sole purpose of achieving interoperability of an independently created computer program with the original program or any other program.

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

Defence--encryption research

(4) Subsection (1) does not apply to the person if:

(a) the technological protection measure is an access control technological protection measure; and

(b) the circumvention device will be used to circumvent the access control technological protection measure to enable a person (the **researcher** ) to do an act; and

(c) the act:

(i) relates to a copy of a work or other subject-matter that is not an infringing copy and that was lawfully obtained; and

(ii) will not infringe the copyright in the work or other subject-matter; and

(iii) will be done for the sole purpose of identifying and analysing flaws and vulnerabilities of encryption technology; and

(d) the researcher is:

(i) engaged in a course of study at an educational institution in the field of encryption technology; or

(ii) employed, trained or experienced in the field of encryption technology; and

(e) the researcher:

(i) has obtained permission from the owner or exclusive licensee of the copyright to do the act; or

(ii) has made, or will make, a good faith effort to obtain such permission.

In this subsection, **encryption technology** means the scrambling and descrambling of information using mathematical formulas or algorithms.

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

Defence--computer security testing

(5) Subsection (1) does not apply to the person if:

(a) the technological protection measure is an access control technological protection measure; and

(b) the circumvention device will be used to circumvent the access control technological protection measure to enable the doing of an act; and

(c) the act:

- (i) relates to a copy of a computer program that is not an infringing copy; and
- (ii) will not infringe the copyright in the computer program; and
- (iii) will be done for the sole purpose of testing, investigating or correcting the security of a computer, computer system or computer network; and
- (iv) will be done with the permission of the owner of the computer, computer system or computer network.

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

Defence--law enforcement and national security

(6) Subsection (1) does not apply in relation to anything lawfully done for the purposes of:

- (a) law enforcement; or
- (b) national security; or
- (c) performing a statutory function, power or duty;

by or on behalf of the Commonwealth, a State or a Territory, or an authority of one of those bodies.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code* ).

Defence--libraries etc.

(7) Subsection (1) does not apply in respect of anything lawfully done by the following bodies in performing their functions:

- (a) a library (other than a library that is conducted for the profit, direct or indirect, of an individual or individuals);
- (b) a body mentioned in:
  - (i) paragraph (a) of the definition of **archives** in subsection 10(1); or
  - (ii) subsection 10(4);
- (c) an educational institution;
- (d) a public non-commercial broadcaster (including a body that provides a national broadcasting service, within the meaning of the *Broadcasting Services Act 1992*, and a body that holds a community broadcasting licence within the meaning of that Act).

Note 1: A library that is owned by a person conducting a business for profit

might not itself be conducted for profit (see section 18).

Note 2: A defendant bears an evidential burden in relation to the matter in subsection (7) (see subsection 13.3(3) of the *Criminal Code* ).

(8) This section does not apply in respect of anything lawfully done by a person in connection with a work or other subject-matter if:

- a) the person has custody of the work or other subject-matter under an arrangement referred to in section 64 of the *Archives Act 1983* ; and
- (b) under subsection (7), it would be lawful for the National Archives of Australia to do that thing.

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

### **Section 132APE of the Copyright Act 1968**

Providing etc. a circumvention service for a technological protection measure

(1) A person commits an offence if:

a) the person:

- (i) provides a service to another person; or
- (ii) offers a service to the public; and

(b) the person does so with the intention of obtaining a commercial advantage or profit; and

(c) the service is a circumvention service for a technological protection measure.

Penalty: 550 penalty units or imprisonment for 5 years, or both.

Defence--no promotion, advertising etc.

(2) Subsection (1) does not apply to the person if:

(a) the service is a circumvention service for the technological protection measure only because it was promoted, advertised or marketed as having the purpose of circumventing the technological protection measure; and

(b) both of the following apply:

- (i) the person did not do such promoting, advertising or marketing;
- (ii) the person did not direct or request (expressly or impliedly) another person to do such promoting, advertising or marketing.

Note: A defendant bears an evidential burden in relation to the matter in

subsection (2) (see subsection 13.3(3) of the *Criminal Code* ).

#### Defence--interoperability

(3) Subsection (1) does not apply to the person if:

(a) the circumvention service will be used to circumvent a technological protection measure to enable the doing of an act; and

(b) the act:

(i) relates to a copy of a computer program (the *original program* ) that is not an infringing copy and that was lawfully obtained; and

(ii) will not infringe the copyright in the original program; and

(iia) relates to elements of the original program that will not be readily available to the person doing the act when the circumvention occurs; and

(iii) will be done for the sole purpose of achieving interoperability of an independently created computer program with the original program or any other program.

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

#### Defence--encryption research

(4) Subsection (1) does not apply to the person if:

(a) the technological protection measure is an access control technological protection measure; and

(b) the circumvention service will be used to circumvent the access control technological protection measure to enable a person (the *researcher* ) to do an act; and

(c) the act:

(i) relates to a copy of a work or other subject-matter that is not an infringing copy and that was lawfully obtained; and

(ii) will not infringe the copyright in the work or other subject-matter; and

(iii) will be done for the sole purpose of identifying and analysing flaws and vulnerabilities of encryption technology; and

(d) the researcher is:

(i) engaged in a course of study at an educational institution in the field of encryption technology; or

(ii) employed, trained or experienced in the field of encryption technology;

and  
(e) the researcher:  
(i) has obtained permission from the owner or exclusive licensee of the copyright to do the act; or  
(ii) has made, or will make, a good faith effort to obtain such permission.  
In this subsection, *encryption technology* means the scrambling and descrambling of information using mathematical formulas or algorithms.  
Note: A defendant bears an evidential burden in relation to the matter in subsection (4) (see subsection 13.3(3) of the *Criminal Code* ).

Defence--computer security testing

(5) Subsection (1) does not apply to the person if:  
(a) the technological protection measure is an access control technological protection measure; and  
(b) the circumvention service will be used to circumvent the access control technological protection measure to enable the doing of an act; and  
(c) the act:  
(i) relates to a copy of a computer program that is not an infringing copy; and  
(ii) will not infringe the copyright in the computer program; and  
(iii) will be done for the sole purpose of testing, investigating or correcting the security of a computer, computer system or computer network; and  
(iv) will be done with the permission of the owner of the computer, computer system or computer network.

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

Defence--law enforcement and national security

(6) Subsection (1) does not apply in relation to anything lawfully done for the purposes of:  
(a) law enforcement; or  
(b) national security; or  
(c) performing a statutory function, power or duty;  
by or on behalf of the Commonwealth, a State or a Territory, or an authority of one of those bodies.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code* ).

	<p>Defence--libraries etc.</p> <p>(7) Subsection (1) does not apply in respect of anything lawfully done by the following bodies in performing their functions:</p> <p>(a) a library (other than a library that is conducted for the profit, direct or indirect, of an individual or individuals);</p> <p>(b) a body mentioned in:</p> <p>(i) paragraph (a) of the definition of <i>archives</i> in subsection 10(1); or</p> <p>(ii) subsection 10(4);</p> <p>(c) an educational institution;</p> <p>(d) a public non-commercial broadcaster (including a body that provides a national broadcasting service, within the meaning of the <i>Broadcasting Services Act 1992</i>, and a body that holds a community broadcasting licence within the meaning of that Act).</p> <p>Note 1: A library that is owned by a person conducting a business for profit might not itself be conducted for profit (see section 18).</p> <p>Note 2: A defendant bears an evidential burden in relation to the matter in subsection (7) (see subsection 13.3(3) of the <i>Criminal Code</i> ).</p> <p>(8) This section does not apply in respect of anything lawfully done by a person in connection with a work or other subject-matter if:</p> <p>(a) the person has custody of the work or other subject-matter under an arrangement referred to in section 64 of the <i>Archives Act 1983</i> ; and</p> <p>(b) under subsection (7), it would be lawful for the National Archives of Australia to do that thing.</p> <p>Note: A defendant bears an evidential burden in relation to the matter in subsection (8) (see subsection 13.3(3) of the <i>Criminal Code</i> ).</p>
<i>Title 5 – Ancillary liability and sanctions</i>	
<p><b>Article 11 – Attempt and aiding or abetting</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be</p>	<p><b>For Art. 11(2)</b></p> <p><b>Art. 477.1 (8) of Criminal Code Act 1995 (Act n°12 of 1995) of Australia</b></p> <p><b>Unauthorised access, modification or impairment with intent to commit a serious offence</b></p> <p><i>No offence of attempt</i></p> <p>(8) It is not an offence to attempt to commit an offence against this section.</p>



necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

**Art. 478.3(3) of Criminal Code Act 1995 (Act n°12 of 1995) of Australia**  
**Possession or control of data with intent to commit a computer offence**

*No offence of attempt*

(3) It is not an offence to attempt to commit an offence against this section.

**Art. 478.4(3) of Criminal Code Act 1995 (Act n°12 of 1995) of Australia**  
**Producing, supplying or obtaining data with intent to commit a computer offence**

*No offence of attempt*

(3) It is not an offence to attempt to commit an offence against this section.

**Section 7 of TIA Act**

Telecommunications not to be intercepted

(1) A person shall not:

(a) intercept;

(b) authorize, suffer or permit another person to intercept; or

(c) do any act or thing that will enable him or her or another person to intercept; a communication passing over a telecommunications system.

(2) Subsection (1) does not apply to or in relation to:

(a) an act or thing done by an employee of a carrier in the course of his or her duties for or in connection with:

(i) the installation of any line, or the installation of any equipment, used or intended for use in connection with a telecommunications service; or

(ii) the operation or maintenance of a telecommunications system; or

(iii) the identifying or tracing of any person who has contravened, or is suspected of having contravened or being likely to contravene, a provision of Part 10.6 of the *Criminal Code*;

where it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively; or

(aa) the interception of a communication by another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line, where it is reasonably necessary for the person to intercept the communication in order to perform those duties effectively; or

(aaa) the interception of a communication by a person if:

(i) the person is authorised, in writing, by a responsible person for a computer network to engage in network protection duties in relation to the network; and

(ii) it is reasonably necessary for the person to intercept the communication in order to perform those duties effectively; or

(ab) the interception of a communication by a person lawfully engaged in duties relating to the installation, connection or maintenance of equipment used, or to be used, for the interception of communications under warrants; or

(ac) the interception of a communication where the interception results from, or is incidental to, action taken by an officer of the Organisation, in the lawful performance of his or her duties, for the purpose of:

(i) discovering whether a listening device is being used at, or in relation to, a particular place; or

(ii) determining the location of a listening device; or

(b) the interception of a communication under a warrant; or

(c) the interception of a communication pursuant to a request made, or purporting to be made, under subsection 30(1) or (2); or

(d) the interception of a communication under an authorisation under section 31A.

(2A) For the purposes of paragraphs (2)(a), (aa) and (aaa), in determining whether an act or thing done by a person was reasonably necessary in order for the person to perform his or her duties effectively, a court is to have regard to

such matters (if any) as are specified in, or ascertained in accordance with, the regulations.

(3) Paragraph (2)(aaa) does not apply to a voice communication in the form of speech (including a communication that involves a recorded or synthetic voice).

(4) Subsection (1) does not apply to, or in relation to, an act done by an officer of an agency in relation to a communication if the following conditions are satisfied:

(a) the officer or another officer of the agency is a party to the communication; and

(b) there are reasonable grounds for suspecting that another party to the communication has:

(i) done an act that has resulted, or may result, in loss of life or the infliction of serious personal injury; or

(ii) threatened to kill or seriously injure another person or to cause serious damage to property; or

(iii) threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety; and

(c) because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a Part 2-5 warrant to be made.

(5) Subsection (1) does not apply to, or in relation to, an act done by an officer of an agency in relation to a communication if the following conditions are satisfied:

(a) the person to whom the communication is directed has consented to the doing of the act; and

(b) there are reasonable grounds for believing that that person is likely to receive a communication from a person who has:

(i) done an act that has resulted, or may result, in loss of life or the infliction of serious personal injury; or

	<p>(ii) threatened to kill or seriously injure another person or to cause serious damage to property; or</p> <p>(iii) threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety; and</p> <p>(c) because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a Part 2-5 warrant to be made.</p> <p>(6) As soon as practicable after the doing of an act in relation to a communication under the provisions of subsection (4) or (5), an officer of the agency which is concerned with the communication shall cause an application for a Part 2-5 warrant to be made in relation to the matter.</p> <p>(6A) Subsection (6) does not apply if action has been taken under subsection (4) or (5) to intercept a communication, or cause it to be intercepted, and the action has ceased before it is practicable for an application for a Part 2-5 warrant to be made.</p> <p>(7) Where after considering an application made in relation to a matter arising under subsections (4) or (5) and (6) a Judge or nominated AAT member does not issue a warrant in relation to the application, the chief officer of the agency concerned shall ensure that no further action is taken by the agency to intercept the communication or to cause it to be intercepted.</p> <p>(8) Subsections (4), (5), (6) and (7) only apply where the agency concerned is:</p> <p>(a) the Australian Federal Police; or</p> <p>(b) the Police Force of a State.</p> <p>(9) The doing of an act mentioned in subparagraph (4)(b)(ii) or (iii) or (5)(b)(ii) or (iii) in a particular case is taken to constitute a serious offence, even if it would not constitute a serious offence apart from this subsection.</p> <p>Note: See subsection (6). A Part 2-5 warrant can only be issued for the purposes of an investigation relating to the commission of a serious offence.</p> <p>(10) Subsection (9) has effect only to the extent necessary:</p>
--	--

	<p>(a) to enable an application to be made for the purposes of subsection (6); and</p> <p>(b) to enable a decision to be made on such an application and, if a Judge so decides, a Part 2-5 warrant to be issued; and</p> <p>(c) to enable this Act to operate in relation to a Part 2-5 warrant issued on such an application.</p>
<p><b>Article 12 – Corporate liability</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> <li>a a power of representation of the legal person;</li> <li>b an authority to take decisions on behalf of the legal person;</li> <li>c an authority to exercise control within the legal person.</li> </ul> <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	<p><b>Part 2.5—Corporate criminal responsibility</b></p> <p><b>Division 12</b></p> <p><b>12.1 General principles</b></p> <p><b>(1) This Code applies to bodies corporate in the same way as it applies to individuals. It so applies with such modifications as are set out in this Part, and with such other modifications as are made necessary by the fact that criminal liability is being imposed on bodies corporate rather than individuals.</b></p> <p><b>(2) A body corporate may be found guilty of any offence, including one punishable by imprisonment.</b></p> <p>Note: Section 4B of the <i>Crimes Act 1914</i> enables a fine to be imposed for offences that only specify imprisonment as a penalty.</p> <p><b>12.2 Physical elements</b></p> <p>If a physical element of an offence is committed by an employee, agent or officer of a body corporate acting within the actual or apparent scope of his or her employment, or within his or her actual or apparent authority, the physical element must also be attributed to the body corporate.</p> <p><b>12.3 Fault elements other than negligence</b></p> <p>(1) If intention, knowledge or recklessness is a fault element in relation to a physical element of an offence, that fault element must be attributed to a body corporate that expressly, tacitly or impliedly authorised or permitted the commission of the offence.</p> <p>(2) The means by which such an authorisation or permission may be established include:</p> <ul style="list-style-type: none"> <li>(a) proving that the body corporate’s board of directors intentionally, knowingly or recklessly carried out the relevant conduct, or expressly, tacitly or impliedly authorised or permitted the commission of the offence; or</li> </ul>

(b) proving that a high managerial agent of the body corporate intentionally, knowingly or recklessly engaged in the relevant conduct, or expressly, tacitly or impliedly authorised or permitted the commission of the offence; or

(c) proving that a corporate culture existed within the body corporate that directed, encouraged, tolerated or led to non-compliance with the relevant provision; or

(d) proving that the body corporate failed to create and maintain a corporate culture that required compliance with the relevant provision.

(3) Paragraph (2)(b) does not apply if the body corporate proves that it exercised due diligence to prevent the conduct, or the authorisation or permission.

(4) Factors relevant to the application of paragraph (2)(c) or (d) include:

(a) whether authority to commit an offence of the same or a similar character had been given by a high managerial agent of the body corporate; and

(b) whether the employee, agent or officer of the body corporate who committed the offence believed on reasonable grounds, or entertained a reasonable expectation, that a high managerial agent of the body corporate would have authorised or permitted the commission of the offence.

(5) If recklessness is not a fault element in relation to a physical element of an offence, subsection (2) does not enable the fault element to be proved by proving that the board of directors, or a high managerial agent, of the body corporate recklessly engaged in the conduct or recklessly authorised or permitted the commission of the offence.

(6) In this section:

**board of directors** means the body (by whatever name called) exercising the executive authority of the body corporate.

**corporate culture** means an attitude, policy, rule, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant activities takes place.

**high managerial agent** means an employee, agent or officer of the body corporate with duties of such responsibility that his or her conduct may fairly be assumed to represent the body corporate's policy.

#### **12.4 Negligence**

(1) The test of negligence for a body corporate is that set out in section 5.5.

(2) If:

	<p>(a) negligence is a fault element in relation to a physical element of an offence; and</p> <p>(b) no individual employee, agent or officer of the body corporate has that fault element;</p> <p>that fault element may exist on the part of the body corporate if the body corporate's conduct is negligent when viewed as a whole (that is, by aggregating the conduct of any number of its employees, agents or officers).</p> <p>(3) Negligence may be evidenced by the fact that the prohibited conduct was substantially attributable to:</p> <p>(a) inadequate corporate management, control or supervision of the conduct of one or more of its employees, agents or officers; or</p> <p>(b) failure to provide adequate systems for conveying relevant information to relevant persons in the body corporate.</p> <p><b>12.5 Mistake of fact (strict liability)</b></p> <p>(1) A body corporate can only rely on section 9.2 (mistake of fact (strict liability)) in respect of conduct that would, apart from this section, constitute an offence on its part if:</p> <p>(a) the employee, agent or officer of the body corporate who carried out the conduct was under a mistaken but reasonable belief about facts that, had they existed, would have meant that the conduct would not have constituted an offence; and</p> <p>(b) the body corporate proves that it exercised due diligence to prevent the conduct.</p> <p>(2) A failure to exercise due diligence may be evidenced by the fact that the prohibited conduct was substantially attributable to:</p> <p>(a) inadequate corporate management, control or supervision of the conduct of one or more of its employees, agents or officers; or</p> <p>(b) failure to provide adequate systems for conveying relevant information to relevant persons in the body corporate.</p> <p><b>12.6 Intervening conduct or event</b></p> <p>A body corporate cannot rely on section 10.1 (intervening conduct or event) in respect of a physical element of an offence brought about by another person if the other person is an employee, agent or officer of the body corporate.</p>
<b>Article 13 – Sanctions and measures</b>	Australia's domestic offences establish appropriate penalties, including

<p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p> <p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.</p>	<p>imprisonment. The penalty for each offence is contained within the specific offence provision.</p>
<p><b>Section 2 – Procedural law</b></p>	
<p><b>Article 14 – Scope of procedural provisions</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.</p> <p>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> <li>a the criminal offences established in accordance with Articles 2 through 11 of this Convention;</li> <li>b other criminal offences committed by means of a computer system; and</li> <li>c the collection of evidence in electronic form of a criminal offence.</li> </ul> <p>3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.</p> <ul style="list-style-type: none"> <li>b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: <ul style="list-style-type: none"> <li>i is being operated for the benefit of a closed group of users, and</li> <li>ii does not employ public communications networks and is</li> </ul> </li> </ul>	<p>Australian law currently provides for all of the powers required by the Convention (powers are contained in Articles 14 – 21 inclusive).</p> <p>Australia anticipates pursuing this reservation.</p> <p>Domestic Australia law restricts real-time collection of traffic data to criminal offences with a minimum penalty threshold of 3 years imprisonment.</p>



<p>not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	
<p><b>Article 15 – Conditions and safeguards</b> 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.</p>	<p><b>See TIA act attached separately as well as the Mutual Assistance In Criminal Matters Act 1987 (MA Act)</b></p>
<p><b>Article 16 – Expedited preservation of stored computer data</b> 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may</p>	<p><b>Subsections 313 (3) of the Telecommunication Act</b></p> <p>(3) A carrier or carriage service provider must, in connection with:</p> <ul style="list-style-type: none"> <li>(a) the operation by the carrier or provider of telecommunications networks or facilities; or</li> <li>(b) the supply by the carrier or provider of carriage services; give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:</li> <li>(c) enforcing the criminal law and laws imposing pecuniary penalties;</li> <li>(d) protecting the public revenue;</li> <li>(e) safeguarding national security.</li> </ul>

<p>be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>See the text attached on general search and seizure powers of Part 1AA of the Crimes Act 1914 (Crimes Act).</b></p>
<p><b>Article 17 – Expedited preservation and partial disclosure of traffic data</b></p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <p>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</p> <p>b ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Section 180 of TIA Act Authorisations for access to prospective information or documents</b></p> <p>(1) Sections 276, 277 and 278 of the <i>Telecommunications Act 1997</i> do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under this section.</p> <p>Prospective authorisation</p> <p>(2) An authorised officer of a criminal law-enforcement agency may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force. Authorisation for access to existing information or documents may also be sought</p> <p>(3) The authorised officer may, in that authorisation, also authorise the disclosure of specified information or specified documents that came into existence before the time the authorisation comes into force.</p> <p>Limits on making the authorisation</p> <p>(4) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.</p> <p>(5) Before making the authorisation, the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.</p>

	<p>Period for which authorisation is in force</p> <p>(6) An authorisation under this section:</p> <p>(a) comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation; and</p> <p>(b) ends at the time specified in the authorisation (which must be a time that is no longer than the end of the period of 45 days beginning on the day the authorisation is made), unless it is revoked earlier.</p> <p>Note: Section 184 deals with notification of authorisations.</p> <p>Revoking the authorisation</p> <p>(7) An authorised officer of the criminal law-enforcement agency must revoke the authorisation if he or she is satisfied that the disclosure is no longer required.</p> <p>Note: Section 184 deals with notification of revocations.</p>
<p><b>Article 18 – Production order</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and</p> <p>b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:</p> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;</p> <p>c any other information on the site of the installation of communication equipment, available on the basis of the service</p>	<p><b>For Art. 18(1/a)- Art. 3LB(2) of Crimes Act 1914 of Australia.</b></p> <p><b>3LB Accessing data held on other premises—notification to occupier of that premises</b></p> <p>(2) A notification under subsection (1) must include sufficient information to allow the occupier of the other premises to contact the executing officer.</p> <p><b>For Art. 18(1/a)- Subsection 24, Art. 201(1) (1 Note) of Customs Act 1901 of Australia</b></p> <p><b>24 Subsection 201(1)</b></p> <p>Repeal the subsection, substitute:</p> <p>(1) The executing officer or a person assisting may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she believes on reasonable grounds that:</p> <p>(a) the data might constitute evidential material; and</p> <p>(b) the equipment can be operated without damaging it.</p> <p>Note: An executing officer can obtain an order requiring a person with knowledge of a computer or computer system to provide assistance: see section 201A.</p> <p>(1A) If the executing officer or person assisting believes on reasonable grounds that any data accessed by operating the electronic equipment might constitute evidential material, he or she may:</p>

<p>agreement or arrangement.</p>	<p>(a) copy the data to a disk, tape or other associated device brought to the premises; or  (b) if the occupier of the premises agrees in writing—copy the data to a disk, tape or other associated device at the premises; and take the device from the premises.  (1B) If:  (a) the executing officer or person assisting takes the device from the premises; and  (b) the CEO is satisfied that the data is not required (or is no longer required) for:  (i) investigating an offence against the law of the Commonwealth, a State or a Territory; or  (ii) judicial proceedings or administrative review proceedings; or  (iii) investigating or resolving a complaint under the</p>
<p><b>Article 19 – Search and seizure of stored computer data</b>  1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:  a a computer system or part of it and computer data stored therein; and  b a computer-data storage medium in which computer data may be stored  in its territory.  2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.  3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:  a seize or similarly secure a computer system or part of it or a computer-data storage medium;</p>	<p><b>For Art. 19(1)- Art. 3LA(a) of Crimes Act 1914 of Australia</b>  <b>Person with knowledge of a computer or a computer system to assist access etc.</b>  (1) The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:  (a) access data held in, or accessible from, a computer that is on warrant premises;  <b>For Art. 19(3/a)- Art. 3LA(b) of Crimes Act 1914 of Australia</b>  <b>3LB Accessing data held on other premises—notification to occupier of that premises</b>  (1) If:  (b) it is practicable to notify the occupier of the other premises that the data has been accessed under a warrant; the executing officer must:  (c) do so as soon as practicable; and  (d) if the executing officer has arranged, or intends to arrange, for continued access to the data under subsection 3L(1A) or  (2)—include that information in the notification.  <b>For Art.19(4)- Art. 3LA(3) of Crimes Act 1914 of Australia.</b></p>

<p>b make and retain a copy of those computer data;</p> <p>c maintain the integrity of the relevant stored computer data;</p> <p>d render inaccessible or remove those computer data in the accessed computer system.</p> <p>4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Person with knowledge of a computer or a computer system to assist access etc.</b></p> <p>(3) A person commits an offence if the person fails to comply with the order.</p> <p><b>For Art.19(1)- Subsection 24, Art. 201(1) (1) of Customs Act 1901 of Australia.</b></p> <p><b>24 Subsection 201(1)</b></p> <p>Repeal the subsection, substitute:</p> <p>(1) The executing officer or a person assisting may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she believes on reasonable grounds that:</p> <p>(a) the data might constitute evidential material; and</p> <p>(b) the equipment can be operated without damaging it.</p> <p><b>For Art. 19 (3/b)- Subsection 24, Art. 201(1) (1A/a) of Customs Act 1901 of Australia.</b></p> <p>(1A) If the executing officer or person assisting believes on reasonable grounds that any data accessed by operating the electronic equipment might constitute evidential material, he or she may:</p> <p>(a) copy the data to a disk, tape or other associated device brought to the premises; or</p> <p><b>subsections 313 (3) of the Telecommunication Act</b></p> <p>(3) A carrier or carriage service provider must, in connection with:</p> <p>(a) the operation by the carrier or provider of telecommunications networks or facilities; or</p> <p>(b) the supply by the carrier or provider of carriage services; give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:</p> <p>(c) enforcing the criminal law and laws imposing pecuniary penalties;</p> <p>(d) protecting the public revenue;</p> <p>(e) safeguarding national security.</p>
<p><b>Article 20 – Real-time collection of traffic data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be</p>	<p><b>Section 180 of TIA Act Authorisations for access to prospective information or documents</b></p>

<p>necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> <li>a collect or record through the application of technical means on the territory of that Party, and</li> <li>b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> <li>i to collect or record through the application of technical means on the territory of that Party; or</li> <li>ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.</li> </ul> </li> </ul> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>(1) Sections 276, 277 and 278 of the <i>Telecommunications Act 1997</i> do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under this section. Prospective authorisation</p> <p>(2) An authorised officer of a criminal law-enforcement agency may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force. Authorisation for access to existing information or documents may also be sought</p> <p>(3) The authorised officer may, in that authorisation, also authorise the disclosure of specified information or specified documents that came into existence before the time the authorisation comes into force. Limits on making the authorisation</p> <p>(4) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.</p> <p>(5) Before making the authorisation, the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure. Period for which authorisation is in force</p> <p>(6) An authorisation under this section: (a) comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation; and (b) ends at the time specified in the authorisation (which must be a time that is no longer than the end of the period of 45 days beginning on the day the authorisation is made), unless it is revoked earlier. Note: Section 184 deals with notification of authorisations. Revoking the authorisation</p> <p>(7) An authorised officer of the criminal law-enforcement agency must revoke</p>
---	--

	<p>the authorisation if he or she is satisfied that the disclosure is no longer required.  Note: Section 184 deals with notification of revocations.</p>
<p><b>Article 21 – Interception of content data</b>  1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:  a collect or record through the application of technical means on the territory of that Party, and  b compel a service provider, within its existing technical capability:  i to collect or record through the application of technical means on the territory of that Party, or  ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.  2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.  3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.  4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>section 63 of the TIA Act No dealing in intercepted information or interception warrant information</b>  (1) Subject to this Part, a person shall not, after the commencement of this Part:  (a) communicate to another person, make use of, or make a record of; or  (b) give in evidence in a proceeding;  lawfully intercepted information or information obtained by intercepting a communication in contravention of subsection 7(1).  (2) Subject to this Part, a person must not, after the commencement of this subsection:  (a) communicate interception warrant information to another person; or  (b) make use of interception warrant information; or  (c) make a record of interception warrant information; or  (d) give interception warrant information in evidence in a proceeding.</p>
<b>Section 3 – Jurisdiction</b>	
<p><b>Article 22 – Jurisdiction</b>  1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:  a in its territory; or</p>	<p><b>Section 4 and 4A of the TIA Act</b>  <b>SECT 4</b>  <b>Application</b>  This Act binds the Crown in right of the Commonwealth, of a State and of the Northern Territory.</p>

<p>b on board a ship flying the flag of that Party; or</p> <p>c on board an aircraft registered under the laws of that Party; or</p> <p>d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.</p> <p>2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.</p> <p>3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.</p>	<p><b>SECT 4A</b>  <b>Application of the Criminal Code</b>  Chapter 2 of the <i>Criminal Code</i> applies to all offences against this Act.  Note: Chapter 2 of the <i>Criminal Code</i> sets out the general principles of criminal responsibility.</p> <p><b>Section 132 AB of the Copyright Act.</b>  <b>SECT 132AB</b>  <b>Geographical application</b>  (1) Subdivisions B, C, D, E and F apply only to acts done in Australia.  (2) This section has effect despite section 14.1 (Standard geographical jurisdiction) of the <i>Criminal Code</i> .</p>
<p><b>Chapter III – International co-operation</b></p>	
<p><b>Article 24 – Extradition</b></p> <p>1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.</p> <p>b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.</p> <p>2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be</p>	<p><b>For Art. 24(5) - Part II, Art. 12 of Extradition Act 1988 of Australia</b></p> <p><b>Art. 12- Provisional arrest warrants</b></p> <p>(1)Where:</p> <p>(a) an application is made, in the statutory form, on behalf of an extradition country to a magistrate for the issue of a warrant for the arrest of a person; and</p> <p>(b) the magistrate is satisfied, on the basis of information given by affidavit, that the person is an extraditable person in relation to the extradition country;</p> <p>the magistrate shall issue a warrant, in the statutory form, for the arrest of the person.</p> <p>(2)The magistrate shall forthwith send to the Attorney-General a report stating that the magistrate has issued the warrant, together with a copy of the affidavit.</p>



<p>concluded between or among them.</p> <p>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.</p> <p>4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.</p> <p>5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.</p> <p>6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.</p> <p>7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.</p> <p>b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure</p>	<p>(3)Where:</p> <ul style="list-style-type: none"> <li>(a) the Attorney-General has received the report under subsection (2) or has otherwise become aware of the issue of the warrant;</li> <li>(b) the person has not been arrested under the warrant; and</li> <li>(c) either: <ul style="list-style-type: none"> <li>(i) the Attorney-General decides not to issue a notice under subsection 16(1) in relation to the person; or</li> <li>(ii) the Attorney-General considers for any other reason that the warrant should be cancelled;</li> </ul> </li> </ul> <p>the Attorney-General shall, by notice in writing in the statutory form, direct a magistrate to cancel the warrant.</p>
<p><b>Article 25 – General principles relating to mutual assistance</b></p> <p>1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.</p>	<p><b>For Art. 25(4)- Sec. 8 of Mutual Assistance in Criminal Matters Act 1987 of Australia Refusal of assistance</b></p> <p>(1) A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Attorney-General:</p> <ul style="list-style-type: none"> <li>(a) the request relates to the prosecution or punishment of a person for an</li> </ul>

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, a political offence; or

(b) there are substantial grounds for believing that the request has been made with a view to prosecuting or punishing a person for a political offence; or

(c) there are substantial grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, religion, nationality or political opinions; or

(d) the request relates to the prosecution or punishment of a person in respect of an act or omission that if it had occurred in Australia, would have constituted an offence under the military law of Australia but not also under the ordinary criminal law of Australia; or

(e) the granting of the request would prejudice the sovereignty, security or national interest of Australia or the essential interests of a State or Territory; or

(f) the request relates to the prosecution of a person for an offence in a case where the person has been acquitted or pardoned by a competent tribunal or authority in the foreign country, or has undergone the punishment provided by the law of that country, in respect of that offence or of another offence constituted by the same act or omission as that offence.

(1A) A request by a foreign country for assistance under this Act must be refused if it relates to the prosecution or punishment of a person charged with, or convicted of, an offence in respect of which the death penalty may be imposed in the foreign country, unless the Attorney-General is of the opinion, having regard to the special circumstances of the case, that the assistance requested should be granted.

(1B) A request by a foreign country for assistance under this Act may be refused if the Attorney-General:

(a) believes that the provision of the assistance may result in the death

	<p>penalty being imposed on a person; and</p> <p>(b) after taking into consideration the interests of international criminal co-operation, is of the opinion that in the circumstances of the case the request should not be granted.</p> <p>(2) A request by a foreign country for assistance under this Act may be refused if, in the opinion of the Attorney-General:</p> <p>(a) the request relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Australia, would not have constituted an offence against Australian law; or</p> <p>(b) the request relates to the prosecution or punishment of a person in respect of an act or omission that occurred, or is alleged to have occurred, outside the foreign country and a similar act or omission occurring outside Australia in similar circumstances would not have constituted an offence against Australian law; or</p> <p>(c) the request relates to the prosecution or punishment of a person in respect of an act or omission where, if it had occurred in Australia at the same time and had constituted an offence against Australian law, the person responsible could no longer be prosecuted by reason of lapse of time or any other reason; or</p> <p>(d) the provision of the assistance could prejudice an investigation or proceeding in relation to a criminal matter in Australia; or</p> <p>(e) the provision of the assistance would, or would be likely to, prejudice the safety of any person (whether in or outside Australia); or</p> <p>(f) the provision of the assistance would impose an excessive burden on the resources of the Commonwealth or of a State or Territory; or</p> <p>(g) it is appropriate, in all the circumstances of the case, that the assistance requested should not be granted.</p>
<p><b>Article 26 – Spontaneous information</b>  1 A Party may, within the limits of its domestic law and without prior</p>	

<p>request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	
<p><b>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</b></p> <p>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.</p> <p>b The central authorities shall communicate directly with each other;</p> <p>c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;</p> <p>d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.</p> <p>3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.</p>	<p><b>For. Art. 27(4-6)- Sec. 8 of Mutual Assistance in Criminal Matters Act 1987 of Australia</b></p> <p>.</p> <p><b>For Art. 25(4)- Sec. 8 of Mutual Assistance in Criminal Matters Act 1987 of Australia Refusal of assistance</b></p> <p>(1) A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Attorney-General:</p> <p>(a) the request relates to the prosecution or punishment of a person for an offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, a political offence; or</p> <p>(b) there are substantial grounds for believing that the request has been made with a view to prosecuting or punishing a person for a political offence; or</p> <p>(c) there are substantial grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of the person’s race, sex, religion, nationality or political opinions; or</p> <p>(d) the request relates to the prosecution or punishment of a person in respect of an act or omission that if it had occurred in Australia, would have constituted an offence under the military law of Australia but not also under</p>

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
- b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent

the ordinary criminal law of Australia; or

(e) the granting of the request would prejudice the sovereignty, security or national interest of Australia or the essential interests of a State or Territory; or

(f) the request relates to the prosecution of a person for an offence in a case where the person has been acquitted or pardoned by a competent tribunal or authority in the foreign country, or has undergone the punishment provided by the law of that country, in respect of that offence or of another offence constituted by the same act or omission as that offence.

(1A) A request by a foreign country for assistance under this Act must be refused if it relates to the prosecution or punishment of a person charged with, or convicted of, an offence in respect of which the death penalty may be imposed in the foreign country, unless the Attorney-General is of the opinion, having regard to the special circumstances of the case, that the assistance requested should be granted.

(1B) A request by a foreign country for assistance under this Act may be refused if the Attorney-General:

(a) believes that the provision of the assistance may result in the death penalty being imposed on a person; and

(b) after taking into consideration the interests of international criminal co-operation, is of the opinion that in the circumstances of the case the request should not be granted.

(2) A request by a foreign country for assistance under this Act may be refused if, in the opinion of the Attorney-General:

(a) the request relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Australia, would not have constituted an offence against Australian law; or

(b) the request relates to the prosecution or punishment of a person in respect of an act or omission that occurred, or is alleged to have occurred, outside the foreign country and a similar act or omission occurring outside

authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Australia in similar circumstances would not have constituted an offence against Australian law; or

(c) the request relates to the prosecution or punishment of a person in respect of an act or omission where, if it had occurred in Australia at the same time and had constituted an offence against Australian law, the person responsible could no longer be prosecuted by reason of lapse of time or any other reason; or

(d) the provision of the assistance could prejudice an investigation or proceeding in relation to a criminal matter in Australia; or

(e) the provision of the assistance would, or would be likely to, prejudice the safety of any person (whether in or outside Australia); or

(f) the provision of the assistance would impose an excessive burden on the resources of the Commonwealth or of a State or Territory; or

(g) it is appropriate, in all the circumstances of the case, that the assistance requested should not be granted.

**For Art. 27(2/a)- Sec. 10-11 of Mutual Assistance in Criminal Matters Act 1987 of Australia.**

**Sec.10- Request by Australia**

(1) A request for international assistance in a criminal matter that Australia is authorised to make under this Act may be made only by the Attorney-General.

(2) Subsection (1) does not prevent the Attorney-General on behalf of Australia from requesting international assistance in a criminal matter other than assistance of a kind that may be requested under this Act.

**Sec.11- Request by foreign country**

(1) A request by a foreign country for international assistance in a criminal matter may be made to the Attorney-General or a person authorised by the Attorney-General, in writing, to receive requests by foreign countries under this Act.

(2) A request must be in writing and must include or be accompanied by the

	<p>following information:</p> <ul style="list-style-type: none"> <li>(a) the name of the authority concerned with the criminal matter to which the request relates;</li> <li>(b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;</li> <li>(c) a description of the purpose of the request and of the nature of the assistance being sought;</li> <li>(d) any information that may assist in giving effect to the request.</li> </ul> <p>However, a failure to comply with this subsection is not a ground for refusing the request.</p> <p>(3) Where a request by a foreign country is made to a person authorised under subsection (1), the request shall be taken, for the purposes of this Act, to have been made to the Attorney-General.</p> <p>(4) If a foreign country makes a request to a court in Australia for international assistance in a criminal matter:</p> <ul style="list-style-type: none"> <li>(a) the court must refer the request to the Attorney-General; and</li> <li>(b) the request is then taken, for the purposes of this Act, to have been made to the Attorney-General.</li> </ul>
<p><b>Article 28 – Confidentiality and limitation on use</b></p> <p>1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:</p> <p>a kept confidential where the request for mutual legal assistance could</p>	

not be complied with in the absence of such condition, or  
b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

**Article 29 – Expedited preservation of stored computer data**

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:  
a the authority seeking the preservation;  
b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;  
c the stored computer data to be preserved and its relationship to the offence;  
d any available information identifying the custodian of the stored computer data or the location of the computer system;  
e the necessity of the preservation; and  
f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences



other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

#### **Article 30 – Expedited disclosure of preserved traffic data**

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

<p><b>Article 31 – Mutual assistance regarding accessing of stored computer data</b></p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <ul style="list-style-type: none"> <li>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</li> <li>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</li> </ul>	
<p><b>Article 32 – Trans-border access to stored computer data with consent or where publicly available</b></p> <p>A Party may, without the authorisation of another Party:</p> <ul style="list-style-type: none"> <li>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</li> <li>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</li> </ul>	
<p><b>Article 33 – Mutual assistance in the real-time collection of traffic data</b></p> <p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	
<p><b>Article 34 – Mutual assistance regarding the interception of content data</b></p>	

<p>The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	
<p><b>Article 35 – 24/7 Network</b></p> <p>1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:</p> <ul style="list-style-type: none"> <li>a the provision of technical advice;</li> <li>b the preservation of data pursuant to Articles 29 and 30;</li> <li>c the collection of evidence, the provision of legal information, and locating of suspects.</li> </ul> <p>2 a A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.</p> <p>b If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	
<p><b>Article 42 – Reservations</b></p> <p>By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.</p>	

## **General search and seizure powers of Part 1AA of the Crimes Act 1914 (Crimes Act).**

### **Part IAA—Search, information gathering, arrest and related powers**

#### **Division 1—Preliminary**

##### **3C Interpretation**

- (1) In this Part, unless the contrary intention appears:

*constable assisting*, in relation to a warrant, means:

- (a) a person who is a constable and who is assisting in executing the warrant; or
- (b) a person who is not a constable and who has been authorised by the relevant executing officer to assist in executing the warrant.

*data held in a computer* includes:

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

*emergency situation*, in relation to the execution of a warrant in relation to premises, means a situation that the executing officer or a constable assisting believes, on reasonable grounds, involves a serious and imminent threat to a person's life, health or safety that requires the executing officer and constables assisting to leave the premises.

*evidential material* means a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form.

*executing officer*, in relation to a warrant, means:

- (a) the constable named in the warrant by the issuing officer as being responsible for executing the warrant; or
- (b) if that constable does not intend to be present at the execution of the warrant—another constable whose name has been written in the warrant by the constable so named; or

- (c) another constable whose name has been written in the warrant by the constable last named in the warrant.

***frisk search*** means:

- (a) a search of a person conducted by quickly running the hands over the person's outer garments; and
- (b) an examination of anything worn or carried by the person that is conveniently and voluntarily removed by the person.

***issuing officer***, in relation to a warrant to search premises or a person or a warrant for arrest under this Part, means:

- (a) a magistrate; or
- (b) a justice of the peace or other person employed in a court of a State or Territory who is authorised to issue search warrants or warrants for arrest, as the case may be.

***magistrate***, in sections 3ZI, 3ZJ, 3ZK, 3ZN and 3ZQZB, has a meaning affected by section 3CA.

***offence*** means:

- (a) an offence against a law of the Commonwealth (other than the *Defence Force Discipline Act 1982*); or
- (b) an offence against a law of a Territory; or
- (c) a State offence that has a federal aspect.

***ordinary search*** means a search of a person or of articles in the possession of a person that may include:

- (a) requiring the person to remove his or her overcoat, coat or jacket and any gloves, shoes and hat; and
- (b) an examination of those items.

***police station*** includes:

- (a) a police station of a State or Territory; and
- (b) a building occupied by the Australian Federal Police.

***premises*** includes a place and a conveyance.

**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.

**seizable item** means anything that would present a danger to a person or that could be used to assist a person to escape from lawful custody.

**serious offence** means an offence:

- (a) that is punishable by imprisonment for 2 years or more; and
- (b) that is one of the following:
  - (i) a Commonwealth offence;
  - (ii) an offence against a law of a State that has a federal aspect;
  - (iii) an offence against a law of a Territory; and
- (c) that is not a serious terrorism offence.

**serious terrorism offence** means:

- (a) a terrorism offence (other than offence against section 102.8, Division 104 or Division 105 of the *Criminal Code*); or
- (b) an offence against a law of a State:
  - (i) that has a federal aspect; and
  - (ii) that has the characteristics of a terrorism offence (other than such an offence that has the characteristics of an offence against section 102.8, Division 104 or Division 105 of the *Criminal Code*); or
- (c) an offence against a law of a Territory that has the characteristics of a terrorism offence (other than such an offence that has the characteristics of an offence against section 102.8, Division 104 or Division 105 of the *Criminal Code*).

**strip search** means a search of a person or of articles in the possession of a person that may include:

- (a) requiring the person to remove all of his or her garments; and
- (b) an examination of the person's body (but not of the person's body cavities) and of those garments.

**warrant** means a warrant under this Part.

**warrant premises** means premises in relation to which a warrant is in force.

(2) A person referred to in paragraph (b) of the definition of *constable assisting* in subsection (1) must not take part in searching or arresting a person.

### **3CA Nature of functions of magistrate**

(1) A function of making an order conferred on a magistrate by section 3ZI, 3ZJ, 3ZK, 3ZN or 3ZQZB is conferred on the magistrate in a personal capacity and not as a court or a member of a court.

(2) Without limiting the generality of subsection (1), an order made by a magistrate under section 3ZI, 3ZJ, 3ZK, 3ZN or 3ZQZB has effect only by virtue of this Act and is not to be taken by implication to be made by a court.

(3) A magistrate performing a function of, or connected with, making an order under section 3ZI, 3ZJ, 3ZK, 3ZN or 3ZQZB has the same protection and immunity as if he or she were performing that function as, or as a member of, a court (being the court of which the magistrate is a member).

(4) The Governor-General may make arrangements with the Governor of a State, the Chief Minister of the Australian Capital Territory, the Administrator of the Northern Territory or the Administrator of Norfolk Island for the performance, by all or any of the persons who from time to time hold office as magistrates in that State or Territory, of the function of making orders under sections 3ZI, 3ZJ, 3ZK, 3ZN and 3ZQZB.

### **3D Application of Part**

(1) This Part is not intended to limit or exclude the operation of another law of the Commonwealth relating to:

- (a) the search of premises; or
- (b) arrest and related matters; or
- (c) the stopping, detaining or searching of conveyances or persons; or
- (d) the seizure of things; or
- (e) the requesting of information or documents from persons.

(2) To avoid any doubt, it is declared that even though another law of the Commonwealth provides power to do one or more of the things referred to in subsection (1), a similar power conferred by this Part may be used despite the existence of the power under the other law.

- (4) This Part is not intended to limit or exclude the operation of a law of a Territory relating to:
- (a) the search of premises; or
  - (b) arrest and related matters; or
  - (c) the stopping, detaining or searching of conveyances or persons; or
  - (d) the seizure of things; or
  - (e) the requesting of information or documents from persons;

in relation to offences against a law of that Territory.

- (5) This Part does not apply to the exercise by a constable of powers under the *Defence Force Discipline Act 1982*.

(6) The application of this Part in relation to State offences that have a federal aspect is not intended to limit or exclude the concurrent operation of any law of a State or of the Australian Capital Territory.

Note 1: Subsection 3(1) defines *State* to include the Northern Territory.

Note 2: Section 3AA has the effect that an offence against the law of the Australian Capital Territory is a State offence that has a federal aspect.



## **Division 2—Search warrants**

### **3E When search warrants can be issued**

(1) An issuing officer may issue a warrant to search premises if the officer is satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises.

(2) An issuing officer may issue a warrant authorising an ordinary search or a frisk search of a person if the officer is satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that the person has in his or her possession, or will within the next 72 hours have in his or her possession, any evidential material.

(3) If the person applying for the warrant suspects that, in executing the warrant, it will be necessary to use firearms, the person must state that suspicion, and the grounds for that suspicion, in the information.

(4) If the person applying for the warrant is a member or special member of the Australian Federal Police and has, at any time previously, applied for a warrant relating to the same person or premises the person must state particulars of those applications and their outcome in the information.

(5) If an issuing officer issues a warrant, the officer is to state in the warrant:

(a) the offence to which the warrant relates; and

(b) a description of the premises to which the warrant relates or the name or description of the person to whom it relates; and

(c) the kinds of evidential material that are to be searched for under the warrant; and

(d) the name of the constable who, unless he or she inserts the name of another constable in the warrant, is to be responsible for executing the warrant; and

(e) the time at which the warrant expires (see subsection (5A)); and

(f) whether the warrant may be executed at any time or only during particular hours.

(5A) The time stated in the warrant under paragraph 3E(5)(e) 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.

(6) The issuing officer is also to state, in a warrant in relation to premises:

(a) that the warrant authorises the seizure of a thing (other than evidential material of the kind referred to in paragraph (5)(c)) found at the premises in the course of the search that the executing officer or a constable assisting believes on reasonable grounds to be:

- (i) evidential material in relation to an offence to which the warrant relates; or
- (ii) a thing relevant to another offence that is an indictable offence; or
- (iii) evidential material (within the meaning of the *Proceeds of Crime Act 2002*) or tainted property (within the meaning of that Act);

if the executing officer or a constable assisting believes on reasonable grounds that seizure of the thing is necessary to prevent its concealment, loss or destruction or its use in committing an offence; and

(b) whether the warrant authorises an ordinary search or a frisk search of a person who is at or near the premises when the warrant is executed if the executing officer or a constable assisting suspects on reasonable grounds that the person has any evidential material or seizable items in his or her possession.

(7) The issuing officer is also to state, in a warrant in relation to a person:

(a) that the warrant authorises the seizure of a thing (other than evidential material of the kind referred to in paragraph (5)(c)) found, in the course of the search, on or in the possession of the person or in a recently used conveyance, being a thing that the executing officer or a constable assisting believes on reasonable grounds to be:

- (i) evidential material in relation to an offence to which the warrant relates; or
- (ii) a thing relevant to another offence that is an indictable offence; or
- (iii) evidential material (within the meaning of the *Proceeds of Crime Act 2002*) or tainted property (within the meaning of that Act);

if the executing officer or a constable assisting believes on reasonable grounds that seizure of the thing 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.

(8) Paragraph (5)(e) and subsection (5A) do not prevent the issue of successive warrants in relation to the same premises or person.

(9) If the application for the warrant is made under section 3R, this section (other than subsection (5A)) applies as if:

(a) subsections (1) and (2) referred to 48 hours rather than 72 hours; and

(b) paragraph (5)(e) required the issuing officer to state in the warrant the period for which the warrant is to remain in force, which must not be more than 48 hours.

(10) An issuing officer in New South Wales or the Australian Capital Territory may issue a warrant in relation to premises or a person in the Jervis Bay Territory.

(11) An issuing officer in a State or internal Territory may:

(a) issue a warrant in relation to premises or a person in that State or Territory; or

(b) issue a warrant in relation to premises or a person in an external Territory; or

(c) issue a warrant in relation to premises or a person in another State or internal Territory (including the Jervis Bay Territory) if he or she is satisfied that there are special circumstances that make the issue of the warrant appropriate; or

(d) issue a warrant in relation to a person wherever the person is in Australia or in an external Territory if he or she is satisfied that it is not possible to predict where the person may be.

### **3F The things that are authorised by a search warrant**

(1) A warrant that is in force in relation to premises authorises the executing officer or a constable assisting:

(a) to enter the warrant premises and, if the premises are a conveyance, to enter the conveyance, wherever it is; and

(b) to search for and record fingerprints found at the premises and to take samples of things found at the premises for forensic purposes; and

(c) to search the premises for the kinds of evidential material specified in the warrant, and to seize things of that kind found at the premises;  
and

(d) to seize other things found at the premises in the course of the search that the executing officer or a constable assisting believes on reasonable grounds to be:

(i) evidential material in relation to an offence to which the warrant relates; or

(ii) evidential material in relation to another offence that is an indictable offence; or

(iii) evidential material (within the meaning of the *Proceeds of Crime Act 2002*) or tainted property (within the meaning of that Act);

if the executing officer or a constable assisting believes on reasonable grounds that seizure of the things is necessary to prevent their concealment, loss or destruction or their use in committing an offence; and

(e) to seize other things found at the premises in the course of the search that the executing officer or a constable assisting believes on reasonable grounds to be seizable items; and

(f) if the warrant so allows—to conduct an ordinary search or a frisk search of a person at or near the premises if the executing officer or a constable assisting suspects on reasonable grounds that the person has any evidential material or seizable items in his or her possession.

(2) A warrant that is in force in relation to a person authorises the executing officer or a constable assisting:

(a) to search the person as specified in the warrant and things found in the possession of the person and any recently used conveyance for things of the kind specified in the warrant; and

(b) to:

- (i) seize things of that kind; or
- (ii) record fingerprints from things; or
- (iii) to take forensic samples from things;

found in the course of the search; and

(c) to seize other things found on or in the possession of the person or in the conveyance in the course of the search that the executing officer or a constable assisting believes on reasonable grounds to be:

- (i) evidential material in relation to an offence to which the warrant relates; or
- (ii) a thing relevant to another offence that is an indictable offence; or
- (iii) evidential material (within the meaning of the *Proceeds of Crime Act 2002*) or tainted property (within the meaning of that Act);

if the executing officer or a constable assisting believes on reasonable grounds that seizure of the things is necessary to prevent their concealment, loss or destruction or their use in committing an offence; and

(d) to seize other things found in the course of the search that the executing officer or a constable assisting believes on reasonable grounds to be seizable items.

(3) If the warrant states that it may be executed only during particular hours, the warrant must not be executed outside those hours.

(4) If the warrant authorises an ordinary search or a frisk search of a person, a search of the person different to that so authorised must not be done under the warrant.

### **3G Availability of assistance and use of force in executing a warrant**

In executing a warrant:

- (a) the executing officer may obtain such assistance; and
- (b) the executing officer, or a person who is a constable and who is assisting in executing the warrant may use such force against persons and things; and
- (c) a person who is not a constable and who has been authorised to assist in executing the warrant may use such force against things; as is necessary and reasonable in the circumstances.

### **3H Details of warrant to be given to occupier etc.**

(1) If a warrant in relation to premises is being executed and the occupier of the premises or another person who apparently represents the occupier is present at the premises, the executing officer or a constable assisting must make available to that person a copy of the warrant.

(2) If a warrant in relation to a person is being executed, the executing officer or a constable assisting must make available to that person a copy of the warrant.

(3) If a person is searched under a warrant in relation to premises, the executing officer or a constable assisting must show the person a copy of the warrant.

(4) The executing officer must identify himself or herself to the person at the premises or the person being searched, as the case may be.

(5) The copy of the warrant referred to in subsections (1) and (2) need not include the signature of the issuing officer or the seal of the relevant court.

### **3J Specific powers available to constables executing warrant**

(1) In executing a warrant in relation to premises, the executing officer or a constable assisting may:

- (a) for a purpose incidental to the execution of the warrant; or
- (b) if the occupier of the premises consents in writing;

take photographs (including video recordings) of the premises or of things at the premises.

(2) If a warrant in relation to premises is being executed, the executing officer and the constables assisting may, if the warrant is still in force, complete the execution of the warrant after all of them temporarily cease its execution and leave the premises:

- (a) for not more than one hour; or
- (aa) if there is an emergency situation, for not more than 12 hours or such longer period as allowed by an issuing officer under section 3JA;  
or
- (b) for a longer period if the occupier of the premises consents in writing.

(3) If:

- (a) the execution of a warrant is stopped by an order of a court; and
- (b) the order is later revoked or reversed on appeal; and
- (c) the warrant is still in force;

the execution of the warrant may be completed.

### **3JA Extension of time to re-enter premises in emergency situations**

- (1) If:
  - (a) a warrant in relation to premises is being executed; and
  - (b) there is an emergency situation; and
  - (c) the executing officer or a constable assisting believes on reasonable grounds that the executing officer and the constables assisting will not be able to return to the premises within the 12 hour period mentioned in paragraph 3J(2)(aa);

he or she may apply to an issuing officer for an extension of that period.

(2) Before making the application, the executing officer or a constable assisting must, if it is practicable to do so, give notice to the occupier of the premises of his or her intention to apply for an extension.

(3) If an application mentioned in subsection (1) has been made, an issuing officer may extend the period during which the executing officer and constables assisting may be away from the premises if:

- (a) the issuing officer is satisfied, by information on oath or affirmation, that there are exceptional circumstances that justify the extension; and
- (b) the extension would not result in the period ending after the expiry of the warrant.

### **3K Use of equipment to examine or process things**

#### *Equipment may be brought to warrant premises*

(1) The executing officer of a warrant in relation to premises, or constable assisting, may bring to the warrant premises any equipment reasonably necessary for the examination or processing of a thing found at the premises in order to determine whether it is a thing that may be seized under the warrant.

#### *Thing may be moved for examination or processing*

(2) A thing found at warrant premises, or a thing found during a search under a warrant that is in force in relation to a person, may be moved to another place for examination or processing in order to determine whether it may be seized under a warrant if:

- (a) both of the following apply:
  - (i) it is significantly more practicable to do so having regard to the timeliness and cost of examining or processing the thing at another place and the availability of expert assistance;
  - (ii) the executing officer or constable assisting suspects on reasonable grounds that the thing contains or constitutes evidential material; or
- (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.

*Notification of examination or processing and right to be present*

(3) If a thing is moved to another place for the purpose of examination or processing under subsection (2), the executing officer must, if it is practicable to do so:

(a) inform the person referred to in paragraph (2)(b) or (c) (as the case requires) of the address of the place and the time at which the examination or processing will be carried out; and

(b) allow that person or his or her representative to be present during the examination or processing.

(3AA) The executing officer need not comply with paragraph (3)(a) or (b) if he or she believes on reasonable grounds that to do so might:

(a) endanger the safety of a person; or

(b) prejudice an investigation or prosecution.

*Time limit on moving a thing*

(3A) The thing may be moved to another place for examination or processing for no longer than 14 days.

(3B) An executing officer may apply to an issuing officer for one or more extensions of that time if the executing officer believes on reasonable grounds that the thing cannot be examined or processed within 14 days or that time as previously extended.

(3C) The executing officer must give notice of the application to the person referred to in paragraph (2)(b) or (c) (as the case requires), and that person is entitled to be heard in relation to the application.

(3D) A single extension cannot exceed 7 days.

*Equipment at warrant premises may be operated*

(4) The executing officer of a warrant in relation to premises, or a constable assisting, may operate equipment already at the warrant premises to carry out the examination or processing of a thing found at the premises in order to determine whether it is a thing that may be seized under the warrant if the executing officer or constable believes on reasonable grounds that:

(a) the equipment is suitable for the examination or processing; and

(b) the examination or processing can be carried out without damage to the equipment or the thing.



### **3L Use of electronic equipment at premises**

(1) The executing officer of a warrant in relation to premises, or a constable assisting, may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she suspects on reasonable grounds that the data constitutes evidential material.

Note: A constable can obtain an order requiring a person with knowledge of a computer or computer system to provide assistance: see section 3LA.

(1A) If the executing officer or constable assisting suspects on reasonable grounds that any data accessed by operating the electronic equipment constitutes evidential material, he or she may:

(a) copy any or all of the data accessed by operating the electronic equipment to a disk, tape or other associated device brought to the premises; or

(b) if the occupier of the premises agrees in writing—copy any or all of the data accessed by operating the electronic equipment to a disk, tape or other associated device at the premises;

and take the device from the premises.

(1B) If:

(a) the executing officer or constable assisting takes the device from the premises; and

(b) the Commissioner is satisfied that the data is not required (or is no longer required) for a purpose mentioned in section 3ZQU or for other judicial or administrative review proceedings;

the Commissioner must arrange for:

(c) the removal of the data from any device in the control of the Australian Federal Police; and

(d) the destruction of any other reproduction of the data in the control of the Australian Federal Police.

(2) If the executing officer or a constable assisting, after operating the equipment, finds that evidential material is accessible by doing so, he or she may:

(a) seize the equipment and any disk, tape or other associated device; or

(b) if the material can, by using facilities at the premises, be put in documentary form—operate the facilities to put the material in that form and seize the documents so produced.

(3) A constable may seize equipment under paragraph (2)(a) only if:

(a) it is not practicable to copy the data as mentioned in subsection (1A) or to put the material in documentary form as mentioned in paragraph (2)(b); or

(b) possession by the occupier of the equipment could constitute an offence.

(4) If the executing officer or a constable assisting suspects on reasonable grounds that:

(a) evidential material may be accessible by operating electronic equipment at the premises; and

(b) expert assistance is required to operate the equipment; and

(c) if he or she does not take action under this subsection, the material may be destroyed, altered or otherwise interfered with;

he or she may do whatever is necessary to secure the equipment, whether by locking it up, placing a guard or otherwise.

(5) The executing officer or a constable assisting must give notice to the occupier of the premises of his or her intention to secure equipment and of the fact that the equipment may be secured for up to 24 hours.

(6) The equipment may be secured:

(a) for a period not exceeding 24 hours; or

(b) until the equipment has been operated by the expert;

whichever happens first.

(7) If the executing officer or a constable assisting believes on reasonable grounds that the expert assistance will not be available within 24 hours, he or she may apply to an issuing officer for an extension of that period.

(8) The executing officer or a constable assisting must give notice to the occupier of the premises of his or her intention to apply for an extension, and the occupier is entitled to be heard in relation to the application.

(9) The provisions of this Division relating to the issue of warrants apply, with such modifications as are necessary, to the issuing of an extension.

### **3LAA Use of electronic equipment at other place**

(1) If electronic equipment is moved to another place under subsection 3K(2), the executing officer or a constable assisting may operate the equipment to access data (including data held at another place).

(2) If the executing officer or constable assisting suspects on reasonable grounds that any data accessed by operating the electronic equipment constitutes evidential material, he or she 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 Commissioner is satisfied that the data is not required (or is no longer required) for a purpose mentioned in section 3ZQU or for other judicial or administrative review proceedings, the Commissioner must arrange for:

- (a) the removal of the data from any device in the control of the Australian Federal Police; and
- (b) the destruction of any other reproduction of the data in the control of the Australian Federal Police.

(4) If the executing officer or a constable assisting, after operating the equipment, finds that evidential material is accessible by doing so, he or she 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) A constable 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 3K(2)(a) or (b) (as the case requires), could constitute an offence.

**3LA Person with knowledge of a computer or a computer system to assist access etc.**

(1) A constable may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow a constable 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 on warrant premises; or
  - (ii) has been moved under subsection 3K(2) and is at a place for examination or processing; or
  - (iii) has been seized under this Division;
- (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 a constable:
  - (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 data storage device removed from warrant premises under subsection 3L(1A).

(2) The magistrate may grant the order if the magistrate is satisfied that:

- and
- (a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device;
  - (b) the specified person is:
    - (i) reasonably suspected of having committed the offence stated in the relevant warrant; 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, or accessible from, the computer or device.

- (3) If:
  - (a) the computer or data storage device that is the subject of the order is seized under this Division; and
  - (b) the order was granted on the basis of an application made before the seizure;

the order does not have effect on or after the seizure.

Note: An application for another order under this section relating to the computer or data storage device may be made after the seizure.

- (4) If the computer or data storage device is not on warrant premises, 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 magistrate as the conditions to which the requirement on the person to provide the information or assistance is subject.
- (5) A person commits an offence if the person fails to comply with the order.

Penalty for contravention of this subsection: Imprisonment for 2 years.

### **3LB Accessing data held on certain premises—notification to occupier of that premises**

- (1) If:
  - (a) data is accessed, in relation to a warrant, under subsection 3L(1) or 3LAA(1); and
  - (aa) either:
    - (i) if the warrant is in relation to premises—the data is held on premises other than the warrant premises; or
    - (ii) if the warrant is in relation to a person—the data is held on any premises; and
  - (b) it is practicable to notify the occupier of the premises on which the data is held that the data has been accessed under a warrant;

the executing officer must:

- (c) do so as soon as practicable; and
  - (d) if the executing officer has arranged, or intends to arrange, for continued access to the data under subsection 3L(1A) or (2) or 3LAA(2) or (4)—include that information in the notification.
- (2) A notification under subsection (1) must include sufficient information to allow the occupier of the premises on which the data is held to contact the executing officer.

### **3M Compensation for damage to electronic equipment**

- (1) This section applies if:
  - (a) as a result of equipment being operated as mentioned in section 3K, 3L or 3LAA:
    - (i) damage is caused to the equipment; or
    - (ii) damage is caused to data recorded on the equipment or data access to which was obtained from the operation of the equipment; or
    - (iii) programs associated with the use of the equipment, or with the use of the data, are damaged or corrupted; and
  - (b) the damage or corruption occurs because:
    - (i) insufficient care was exercised in selecting the person who was to operate the equipment; or
    - (ii) insufficient care was exercised by the person operating the equipment.
- (2) The Commonwealth must pay the owner of the equipment, or the user of the data or programs, such reasonable compensation for the damage or corruption as the Commonwealth and the owner or user agree on.
- (3) However, if the owner or user and the Commonwealth fail to agree, the owner or user may institute proceedings in a court of competent jurisdiction for such reasonable amount of compensation as the court determines.
- (4) In determining the amount of compensation payable, regard is to be had to whether any of the following persons, if they were available at the time, provided any appropriate warning or guidance on the operation of the equipment:
  - (a) if the equipment was operated under a warrant issued in relation to premises—the occupier of the premises, or the occupier’s employees or agents;
  - (b) if the equipment was operated under a warrant issued in relation to a person—that person, or that person’s agents.

- (5) Compensation is payable out of money appropriated by the Parliament.
- (6) For the purposes of subsection (1):

*damage*, in relation to data, includes damage by erasure of data or addition of other data.

### **3N Copies of seized things to be provided**

- (1) Subject to subsection (2), if a constable seizes, under a warrant relating to premises:
  - (a) a document, film, computer file or other thing that can be readily copied; or
  - (b) a storage device the information in which can be readily copied;

the constable must, if requested to do so by the occupier of the premises or another person who apparently represents the occupier and who is present when the warrant is executed, give a copy of the thing or the information to that person as soon as practicable after the seizure.

- (2) Subsection (1) does not apply if:
  - (a) the thing that has been seized was seized under subsection 3L(1A) or paragraph 3L(2)(b) or 3LAA(4)(b); or
  - (b) possession by the occupier of the document, film, computer file, thing or information could constitute an offence.

### **3P Occupier entitled to be present during search**

- (1) If a warrant in relation to premises is being executed and the occupier of the premises or another person who apparently represents the occupier is present at the premises, the person is, subject to Part IC, entitled to observe the search being conducted.
- (2) The right to observe the search being conducted ceases if the person impedes the search.
- (3) This section does not prevent 2 or more areas of the premises being searched at the same time.

### **3Q Receipts for things seized under warrant**

- (1) If a thing is seized under a warrant or moved under subsection 3K(2), the executing officer or a constable assisting must provide a receipt for the thing.

- (2) If 2 or more things are seized or moved, they may be covered in the one receipt.

### **3R Warrants by telephone or other electronic means**

- (1) A constable may make an application to an issuing officer for a warrant by telephone, telex, facsimile or other electronic means:
  - (a) in an urgent case; or
  - (b) if the delay that would occur if an application were made in person would frustrate the effective execution of the warrant.
- (2) The issuing officer:
  - (a) may require communication by voice to the extent that it is practicable in the circumstances; and
  - (b) may make a recording of the whole or any part of any such communication by voice.
- (3) An application under this section must include all information required to be provided in an ordinary application for a warrant, but the application may, if necessary, be made before the information is sworn.
- (4) If an application is made to an issuing officer under this section and the issuing officer, after considering the information and having received and considered such further information (if any) as the issuing officer required, is satisfied that:
  - (a) a warrant in the terms of the application should be issued urgently; or
  - (b) the delay that would occur if an application were made in person would frustrate the effective execution of the warrant;the issuing officer may complete and sign the same form of warrant that would be issued under section 3E.
- (5) If the issuing officer decides to issue the warrant, the issuing officer is to inform the applicant, by telephone, telex, facsimile or other electronic means, of the terms of the warrant and the day on which and the time at which it was signed.
- (6) The applicant must then complete a form of warrant in terms substantially corresponding to those given by the issuing officer, stating on the form the name of the issuing officer and the day on which and the time at which the warrant was signed.



(7) The applicant must, not later than the day after the day of expiry of the warrant or the day after the day on which the warrant was executed, whichever is the earlier, give or transmit to the issuing officer the form of warrant completed by the applicant and, if the information referred to in subsection (3) was not sworn, that information duly sworn.

(8) The issuing officer is to attach to the documents provided under subsection (7) the form of warrant completed by the issuing officer.

(9) If:

(a) it is material, in any proceedings, for a court to be satisfied that the exercise of a power under a warrant issued under this section was duly authorised; and

(b) the form of warrant signed by the issuing officer is not produced in evidence;

the court is to assume, unless the contrary is proved, that the exercise of the power was not duly authorised.

### **3S Restrictions on personal searches**

A warrant cannot authorise a strip search or a search of a person's body cavities.

## **Division 3—Stopping and searching conveyances**

### **3T Searches without warrant in emergency situations**

- (1) This section applies if a constable suspects, on reasonable grounds, that:
  - (a) a thing relevant to an indictable offence is in or on a conveyance; and
  - (b) it is necessary to exercise a power under subsection (2) in order to prevent the thing from being concealed, lost or destroyed; and
  - (c) it is necessary to exercise the power without the authority of a search warrant because the circumstances are serious and urgent.
- (2) The constable may:
  - (a) stop and detain the conveyance; and
  - (b) search the conveyance and any container in or on the conveyance, for the thing; and
  - (c) seize the thing if he or she finds it there.
- (3) If, in the course of searching for the thing, the constable finds another thing relevant to an indictable offence or a thing relevant to a summary offence, the constable may seize that thing if he or she suspects, on reasonable grounds, that:
  - (a) it is necessary to seize it in order to prevent its concealment, loss or destruction; and
  - (b) it is necessary to seize it without the authority of a search warrant because the circumstances are serious and urgent.
- (4) The constable must exercise his or her powers subject to section 3U.

### **3U How a constable exercises a power under section 3T**

When a constable exercises a power under section 3T in relation to a conveyance, he or she:

- (a) may use such assistance as is necessary; and

- (b) must search the conveyance in a public place or in some other place to which members of the public have ready access; and
  - (c) must not detain the conveyance for longer than is necessary and reasonable to search it and any container found in or on the conveyance;
- and
- (d) may use such force as is necessary and reasonable in the circumstances, but must not damage the conveyance or any container found in or on the conveyance by forcing open a part of the conveyance or container unless:
    - (i) the person (if any) apparently in charge of the conveyance has been given a reasonable opportunity to open that part or container; or
    - (ii) it is not possible to give that person such an opportunity.

## **Division 3A—Powers in relation to terrorist acts and terrorism offences**

### **Subdivision A—Definitions**

#### **3UA Definitions**

In this Division:

*Commonwealth place* means a Commonwealth place within the meaning of the *Commonwealth Places (Application of Laws) Act 1970*.

*police officer* means:

- (a) a member of the Australian Federal Police (within the meaning of the *Australian Federal Police Act 1979*); or
- (b) a special member (within the meaning of that Act); or
- (c) a member, however described, of a police force of a State or Territory.

*prescribed security zone* means a zone in respect of which a declaration under section 3UJ is in force.

*serious offence related item* means a thing that a police officer conducting a search under section 3UD reasonably suspects:

- (a) may be used in a serious offence; or
- (b) is connected with the preparation for, or the engagement of a person in, a serious offence; or
- (c) is evidence of, or relating to, a serious offence.

*terrorism related item* means a thing that a police officer conducting a search under section 3UD reasonably suspects:

- (a) may be used in a terrorist act; or
- (b) is connected with the preparation for, or the engagement of a person in, a terrorist act; or
- (c) is evidence of, or relating to, a terrorist act.

*vehicle* includes any means of transport (and, without limitation, includes a vessel and an aircraft).

## **Subdivision B—Powers**

### **3UB Application of Subdivision**

- (1) A police officer may exercise the powers under this Subdivision in relation to a person if:
  - (a) the person is in a Commonwealth place (other than a prescribed security zone) and the officer suspects on reasonable grounds that the person might have just committed, might be committing or might be about to commit, a terrorist act; or
  - (b) the person is in a Commonwealth place in a prescribed security zone.
- (2) This section does not limit the operation of section 3UEA.

### **3UC Requirement to provide name etc.**

- (1) A police officer may request the person to provide the officer with the following details:
    - (a) the person's name;
    - (b) the person's residential address;
    - (c) the person's reason for being in that particular Commonwealth place;
    - (d) evidence of the person's identity.
  - (2) If a police officer:
    - (a) makes a request under subsection (1); and
    - (b) informs the person:
      - (i) of the officer's authority to make the request; and
      - (ii) that it may be an offence not to comply with the request;
- the person commits an offence if:

- (c) the person fails to comply with the request; or
- (d) the person gives a name or address that is false in a material particular.

Penalty: 20 penalty units.

Note: A more serious offence of obstructing a Commonwealth public official may also apply (see section 149.1 of the *Criminal Code*).

- (3) Subsection (2) does not apply if the person has a reasonable excuse.

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

### **3UD Stopping and searching**

- (1) A police officer may:
  - (a) stop and detain the person for the purpose of conducting a search under paragraph (b); and
  - (b) conduct one of the following searches for a terrorism related item:
    - (i) an ordinary search or a frisk search of the person;
    - (ii) a search of any thing that is, or that the officer suspects on reasonable grounds to be, under the person's immediate control;
    - (iii) a search of any vehicle that is operated or occupied by the person;
    - (iv) a search of any thing that the person has, or that the officer suspects on reasonable grounds that the person has, brought into the Commonwealth place.

#### *Conditions relating to conduct of search of person*

- (2) A police officer who conducts a search of a person under this section must not use more force, or subject the person to greater indignity, than is reasonable and necessary in order to conduct the search.
- (3) A person must not be detained under this section for longer than is reasonably necessary for a search to be conducted under this section.

#### *Other conditions relating to conduct of search of person or thing*

- (4) In searching a thing (including a vehicle) under subsection (1), a police officer may use such force as is reasonable and necessary in the circumstances, but must not damage the thing by forcing it, or a part of it, open unless:

- (a) the person has been given a reasonable opportunity to open the thing or part of it; or
- (b) it is not possible to give that opportunity.

### **3UE Seizure of terrorism related items and serious offence related items**

If a police officer:

- (a) conducts a search under section 3UD; and
- (b) finds, in the course of the search, a thing that is:
  - (i) a terrorism related item; or
  - (ii) a serious offence related item;

the officer may seize the thing.

### **3UEA Emergency entry to premises without warrant**

- (1) A police officer may enter premises in accordance with this section if the police officer suspects, on reasonable grounds, that:

- (a) it is necessary to exercise a power under subsection (2) in order to prevent a thing that is on the premises from being used in connection with a terrorism offence; and

- (b) it is necessary to exercise the power without the authority of a search warrant because there is a serious and imminent threat to a person's life, health or safety.

- (2) The police officer may:

- (a) search the premises for the thing; and
  - (b) seize the thing if he or she finds it there.

- (3) If, in the course of searching for the thing, the police officer finds another thing that the police officer suspects, on reasonable grounds, to be relevant to an indictable offence or a summary offence, the police officer may secure the premises pending the obtaining of a warrant under Part IAA in relation to the premises.

- (4) Premises must not be secured under subsection (3) for longer than is reasonably necessary to obtain the warrant.
- (5) In the course of searching for the thing, the police officer may also seize any other thing, or do anything to make the premises safe, if the police officer suspects, on reasonable grounds, that it is necessary to do so:
  - (a) in order to protect a person's life, health or safety; and
  - (b) without the authority of a search warrant because the circumstances are serious and urgent.
- (6) In exercising powers under this section:
  - (a) the police officer may use such assistance; and
  - (b) the police officer, or a person who is also a police officer and who is assisting the police officer, may use such force against persons and things; and
  - (c) a person (other than a police officer) who is authorised by the police officer to assist the police officer may use such force against things; as is necessary and reasonable in the circumstances.

*Notification*

- (7) If one or more police officers have entered premises in accordance with this section, a police officer must, within 24 hours after the entry:
  - (a) notify the occupier of the premises that the entry has taken place; or
  - (b) if it is not practicable so to notify the occupier—leave a written notice of the entry at the premises.

**3UF Seizure notices**

*Seizure notice to be served*

- (1) A police officer who is for the time being responsible for a thing seized under section 3UE or 3UEA must, within 7 days after the day on which the thing was seized, serve a seizure notice on:



- (a) the owner of the thing; or
- (b) if the owner of the thing cannot be identified after reasonable inquiries—the person from whom the thing was seized.
- (2) Subsection (1) does not apply if:
  - (a) both:
    - (i) the owner of the thing cannot be identified after reasonable inquiries; and
    - (ii) the thing was not seized from a person; or
  - (b) it is not possible to serve the person required to be served under subsection (1).
- (3) A seizure notice must:
  - (a) identify the thing; and
  - (b) state the date on which the thing was seized; and
  - (c) state the ground or grounds on which the thing was seized; and
  - (d) state that, if the owner does not request the return of the thing within 90 days after the date of the notice, the thing is forfeited to the Commonwealth.

*Forfeiture of thing seized*

- (8) A thing is forfeited to the Commonwealth if the owner of the thing does not request its return:
  - (a) before the end of the 90th day after the date of the seizure notice in relation to the thing; or
  - (b) if subsection (2) applied in relation to the thing so that a seizure notice was not served—before the end of the 90th day after the day on which the thing was seized.

**3UH Relationship of Subdivision to other laws**

- (1) The powers conferred, and duties imposed, by this Subdivision on police officers are in addition to, and not in derogation of, any other powers conferred, or duties imposed, by any other law of the Commonwealth or the law of a State or Territory.

(2) This Division is not intended to exclude or limit the operation of any other law of the Commonwealth or the law of a State or Territory in so far as it is capable of operating concurrently with this Subdivision.

## **Subdivision C—Prescribed security zones**

### **3UI Applications for declarations**

A police officer may apply to the Minister for a declaration that a Commonwealth place be declared as a prescribed security zone.

### **3UJ Minister may make declarations**

#### *Declaration*

(1) The Minister may declare, in writing, a Commonwealth place to be a prescribed security zone if he or she considers that a declaration would assist:

- (a) in preventing a terrorist act occurring; or
- (b) in responding to a terrorist act that has occurred.

#### *Declaration has effect*

(2) A declaration under this section has effect accordingly.

#### *Duration of declaration*

(3) A declaration ceases to have effect at the end of 28 days after it is made, unless the declaration is revoked by the Minister before then.

#### *Revocation of declaration*

(4) The Minister must revoke a declaration, in writing, if he or she is satisfied that:

(a) in the case of a declaration made on the ground mentioned in paragraph (1)(a)—there is no longer a terrorism threat that justifies the declaration being continued; or

(b) in the case of a declaration made on the ground mentioned in paragraph (1)(b)—the declaration is no longer required.

*Gazettal and publication of declaration*

- (5) If a declaration of a Commonwealth place as a prescribed security zone under this section is made or revoked, the Minister must arrange for:
- (a) a statement to be prepared that:
    - (i) states that the declaration has been made or revoked, as the case may be; and
    - (ii) identifies the prescribed security zone; and
  - (b) the statement to be:
    - (i) broadcast by a television or radio station so as to be capable of being received within the place; and
    - (ii) published in the *Gazette*; and
    - (iii) published on the internet.

*Effect of failure to publish*

- (6) A failure to comply with subsection (5) does not make the declaration or its revocation ineffective to any extent.

*Declaration or revocation not legislative instruments*

- (7) A declaration or revocation made under this section is not a legislative instrument.

**Subdivision D—Sunset provision**

**3UK Sunset provision**

- (1) A police officer must not exercise powers or perform duties under this Division (other than under section 3UF) after the end of 10 years after the day on which the Division commences.
- (2) A declaration under section 3UJ that is in force at the end of 10 years after the day on which this Division commences ceases to be in force at that time.
- (3) A police officer cannot apply for, and the Minister cannot make, a declaration under section 3UJ after the end of 10 years after the day on which this Division commences.

## Division 4—Arrest and related matters

### 3V Requirement to furnish name etc.

(1) If a constable believes on reasonable grounds that a person whose name or address is, or whose name and address are, unknown to the constable may be able to assist the constable in inquiries in relation to an indictable offence that the constable has reason to believe has been or may have been committed, the constable may request the person to provide his or her name or address, or name and address, to the constable.

(2) If a constable:

- (a) makes a request of a person under subsection (1); and
- (b) informs the person of the reason for the request; and
- (c) complies with subsection (3) if the person makes a request under that subsection;

the person must not:

- (d) refuse or fail to comply with the request; or
  - (e) give a name or address that is false in a material particular.
- (2A) Subsection (2) does not apply if the person has a reasonable excuse.

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

(3) If a constable who makes a request of a person under subsection (1) is requested by the person to provide to the person:

- (a) his or her name or the address of his or her place of duty; or
- (b) his or her name and that address; or
- (c) if he or she is not in uniform and it is practicable for the constable to provide the evidence—evidence that he or she is a constable;

the constable must not:

- (d) refuse or fail to comply with the request; or
- (e) give a name or address that is false in a material particular.

Penalty: 5 penalty units.

### **3W Power of arrest without warrant by constables**

- (1) A constable may, without warrant, arrest a person for an offence if the constable believes on reasonable grounds that:
  - (a) the person has committed or is committing the offence; and
  - (b) proceedings by summons against the person would not achieve one or more of the following purposes:
    - (i) ensuring the appearance of the person before a court in respect of the offence;
    - (ii) preventing a repetition or continuation of the offence or the commission of another offence;
    - (iii) preventing the concealment, loss or destruction of evidence relating to the offence;
    - (iv) preventing harassment of, or interference with, a person who may be required to give evidence in proceedings in respect of the offence;
    - (v) preventing the fabrication of evidence in respect of the offence;
    - (vi) preserving the safety or welfare of the person.
- (2) If:
  - (a) a person has been arrested for an offence under subsection (1); and
  - (b) before the person is charged with the offence, the constable in charge of the investigation ceases to believe on reasonable grounds:
    - (i) that the person committed the offence; or
    - (ii) that holding the person in custody is necessary to achieve a purpose referred to in paragraph (1)(b);

the person must be released.

(3) A constable may, without warrant, arrest a person whom he or she believes on reasonable grounds has escaped from lawful custody to which the person is still liable in respect of an offence.

### **3X Arrest of prisoner unlawfully at large**

- (1) A constable may, without warrant, arrest a person whom the constable believes on reasonable grounds to be a prisoner unlawfully at large.
- (2) The constable must, as soon as practicable, take the person before a Magistrate.
- (3) If the Magistrate is satisfied that the person is a prisoner unlawfully at large, the Magistrate may issue a warrant:
  - (a) authorising any constable to convey the person to a prison or other place of detention specified in the warrant; and
  - (b) directing that the person, having been conveyed to that place in accordance with the warrant, be detained there to undergo the term of imprisonment or other detention that the person is required by law to undergo.
- (4) In this section:

*prisoner unlawfully at large* means a person who is at large (otherwise than because the person has escaped from lawful custody) at a time when the person is required by law to be detained under a provision of a law of the Commonwealth, including Divisions 6 to 9, inclusive, of Part IB.

### **3Y Power of arrest without warrant of person on bail**

- (1) A constable may, without warrant, arrest a person who has been released on bail if the constable believes on reasonable grounds that the person has contravened or is about to contravene a condition of a recognisance on which bail was granted to the person in respect of an offence, even though the condition was imposed in a State or Territory other than the one in which the person is.
- (2) Subject to subsection (3), if a constable arrests a person under subsection (1), the constable must cause the person to be brought before a magistrate as soon as is practicable.
- (3) If a constable arrests a person under subsection (1) in the State or Territory in which the condition was imposed, the person is to be dealt with according to relevant laws of that State or Territory applied by section 68 of the *Judiciary Act 1903*.
- (4) When a person arrested under subsection (1) in a State or Territory other than the one in which the condition was imposed is brought before a magistrate in the State or Territory in which the arrest took place, the court may:
  - (a) release the person unconditionally; or

- (b) admit the person to bail on such recognisances as the court thinks fit to appear again before the same court at such time as the court orders; or
- (c) if the condition was not imposed by the Federal Court of Australia—remand the person in custody for a reasonable time pending the obtaining of a warrant for the apprehension of the person from the State or Territory in which the condition was imposed; or
- (d) if the condition was imposed by the Federal Court of Australia—remand the person in custody for a reasonable time pending the obtaining of a warrant for the apprehension of the person from that Court.
- (5) A release referred to in paragraph (4)(a) does not affect the operation of the bail order or the conditions of the bail imposed in the other State or Territory.

### **3Z Power of arrest without warrant by other persons**

- (1) A person who is not a constable may, without warrant, arrest another person if he or she believes on reasonable grounds that:
  - (a) the other person is committing or has just committed an indictable offence; and
  - (b) proceedings by summons against the other person would not achieve one or more of the purposes referred to in paragraph 3W(1)(b).
- (2) A person who arrests another person under subsection (1) must, as soon as practicable after the arrest, arrange for the other person, and any property found on the other person, to be delivered into the custody of a constable.

### **3ZA Warrants for arrest**

- (1) An issuing officer must not, under a law of a State or Territory applied by section 68 of the *Judiciary Act 1903*, issue a warrant for the arrest of a person for an offence as a result of an information laid before the officer unless:
  - (a) the information is on oath; and
  - (b) except where the issuing officer is informed that the warrant is sought for the purpose of making a request for the extradition of a person from a foreign country—the informant has given the issuing officer an affidavit setting out the reasons why the warrant is sought, including:
    - (i) the reasons why it is believed that the person committed the offence; and
    - (ii) the reasons why it is claimed that proceedings by summons would not achieve one or more of the purposes set out in paragraph 3W(1)(b); and

(c) if the issuing officer has requested further information concerning the reasons for which the issue of the warrant is sought—that information has been provided to the officer; and

(d) the issuing officer is satisfied that there are reasonable grounds for the issue of the warrant.

(2) If an issuing officer issues such a warrant, the officer must write on the affidavit which of the reasons specified in the affidavit, and any other reasons, he or she has relied on as justifying the issue of the warrant.

### **3ZB Power to enter premises to arrest offender**

(1) Subject to subsection (3), if:

(a) a constable has, under a warrant, power to arrest a person for an offence; and

(b) the constable believes on reasonable grounds that the person is on any premises;

the constable may enter the premises, using such force as is necessary and reasonable in the circumstances, at any time of the day or night for the purpose of searching the premises for the person or arresting the person.

(2) Subject to subsection (3), if:

(a) a constable may, under section 3W, arrest a person without warrant for an offence; and

(b) the offence is an indictable offence; and

(c) the constable believes on reasonable grounds that the person is on any premises;

the constable may enter the premises, using such force as is necessary and reasonable in the circumstances, at any time of the day or night for the purpose of searching the premises for the person or arresting the person.

(3) A constable must not enter a dwelling house under subsection (1) or (2) at any time during the period commencing at 9 p.m. on a day and ending at 6 a.m. on the following day unless the constable believes on reasonable grounds that:

(a) it would not be practicable to arrest the person, either at the dwelling house or elsewhere, at another time; or

(b) it is necessary to do so in order to prevent the concealment, loss or destruction of evidence relating to the offence.



(4) In subsection (3):

*dwelling house* includes a conveyance, and a room in a hotel, motel, boarding house or club, in which people ordinarily retire for the night.

### **3ZC Use of force in making arrest**

(1) A person must not, in the course of arresting another person for an offence, use more force, or subject the other person to greater indignity, than is necessary and reasonable to make the arrest or to prevent the escape of the other person after the arrest.

(2) Without limiting the operation of subsection (1), a constable must not, in the course of arresting a person for an offence:

(a) do anything that is likely to cause the death of, or grievous bodily harm to, the person unless the constable believes on reasonable grounds that doing that thing is necessary to protect life or to prevent serious injury to another person (including the constable); or

(b) if the person is attempting to escape arrest by fleeing—do such a thing unless:

(i) the constable believes on reasonable grounds that doing that thing is necessary to protect life or to prevent serious injury to another person (including the constable); and

(ii) the person has, if practicable, been called on to surrender and the constable believes on reasonable grounds that the person cannot be apprehended in any other manner.

### **3ZD Persons to be informed of grounds of arrest**

(1) A person who arrests another person for an offence must inform the other person, at the time of the arrest, of the offence for which the other person is being arrested.

(2) It is sufficient if the other person is informed of the substance of the offence, and it is not necessary that this be done in language of a precise or technical nature.

(3) Subsection (1) does not apply to the arrest of the other person if:

(a) the other person should, in the circumstances, know the substance of the offence for which he or she is being arrested; or

(b) the other person's actions make it impracticable for the person making the arrest to inform the other person of the offence for which he or she is being arrested.

### **3ZE Power to conduct a frisk search of an arrested person**

A constable who arrests a person for an offence, or who is present at such an arrest, may, if the constable suspects on reasonable grounds that it is prudent to do so in order to ascertain whether the person is carrying any seizable items:

- (a) conduct a frisk search of the person at or soon after the time of arrest; and
- (b) seize any seizable items found as a result of the search.

### **3ZF Power to conduct an ordinary search of an arrested person**

A constable who arrests a person for an offence, or who is present at such an arrest, may, if the constable suspects on reasonable grounds that the person is carrying:

- (a) evidential material in relation to that or another offence; or
- (b) a seizable item;

conduct an ordinary search of the person at or soon after the time of arrest, and seize any such thing found as a result of the search.

### **3ZG Power to conduct search of arrested person's premises**

A constable who arrests a person at premises for an offence, or who is present at such an arrest, may seize things in plain view at those premises that the constable believes on reasonable grounds to be:

- (a) evidential material in relation to that or another offence; or
- (b) seizable items.

### **3ZH Power to conduct an ordinary search or a strip search**

- (1) If a person who has been arrested for an offence is brought to a police station, a constable may:
  - (a) if an ordinary search of the person has not been conducted—conduct an ordinary search of the person; or
  - (b) subject to this section, conduct a strip search of the person.

- (2) A strip search may be conducted if:
  - (a) a constable suspects on reasonable grounds that the person has in his or her possession:
    - (i) a seizable item; or
    - (ii) evidential material (other than forensic material as defined in Part ID) in relation to that or another offence; and
  - (b) the constable suspects on reasonable grounds that it is necessary to conduct a strip search of the person in order to recover that item or evidential material; and
  - (c) a constable of the rank of superintendent or higher has approved the conduct of the search.

(2A) If:

- (a) in the course of carrying out a strip search, the constable comes to believe on reasonable grounds that the carrying out of a forensic procedure would be likely to produce evidence relating to the offence for which the person has been arrested or any other offence; and
- (b) Part ID provides for the carrying out of such a forensic procedure;

the forensic procedure must not be carried out except in accordance with Part ID.

(2B) The conducting of a strip search may include taking photographs of evidential material found on the person, whether or not taking photographs is a forensic procedure provided for by Part ID.

(3) Subject to section 3ZI, a strip search may also be conducted if the person consents in writing.

(3A) Subsection (3) does not authorise the conduct of a strip search for the purpose of obtaining forensic material as defined in Part ID. Such a search must not be conducted except in accordance with Part ID.

(4) Subject to section 3ZI, a strip search may be conducted in the presence of a medical practitioner who may assist in the search.

(5) The approval may be obtained by telephone, telex, facsimile or other electronic means.

(6) A constable who gives or refuses to give an approval for the purposes of paragraph (2)(c) must make a record of the decision and of the reasons for the decision.

(7) Such force as is necessary and reasonable in the circumstances may be used to conduct a strip search under subsection (2).

- (8) Any item of a kind referred to in paragraph (2)(a) that is found during a strip search may be seized.

### **3ZI Rules for conduct of strip search**

- (1) A strip search:
- (a) must be conducted in a private area; and
  - (b) must be conducted by a constable who is of the same sex as the person being searched; and
  - (c) subject to subsections (3) and (4), must not be conducted in the presence or view of a person who is of the opposite sex to the person being searched; and
  - (d) must not be conducted in the presence or view of a person whose presence is not necessary for the purposes of the search; and
  - (e) must not be conducted on a person who is under 10; and
  - (f) if the person being searched is at least 10 but under 18, or is incapable of managing his or her affairs:
    - (i) may only be conducted if the person has been arrested and charged or if a magistrate orders that it be conducted; and
    - (ii) must be conducted in the presence of a parent or guardian of the person being searched or, if that is not acceptable to the person, in the presence of another person (other than a constable) who is capable of representing the interests of the person and who, as far as is practicable in the circumstances, is acceptable to the person; and
  - (g) must not involve a search of a person's body cavities; and
  - (h) must not involve the removal of more garments than the constable conducting the search believes on reasonable grounds to be necessary to determine whether the person has in his or her possession the item searched for or to establish the person's involvement in the offence; and
  - (i) must not involve more visual inspection than the constable believes on reasonable grounds to be necessary to establish the person's involvement in the offence.
- (2) In deciding whether to make an order referred to in paragraph (1)(f), the magistrate must have regard to:
- (a) the seriousness of the offence; and
  - (b) the age or any disability of the person; and

(c) such other matters as the magistrate thinks fit.

(3) A strip search may be conducted in the presence of a medical practitioner of the opposite sex to the person searched if a medical practitioner of the same sex as the person being searched is not available within a reasonable time.

(4) Paragraph (1)(c) does not apply to a parent, guardian or personal representative of the person being searched if the person being searched has no objection to the person being present.

(5) If any of a person's garments are seized as a result of a strip search, the person must be provided with adequate clothing.

### **3ZJ Taking fingerprints, recordings, samples of handwriting or photographs**

(1) In this section and in sections 3ZK and 3ZL:

*identification material*, in relation to a person, means prints of the person's hands, fingers, feet or toes, recordings of the person's voice, samples of the person's handwriting or photographs (including video recordings) of the person, but does not include tape recordings made for the purposes of section 23U or 23V.

(2) A constable must not:

(a) take identification material from a person who is in lawful custody in respect of an offence except in accordance with this section; or

(b) require any other person to submit to the taking of identification material, but nothing in this paragraph prevents such a person consenting to the taking of identification material.

(3) If a person is in lawful custody in respect of an offence, a constable who is of the rank of sergeant or higher or who is for the time being in charge of a police station may take identification material from the person, or cause identification material from the person to be taken, if:

(a) the person consents in writing; or

(b) the constable believes on reasonable grounds that it is necessary to do so to:

(i) establish who the person is; or

(ii) identify the person as the person who committed the offence; or

(iii) provide evidence of, or relating to, the offence; or

(ba) both of the following apply:

- (i) the identification material taken, or caused to be taken, is fingerprints or photographs (including video recordings) of the person;
- (ii) the offence is punishable by imprisonment for a period of 12 months or more; or

(c) the constable suspects on reasonable grounds that the person has committed another offence and the identification material is to be taken for the purpose of identifying the person as the person who committed the other offence or of providing evidence of, or relating to, the other offence.

(4) A constable may use such force as is necessary and reasonable in the circumstances to take identification material from a person under this section.

(5) Subject to subsection (9), a constable must not take identification material from a person who is under 10.

(6) Subject to this section, a constable must not take identification material (other than hand prints, finger prints, foot prints or toe prints) from a suspect who:

- (a) is at least 10 but under 18, or is incapable of managing his or her affairs; and
- (b) has not been arrested and charged;

unless a magistrate orders that the material be taken.

(6A) A constable must not take hand prints, finger prints, foot prints or toe prints from a suspect who:

- (a) is at least 10 but under 18, or is incapable of managing his or her affairs; and
- (b) has not been arrested and charged;

except in accordance with Part ID.

(7) In deciding whether to make such an order, the magistrate must have regard to:

- (a) the seriousness of the offence; and
- (b) the age or any disability of the person; and
- (c) such other matters as the magistrate thinks fit.

(8) The taking of identification material from a person who:

- (a) is under 18; or
- (b) is incapable of managing his or her affairs;

must be done in the presence of:

- (c) a parent or guardian of the person; or
- (d) if the parent or guardian of the person is not acceptable to the person, another person (other than a constable) who is capable of representing the interests of the person and who, as far as is practicable in the circumstances, is acceptable to the person.

(9) Despite this section, identification material may be taken from a person who:

- (a) is not a suspect; and
- (b) is under 10 or is incapable of managing his or her affairs;

if a magistrate orders that the material be taken.

(10) Despite this section, identification material may be taken from a person who:

- (a) is not a suspect; and
- (b) is at least 10 but under 18; and
- (c) is capable of managing his or her affairs;

if one of the following paragraphs applies:

(d) the person agrees in writing to the taking of the material and a parent or guardian of the person also agrees in writing or, if a parent or guardian is not acceptable to the person, another person (other than a constable) who is capable of representing the interests of the person and who, as far as is practicable in the circumstances, is acceptable to the person also agrees in writing;

(e) if:

- (i) one of those persons agrees in writing to the taking of the material but the other does not; and
- (ii) a magistrate orders that the material be taken.

- (11) In deciding whether to make such an order, the magistrate must have regard to the matters set out in subsection (7).
- (12) Despite this section, identification material may be taken from a person who:
  - (a) is at least 18; and
  - (b) is capable of managing his or her affairs; and
  - (c) is not a suspect;

if the person consents in writing.

### **3ZK Destruction of identification material**

- (1) If:
  - (a) identification material has been taken from a person under section 3ZJ; and
  - (b) a period of 12 months has elapsed since the identification material was taken; and
  - (c) proceedings in respect of an offence to which the investigation material relates have not been instituted or have been discontinued;

the identification material must be destroyed as soon as practicable.

- (2) If identification material has been taken from a person under section 3ZJ and:
  - (a) the person is found to have committed an offence to which the identification material relates but no conviction is recorded; or
  - (b) the person is acquitted of such an offence and:
    - (i) no appeal is lodged against the acquittal; or
    - (ii) an appeal is lodged against the acquittal and the acquittal is confirmed or the appeal is withdrawn;

the identification material must be destroyed as soon as practicable unless an investigation into, or a proceeding against the person for, another offence to which the identification material relates is pending.



(3) A magistrate may, on application by a constable, extend the period of 12 months referred to in subsection (1) or that period as previously extended under this subsection in relation to particular identification material if the magistrate is satisfied that there are special reasons for doing so.

### **3ZL Offence of refusing to allow identification material to be taken**

- (1) If a person is convicted of an offence, the judge or magistrate presiding at the proceedings at which the person was convicted may order:
- (a) the person to attend a police station; or
  - (b) that a constable be permitted to attend on the person in a place of detention;

within one month after the conviction to allow impressions of the person's fingerprints and/or or a photograph of the person to be taken in accordance with the order.

- (2) A person must not refuse or fail to allow those impressions or a photograph of the person to be taken.

Penalty: Imprisonment for 12 months.

- (3) Subsection (2) does not apply if the person has a reasonable excuse.

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

(3A) The judge or magistrate may also make any other orders that are reasonably necessary for ensuring that the impressions of the person's fingerprints and/or a photograph of the person are taken in accordance with the order under subsection (1). For example, the judge or magistrate may order the person to attend a specified police station at a specified time.

- (3B) A person commits an offence if:
- (a) the person is subject to an order under subsection (3A); and
  - (b) the person engages in conduct; and
  - (c) the person's conduct contravenes the order.

Penalty: Imprisonment for 12 months.

- (3C) In this section:

*engage in conduct* means:

- (a) do an act; or
- (b) omit to perform an act.

(4) Nothing in this section derogates from the right to use the provisions of Part ID as authority for the taking of fingerprints from a prescribed offender or a serious offender.

- (5) In subsection (4), *prescribed offender* and *serious offender* have the meanings given in subsection 23WA(1).

### **3ZM Identification parades**

(1) This section applies to identification parades held in relation to offences.

(2) Subject to subsection (3) and to section 3ZN, an identification parade:

- (a) may be held if the suspect agrees; or
- (b) must be held if:
  - (i) the suspect has requested that an identification parade be held; and
  - (ii) it is reasonable in the circumstances to do so.

(2A) Without limiting the matters that may be taken into account in determining whether it is reasonable in the circumstances to hold an identification parade, the following must be taken into account:

- (a) the kind of offence, and the gravity of the offence, concerned;
- (b) the likely importance in the circumstances of the evidence of identification;
- (c) the practicality of holding an identification parade, having regard, among other things:
  - (i) if the suspect fails to cooperate in the conduct of the parade—to the manner and extent of, and the reason (if any) for, the failure; and
  - (ii) in any case—to whether an identification was made at or about the time of the commission of the offence; and
- (d) the appropriateness of holding an identification parade, having regard, among other things, to the relationship (if any) between the suspect and the person who may make an identification at the identification parade.

- (3) An identification parade must not be held unless the suspect has been informed that:
  - (a) he or she is entitled to refuse to take part in the parade; and
  - (b) if he or she refuses to take part in the parade:
    - (i) evidence of the refusal may be given in later proceedings relating to an offence, for the purpose of explaining why an identification parade was not held; and
    - (ii) evidence may be given in such proceedings of any identification of the suspect by a witness as a result of having seen a photograph or having seen the suspect otherwise than during an identification parade; and
  - (c) in addition to any requirement under section 3ZN, a legal representative or other person of the suspect's choice may be present while the person is deciding whether to take part in the parade, and during the holding of the parade, if arrangements for that person to be present can be made within a reasonable time.
- (4) The giving of the information referred to in subsection (3) must be recorded by a video recording or an audio recording.
- (5) An identification parade must be arranged and conducted in a manner that will not unfairly prejudice the suspect.
- (6) Without limiting the intent of subsection (5), an identification parade must be arranged and conducted in accordance with the following rules:
  - (a) the parade must consist of at least 9 persons;
  - (b) each of the persons who is not the suspect must:
    - (i) resemble the suspect in age, height and general appearance; and
    - (ii) not have features that will be visible during the parade that are markedly different from those of the suspect as described by the witness before viewing the parade;
  - (c) unless it is impracticable for another constable to arrange or conduct the parade, no constable who has taken part in the investigation relating to the offence may take part in the arrangements for, or the conduct of, the parade;
  - (d) no person in the parade is to be dressed in a way that would obviously distinguish him or her from the other participants;
  - (e) if it is practicable to do so, numbers should be placed next to each participant in order to allow the witness to make an identification by indicating the number of the person identified;

- (f) the parade may take place so that the witness can view the parade without being seen if the witness requests that it take place in such a manner and:
  - (i) a legal representative or other person of the suspect's choice is present with the witness; or
  - (ii) the parade is recorded by a video recording;
- (g) nothing is to be done that suggests or is likely to suggest to a witness which member of the parade is the suspect;
- (h) if the witness so requests, members of the parade may be required to speak, move or adopt a specified posture but, if this happens, the witness must be reminded that the members of the parade have been chosen on the basis of physical appearance only;
- (i) the suspect may select where he or she wishes to stand in the parade;
- (j) if more than one witness is to view the parade:
  - (i) each witness must view the parade alone; and
  - (ii) the witnesses are not to communicate with each other at a time after arrangements for the parade have commenced and before each of them has viewed the parade; and
  - (iii) the suspect may change places in the parade after each viewing;
- (k) each witness must be told that:
  - (i) the suspect may not be in the parade; and
  - (ii) if he or she is unable to identify the suspect with reasonable certainty he or she must say so;
- (l) the parade must be recorded by a video recording if it is practicable to do so and, if that is done, a copy of the video recording must be made available to the suspect or his or her legal representative as soon as it is practicable to do so;
- (m) if the parade is not recorded by a video recording:
  - (i) the parade must be photographed in colour; and
  - (ii) a print of a photograph of the parade that is at least 250mm × 200mm in size must be made available to the suspect or his or her legal representative; and
  - (iii) the constable in charge of the parade must take all reasonable steps to record everything said and done at the parade and must make a copy of the record available to the suspect or his or her legal representative;
- (n) the suspect may have present during the holding of the parade a legal representative or other person of his or her choice if arrangements for that person to be present can be made within a reasonable time.

(7) Nothing in this Act affects the determination of the following questions:

- (a) whether or not evidence of a suspect having refused to take part in an identification parade is admissible;
- (b) if evidence of such a refusal is admissible, what inferences (if any) may be drawn by a court or jury from the refusal;
- (c) whether, after such a refusal, evidence of alternative methods of identification is admissible.

(8) If a witness is, under the supervision of a constable, to attempt to identify a suspect otherwise than during an identification parade, the constable must ensure that the attempted identification is done in a manner that is fair to the suspect.

### **3ZN Identification parades for suspects under 18 etc.**

(1) An identification parade must not be held for a suspect who is under 10.

(2) An identification parade must not be held for a suspect who is incapable of managing his or her affairs unless a magistrate orders that it be held.

(3) An identification parade must not be held for a suspect who:

- (a) is at least 10 but under 18; and
- (b) is capable of managing his or her affairs;

unless one of the following paragraphs applies:

(c) the suspect agrees to or requests in writing the holding of the parade and a parent or guardian of the suspect agrees in writing to the holding of the parade or, if the parent or guardian is not acceptable to the suspect, another person (other than a constable) who is capable of representing the interests of the suspect and who, as far as is practicable in the circumstances, is acceptable to the suspect agrees in writing to the holding of the parade;

(d) if:

- (i) one of those persons agrees in writing to the holding of the parade but the other does not; and
- (ii) a magistrate orders that the parade be held.

(4) In deciding whether to make such an order, the magistrate must have regard to:

- (a) the seriousness of the offence; and
- (b) the age or any disability of the person; and
- (c) such other matters as the magistrate thinks fit.

(5) An identification parade for a suspect who is under 18 or is incapable of managing his or her affairs must be held in the presence of:

- (a) a parent or guardian of the suspect; or
- (b) if the parent or guardian is not acceptable to the suspect, another person (other than a constable) who is capable of representing the interests of the suspect and who, as far as is practicable in the circumstances, is acceptable to the suspect.

### **3ZO Identification by means of photographs**

(1) If a suspect is in custody in respect of an offence or is otherwise available to take part in an identification parade, a constable investigating the offence must not show photographs, or composite pictures or pictures of a similar kind, to a witness for the purpose of establishing, or obtaining evidence of, the identity of the suspect unless:

- (a) the suspect has refused to take part in an identification parade; or
- (aa) the suspect's appearance has changed significantly since the offence was committed; or
- (b) the holding of an identification parade would be:
  - (i) unfair to the suspect; or
  - (ii) unreasonable in the circumstances.

(1A) Without limiting the matters that may be taken into account in determining whether it would be unreasonable in the circumstances to hold an identification parade, the following must be taken into account:

- (a) the kind of offence, and the gravity of the offence, concerned;
- (b) the likely importance in the circumstances of the evidence of identification;
- (c) the practicality of holding an identification parade, having regard, among other things:

- (i) if the suspect fails to cooperate in the conduct of the parade—to the manner and extent of, and the reason (if any) for, the failure; and
    - (ii) in any case—to whether an identification was made at or about the time of the commission of the offence; and
  - (d) the appropriateness of holding an identification parade, having regard, among other things, to the relationship (if any) between the suspect and the person who may make an identification at the identification parade.
- (2) If a constable investigating an offence shows photographs or pictures to a witness for the purpose of establishing, or obtaining evidence of, the identity of a suspect, whether or not the suspect is in custody, the following rules apply:
- (a) the constable must show to the witness photographs or pictures of at least 9 different persons;
  - (b) each photograph or picture of a person who is not the suspect must be of a person who:
    - (i) resembles the suspect in age and general appearance; and
    - (ii) does not have features visible in the photograph or picture that are markedly different from those of the suspect as described by the witness before viewing the photographs or pictures;
  - (ba) the photographs or pictures shown to the witness must not suggest that they are photographs or pictures of persons in police custody;
  - (c) the constable must not, in doing so, act unfairly towards the suspect or suggest to the witness that a particular photograph or picture is the photograph or picture of the suspect or of a person who is being sought by the police in respect of an offence;
  - (d) if practicable, the photograph or picture of the suspect must have been taken or made after he or she was arrested or was considered as a suspect;
  - (e) the witness must be told that a photograph or picture of the suspect may not be amongst those being seen by the witness;
  - (f) the constable must keep, or cause to be kept, a record identifying each photograph or picture that is shown to the witness;
  - (g) the constable must notify the suspect or his or her legal representative in writing that a copy of the record is available for the suspect;
  - (h) the constable must retain the photographs or pictures shown, and must allow the suspect or his or her legal representative, upon application, an opportunity to inspect the photographs or pictures.
- (3) If:
- (a) a photograph or picture of a person who is suspected in relation to the commission of an offence is shown to a witness; and

- (b) the photograph was taken or the picture made after the suspect was arrested or was considered to be a suspect; and
- (c) proceedings in relation to the offence referred to in paragraph (a) or another offence arising out of the same course of conduct for which the photograph was taken or picture made are brought against the suspect before a jury; and
- (d) the photograph or picture is admitted into evidence;

the jury must be informed that the photograph was taken or the picture made after the suspect was arrested or was considered as a suspect.

(4) If a suspect is in custody in respect of an offence, a constable investigating the offence must not show a composite picture or a picture of a similar kind to a witness for the purpose of assisting the witness to describe the features of the suspect.

(5) If, after a constable investigating an offence has shown to a witness a composite picture or a picture of a similar kind for the purpose referred to in subsection (4):

- (a) a suspect comes into custody in respect of the offence; and
- (b) an identification parade is to be held in relation to the suspect;

the constable in charge of the investigation of the offence may, unless doing so would be unfair to the suspect or be unreasonable in the circumstances, request the witness to attend the identification parade and make the necessary arrangements for the witness to attend.

(6) If, after the witness has been shown a composite picture or a picture of a similar kind for the purpose referred to in subsection (4), a person is charged with the offence, the constable in charge of investigating the offence must, upon application by that person or his or her legal representative, provide him or her with particulars of any such picture shown to the witness and the comments (if any) of the witness concerning the picture.

(7) If a suspect is in custody in respect of an offence and a constable investigating the offence wishes to investigate the possibility that a person other than the suspect committed the offence, subsection (4) does not prevent a constable from taking action referred to in that subsection for the purpose of assisting a witness to describe the features of a person other than the suspect.



### **3ZP Identification procedures where there is more than one suspect**

If:

- (a) a constable is attempting to ascertain:
  - (i) which of 2 or more suspects committed an offence; or
  - (ii) the identities of 2 or more suspects who may have been jointly involved in an offence; and
- (b) for that purpose, the constable intends to conduct an identification parade or to identify a person by showing a photograph or a picture of a suspect to a person;

the constable must undertake a separate identification process for each of the suspects.

### **3ZQ Descriptions**

(1) If a description of a suspect is given to a constable in relation to an offence, the constable must ensure that a record of the description is made and that the record is retained until any proceedings in respect of the offence are completed.

(2) Subject to subsection (4), a constable must, if requested to do so by a person who has been charged with an offence, provide the person with the name of every person who, to the knowledge of the constable, claims to have seen, at or about the time of the commission of the offence, a person who is suspected of being involved in its commission.

(3) If:

- (a) a record of a description of a person is made under subsection (1); and
- (b) the person is charged with an offence to which the description relates;

a constable must notify the person or his or her legal representative in writing that a copy of the record, and of any other record of a description that the constable knows about of a person who is suspected of being involved in the commission of the offence, is available for the person.

- (4) If the constable suspects on reasonable grounds that providing the name of a person under subsection (2) could:
  - (a) place the person in danger; or

(b) expose the person to harassment or unreasonable interference;  
the constable is not required to provide the name of the person.

## **Division 4A—Determining a person’s age**

### **Subdivision A—Preliminary**

#### **3ZQA Definitions**

- (1) In this Division:

*age determination information* means a photograph (including an X-ray photograph) or any other record or information relating to a person that is obtained by carrying out a prescribed procedure.

*appropriately qualified*, in relation to the carrying out of a prescribed procedure, means:

- (a) having suitable professional qualifications or experience to carry out the prescribed procedure; or
- (b) qualified under the regulations to carry out the prescribed procedure.

*Commonwealth offence* means:

(a) an offence against a law of the Commonwealth, other than an offence that is a service offence for the purposes of the *Defence Force Discipline Act 1982*; or

- (b) a State offence that has a federal aspect.

*investigating official* means:

- (a) a member or special member of the Australian Federal Police; or
- (b) a member of the police force of a State or Territory; or
- (c) a person who holds an office the functions of which include the investigation of Commonwealth offences and who is empowered by a law of the Commonwealth because of the holding of that office to make arrests in respect of such offences.

*prescribed procedure* means a procedure specified by regulations made for the purposes of subsection (2) to be a prescribed procedure for determining a person’s age.

(2) The regulations may specify a particular procedure, which may include the taking of an X-ray of a part of a person's body, to be a prescribed procedure for determining a person's age.

(3) A procedure prescribed for the purposes of subsection (2):

(a) may involve the operation of particular equipment that is specified for the purpose; and

(b) must require that equipment to be operated by an appropriately qualified person.

(4) Before the Governor-General makes a regulation for the purposes of subsection (2), the Minister must consult with the Minister responsible for the administration of the *Therapeutic Goods Act 1989*.

### **Subdivision B—Determination of age during investigation**

#### **3ZQB Circumstances where investigating official may seek authority to carry out a prescribed procedure**

(1) If:

(a) an investigating official suspects, on reasonable grounds, that a person may have committed a Commonwealth offence; and

(b) it is necessary to determine whether or not the person is, or was, at the time of the alleged commission of the offence, under 18 because that question is relevant to the rules governing the person's detention, the investigation of the offence or the institution of criminal proceedings;

the investigating official may, whether or not the person is in custody at the time, arrange for the carrying out of a prescribed procedure in respect of the person only if:

(c) the investigating official obtains, in accordance with section 3ZQC, the requisite consents to the carrying out of the procedure in respect of the person; or

(d) a magistrate orders, on application by the investigating official, the carrying out of the procedure in respect of the person.

(2) An application to a magistrate by an investigating official for the purposes of paragraph (1)(d) may be made:

(a) in person; or

(b) by telephone, telex, fax or other electronic means.

- (3) In deciding whether to make such an order on application by an investigating official, the magistrate must be satisfied that:
- (a) there are reasonable grounds for the suspicion that the person has committed a Commonwealth offence; and
  - (b) there is uncertainty as to whether or not the person is, or was, at the time of the alleged commission of the offence, under 18; and
  - (c) the uncertainty will need to be resolved in order to determine the application of the rules governing the person's detention, the investigation of the offence or the institution of criminal proceedings.

### **3ZQC Obtaining of consents for the carrying out of a prescribed procedure**

- (1) For the purposes of paragraph 3ZQB(1)(c), an investigating official is taken to have obtained the requisite consents to the carrying out of a prescribed procedure in respect of a person if the following persons agree in writing to the carrying out of the procedure:
- (a) the person in respect of whom it is sought to carry out the procedure;
  - (b) either:
    - (i) a parent or guardian of the person; or
    - (ii) if a parent or guardian is not available or is not acceptable to the person—an independent adult person (other than an investigating official involved in the investigation of the person) who is capable of representing the interests of the person and who, as far as is practicable in the circumstances, is acceptable to the person.
- (2) Before seeking the consents referred to in subsection (1), an investigating official must first inform each of the persons from whom such a consent is being sought, in a language in which the person is able to communicate with reasonable fluency:
- (a) the purpose and reasons for which the prescribed procedure is to be carried out; and
  - (b) the nature of the procedure; and
  - (c) if the procedure involves the operation of particular equipment—the nature of that equipment; and
  - (d) that the information obtained from the carrying out of the procedure could affect the manner of dealing with the person on whom the procedure is to be carried out; and
  - (e) the known risks (if any) that would be posed to the health of the person on whom the procedure is to be carried out; and

- (ea) that the persons giving the requisite consent may withdraw that consent at any time; and
  - (f) that the seeking of the requisite consent and any giving of such consent was being, or would be, recorded; and
  - (g) that the persons giving the requisite consent are each entitled to a copy of that record; and
  - (h) that the person on whom the procedure is to be carried out may have, so far as is reasonably practicable, a person of his or her choice present while the procedure is carried out.
- (3) The requisite consents may be given:
- (a) in person; or
  - (b) by telephone, telex, fax or other electronic means.
- (4) Nothing in this section affects the rights of a person under Part IC, in particular a person's rights under:
- (a) section 23G (Right to communicate with friend, relative and legal practitioner); or
  - (b) section 23P (Right of foreign national to communicate with consular office).

### **3ZQD Withdrawal of consent**

If a person who has given consent to the carrying out of a prescribed procedure expressly withdraws consent to the carrying out of that procedure (or if the withdrawal of such consent can reasonably be inferred from the person's conduct) before or during the carrying out of the procedure, the carrying out of the procedure is not to proceed otherwise than by order of a magistrate on the application of an investigating official.

### **3ZQE Recording of giving of information about carrying out a prescribed procedure and relevant responses**

- (1) An investigating official must, if practicable, ensure that:
- (a) the giving of information about a prescribed procedure and the responses (if any) of the persons to whom the information is given are recorded by audio tape, video tape or other electronic means; and
  - (b) a copy of the record is made available to the person on whom it is sought to carry out the procedure.

(2) If recording the giving of information and the responses (if any) of the persons to whom the information is given in the manner referred to in subsection (1) is not practicable, the investigating official must ensure that:

- (a) a written record of the giving of the information and of the responses (if any) is made; and
- (b) a copy of the record is made available to the person on whom it is sought to carry out the procedure.

### **Subdivision C—Determination of age during proceedings**

#### **3ZQF Circumstances where judge or magistrate may order carrying out of a prescribed procedure on own initiative**

If:

- (a) a person is being prosecuted for a Commonwealth offence; and
- (b) the judge or magistrate presiding over the proceedings related to that offence is satisfied that it is necessary to ascertain whether or not the person is, or was, at the time of the alleged commission of that offence, under 18;

the judge or magistrate presiding may make an order requiring the carrying out of a prescribed procedure in respect of the person.

### **Subdivision D—Communication of orders by judges or magistrates**

#### **3ZQG Orders made by judges or magistrates concerning carrying out of a prescribed procedure**

(1) If a judge or a magistrate orders the carrying out of a prescribed procedure (whether as a result of a request by an investigating official or not), the judge or magistrate must:

- (a) ensure that a written record of the order, and of the reasons for the making of the order, is kept; and
- (b) ensure that the person on whom the procedure is to be carried out is told by an investigating official in a language in which the person is able to communicate with reasonable fluency:
  - (i) that an order for the carrying out of the procedure has been made and of the reasons for the making of the order; and
  - (ii) of the arrangements for the carrying out of the procedure; and
  - (iii) of the fact that reasonable force may be used to secure the compliance of the person to whom the order relates.

- (2) The judge or magistrate may give directions as to the time, place and manner in which the procedure is to be carried out.

### **Subdivision E—Matters relating to the carrying out of prescribed procedures**

#### **3ZQH Appropriate medical or other standards to be applied**

A prescribed procedure must be carried out in a manner consistent with either or both of the following:

- (a) appropriate medical standards;
- (b) appropriate other relevant professional standards.

#### **3ZQI Reasonable and necessary force**

Except where the carrying out of a prescribed procedure to determine a person's age is undertaken with the consent of that person and of an additional adult person in accordance with section 3ZQC, the person carrying out the procedure, and any person assisting that person, is entitled to use such force as is reasonable and necessary in the circumstances.

### **Subdivision F—Disclosure and destruction of age determination information**

#### **3ZQJ Disclosure of age determination information**

- (1) A person is guilty of an offence if:
  - (a) the person's conduct causes the disclosure of age determination information other than as provided by this section; and
  - (b) the person is reckless as to any such disclosure.

Penalty: Imprisonment for 2 years.

- (2) A person may only disclose age determination information:
  - (a) for a purpose related to establishing and complying with the rules governing:
    - (i) the detention of the person to whom the age determination information relates; or
    - (ii) the investigation of a Commonwealth offence by that person; or



- (iii) the institution of criminal proceedings against that person for a Commonwealth offence; or
- (b) for a purpose related to the conduct of:
  - (i) the investigation of the person to whom the age determination information relates for a Commonwealth offence; or
  - (ii) proceedings for a Commonwealth offence against that person; or
- (c) for the purpose of an investigation by the Information Commissioner of the Commonwealth or the Commonwealth Ombudsman; or
- (d) if the person to whom the age determination information relates consents in writing to the disclosure.

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

### **3ZQK Destruction of age determination information**

- (1) If, in relation to a Commonwealth offence:
  - (a) age determination information relating to a person has been obtained by carrying out a prescribed procedure; and
  - (b) 12 months have passed since the carrying out of the procedure; and
  - (c) proceedings in respect of the offence have not been instituted against the person from whom the information was taken or have discontinued;

the information must be destroyed as soon as practicable.

(2) If, in relation to a Commonwealth offence, age determination information relating to a person has been obtained by carrying out a prescribed procedure and:

- (a) the person is found to have committed the offence but no conviction is recorded; or
- (b) the person is acquitted of the offence and:
  - (i) no appeal is lodged against the acquittal; or
  - (ii) an appeal is lodged against the acquittal and the acquittal is confirmed or the appeal is withdrawn;

the information must be destroyed as soon as practicable unless an investigation into, or a proceeding against, the person for another Commonwealth offence is pending.

(3) A magistrate may, on application by an investigating official, extend the period of 12 months referred to in subsection (1), or that period as previously extended under this subsection in relation to the information, if the magistrate is satisfied that there are special reasons for doing so.

## **Division 4B—Power to obtain information and documents**

### **Subdivision A—Definitions**

#### **3ZQL Definitions**

In this Division:

*authorised AFP officer* means:

- (a) the Commissioner; or
- (b) a Deputy Commissioner; or
- (c) a senior executive AFP employee who:
  - (i) is a member of the Australian Federal Police; and
  - (ii) is authorised in writing by the Commissioner for the purposes of this paragraph.

*Federal Magistrate* has the meaning given by the *Federal Magistrates Act 1999*.

### **Subdivision B—Power to request information or documents about terrorist acts from operators of aircraft or ships**

#### **3ZQM Power to request information or documents about terrorist acts from operators of aircraft or ships**

(1) This section applies if an authorised AFP officer believes on reasonable grounds that an operator of an aircraft or ship has information or documents (including in electronic form) that are relevant to a matter that relates to the doing of a terrorist act (whether or not a terrorist act has occurred or will occur).

(2) The officer may:

- (a) ask the operator questions relating to the aircraft or ship, or its cargo, crew, passengers, stores or voyage, that are relevant to the matter;
- or

- (b) request the operator to produce documents relating to the aircraft or ship, or its cargo, crew, passengers, stores or voyage:
  - (i) that are relevant to the matter; and
  - (ii) that are in the possession or under the control of the operator.
- (3) A person who is asked a question or requested to produce a document under subsection (2) must answer the question or produce the document as soon as practicable.

*Offence*

- (4) A person commits an offence if:
  - (a) the person is an operator of an aircraft or ship; and
  - (b) the person is asked a question or requested to produce a document under subsection (2); and
  - (c) the person fails to answer the question or produce the document.

Penalty: 60 penalty units.

- (5) Subsection (4) is an offence of strict liability.

Note: For strict liability, see section 6.1 of the *Criminal Code*.

- (6) It is a defence to a prosecution for an offence against subsection (4) if the person charged had a reasonable excuse for:
  - (a) failing to answer the question; or
  - (b) failing to produce the document.

*Definitions*

- (7) In this section:

**operator** has the meaning given by section 4 of the *Customs Act 1901*.

## **Subdivision C—Power to obtain documents relating to serious terrorism and non-terrorism offences**

### **3ZQN Power to obtain documents relating to serious terrorism offences**

(1) This section applies if an authorised AFP officer considers on reasonable grounds that a person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious terrorism offence.

(2) The officer may give the person a written notice requiring the person to produce documents that:

- (a) relate to one or more of the matters set out in section 3ZQP, as specified in the notice; and
- (b) are in the possession or under the control of the person.

(3) The notice must:

- (a) specify the name of the person to whom the notice is given; and
- (b) specify the matters to which the documents to be produced relate; and
- (c) specify the manner in which the documents are to be produced; and
- (d) specify the place at which the documents are to be produced; and
- (e) state that the person must comply with the notice as soon as practicable; and
- (f) set out the effect of section 3ZQS (offence for failure to comply); and
- (g) if the notice specifies that information about the notice must not be disclosed—set out the effect of section 3ZQT (offence for disclosing existence or nature of a notice).

### **3ZQO Power to obtain documents relating to serious offences**

(1) An authorised AFP officer may apply to a Federal Magistrate for a notice under this section in respect of a person if the AFP officer considers on reasonable grounds that the person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious offence.

- (2) If the Magistrate is satisfied on the balance of probabilities, by information on oath or by affirmation, that:
- (a) the person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious offence; and
  - (b) giving the person a notice under this section is reasonably necessary, and reasonably appropriate and adapted, for the purpose of investigating the offence;

the Magistrate may give the person a written notice requiring the person to produce documents that:

- (c) relate to one or more of the matters set out in section 3ZQP, as specified in the notice; and
  - (d) are in the possession or under the control of the person.
- (3) The Magistrate must not give the notice unless the authorised AFP officer or some other person has given to the Magistrate, either orally or by affidavit, such further information (if any) as the Magistrate requires concerning the grounds on which the issue of the notice is being sought.
- (4) The notice must:
- (a) specify the name of the person to whom the notice is given; and
  - (b) specify the matters to which the documents to be produced relate; and
  - (c) specify the manner in which the documents are to be produced; and
  - (d) specify the place at which the documents are to be produced; and
  - (e) state that the person must comply with the notice within 14 days after the day on which the notice is given; and
  - (f) set out the effect of section 3ZQS (offence for failure to comply); and
  - (g) if the notice specifies that information about the notice must not be disclosed—set out the effect of section 3ZQT (offence for disclosing existence or nature of a notice).

### **3ZQP Matters to which documents must relate**

A document to be produced under a notice under section 3ZQN or 3ZQO must relate to one or more of the following matters:

- (a) determining whether an account is held by a specified person with a specified financial institution, and details relating to the account (including details of any related accounts);
- (b) determining whether a specified person is a signatory to an account with a specified financial institution, and details relating to the account (including details of any related accounts);
- (c) determining whether a transaction has been conducted by a specified financial institution on behalf of a specified person, and details relating to the transaction (including details relating to other parties to the transaction);
- (d) determining whether a specified person travelled or will travel between specified dates or specified locations, and details relating to the travel (including details relating to other persons travelling with the specified person);
- (e) determining whether assets have been transferred to or from a specified person between specified dates, and details relating to the transfers (including details relating to the names of any other persons to or from whom the assets were transferred);
- (f) determining whether an account is held by a specified person in respect of a specified utility (such as gas, water or electricity), and details relating to the account (including the names of any other persons who also hold the account);
- (g) determining who holds an account in respect of a specified utility (such as gas, water or electricity) at a specified place, and details relating to the account;
- (h) determining whether a telephone account is held by a specified person, and details relating to the account (including:
  - (i) details in respect of calls made to or from the relevant telephone number; or
  - (ii) the times at which such calls were made or received; or
  - (iii) the lengths of such calls; or
  - (iv) the telephone numbers to which such calls were made and from which such calls were received);
- (i) determining who holds a specified telephone account, and details relating to the account (including details mentioned in paragraph (h));
- (j) determining whether a specified person resides at a specified place;
- (k) determining who resides at a specified place.

### **3ZQQ Powers conferred on Federal Magistrates in their personal capacity**

- (1) A power conferred on a Federal Magistrate by section 3ZQO is conferred on the Magistrate in a personal capacity and not as a court or a member of a court.
- (2) A Federal Magistrate need not accept the power conferred.
- (3) A Federal Magistrate exercising a power conferred by section 3ZQO has the same protection and immunity as if he or she were exercising that power as, or as a member of, the court of which the Magistrate is a member.

### **3ZQR Documents must be produced**

- (1) A person is not excused from producing a document under section 3ZQN or 3ZQO on the ground that to do so:
  - (a) would contravene any other law; or
  - (b) might tend to incriminate the person or otherwise expose the person to a penalty or other liability; or
  - (c) would disclose material that is protected against disclosure by legal professional privilege or any other duty of confidence; or
  - (d) would be otherwise contrary to the public interest.
- (2) However, neither:
  - (a) the production of the document; nor
  - (b) any information, document or thing obtained as a direct or indirect consequence of producing the document;

is admissible in evidence against the person in proceedings other than proceedings for an offence against section 137.1, 137.2 or 149.1 of the *Criminal Code* that relates to this Act.

- (3) A person is not liable to any penalty by reason of his or her producing a document when required to do so under section 3ZQN or 3ZQO.
- (4) The fact that a person is not excused under subsection (1) from producing a document does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that document.



**3ZQS Offence for failure to comply with notice under section 3ZQN or 3ZQO**

A person commits an offence if:

- (a) the person is given a notice under section 3ZQN or 3ZQO; and
- (b) the person fails to comply with the notice.

Penalty: 30 penalty units.

**3ZQT Offence for disclosing existence or nature of notice**

(1) A person commits an offence if:

- (a) the person is given a notice under section 3ZQN or 3ZQO; and
- (b) the notice specifies that information about the notice must not be disclosed; and
- (c) the person discloses the existence or nature of the notice.

Penalty: 120 penalty units or imprisonment for 2 years, or both.

(2) Subsection (1) does not apply if:

- (a) the person discloses the information to another person in order to obtain a document that is required by the notice in order to comply with it, and that other person is directed not to inform the person to whom the document relates about the matter; or
- (b) the disclosure is made to obtain legal advice or legal representation in relation to the notice; or
- (c) the disclosure is made for the purposes of, or in the course of, legal proceedings.

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

## **Division 4C—Using, sharing and returning things seized and documents produced**

### **Subdivision A—Using and sharing things seized and documents produced**

#### **3ZQU Purposes for which things and documents may be used and shared**

*Use and sharing of thing or document by constable or Commonwealth officer*

(1) A constable or Commonwealth officer may use, or make available to another constable or Commonwealth officer to use, a thing seized under this Part, or the original or a copy of a document produced under Division 4B, for the purpose of any or all of the following if it is necessary to do so for that purpose:

- (a) preventing, investigating or prosecuting an offence;
- (b) proceedings under the *Proceeds of Crime Act 1987* or the *Proceeds of Crime Act 2002*;
- (c) proceedings under a corresponding law (within the meaning of either of the Acts mentioned in paragraph (b)) that relate to a State offence that has a federal aspect;
- (d) proceedings for the forfeiture of the thing under a law of the Commonwealth;
- (e) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, Division 104 or 105 of the *Criminal Code*;
- (f) investigating or resolving a complaint or an allegation of misconduct relating to an exercise of a power or the performance of a function or duty under this Part;
- (g) investigating or resolving an AFP conduct or practices issue (within the meaning of the *Australian Federal Police Act 1979*) under Part V of that Act;
- (h) investigating or resolving a complaint under the *Ombudsman Act 1976* or the *Privacy Act 1988*;
- (i) investigating or inquiring into a corruption issue under the *Law Enforcement Integrity Commissioner Act 2006*;
- (j) proceedings in relation to a complaint, allegation or issue mentioned in paragraph (f), (g), (h) or (i);

(k) deciding whether to institute proceedings, to make an application or request, or to take any other action, mentioned in any of the preceding paragraphs of this subsection;

(1) the performance of the functions of the Australian Federal Police under section 8 of the *Australian Federal Police Act 1979*.

(2) A constable or Commonwealth officer may use a thing seized under this Part, or the original or a copy of a document produced under Division 4B, for any other use that is required or authorised by or under a law of a State or a Territory.

(3) A constable or Commonwealth officer may make available to another constable or Commonwealth officer to use a thing seized under this Part, or the original or a copy of a document produced under Division 4B, for any purpose for which the making available of the thing or document is required or authorised by a law of a State or Territory.

(4) To avoid doubt, this section does not limit any other law of the Commonwealth that:

(a) requires or authorises the use of a document or other thing; or

(b) requires or authorises the making available (however described) of a document or other thing.

*Sharing thing or document for use by State, Territory or foreign agency*

(5) A constable or Commonwealth officer may make a thing seized under this Part, or the original or a copy of a document produced under Division 4B, available to:

(a) a State or Territory law enforcement agency; or

(b) an agency that has responsibility for:

(i) law enforcement in a foreign country; or

(ii) intelligence gathering for a foreign country; or

(iii) the security of a foreign country;

to be used by that agency for a purpose mentioned in subsection (1), (2) or (3) and the purpose of any or all of the following (but not for any other purpose):

(c) preventing, investigating or prosecuting an offence against a law of a State or Territory;

(d) proceedings under a corresponding law (within the meaning of the *Proceeds of Crime Act 1987* or the *Proceeds of Crime Act 2002*);

- (e) proceedings for the forfeiture of the thing under a law of a State or Territory;
- (f) deciding whether to institute proceedings or to take any other action mentioned in any of paragraphs (1)(a) to (l) (inclusive), subsection (2) or (3) or paragraph (c), (d) or (e) of this subsection.

*Ministerial arrangements for sharing*

- (6) This Division does not prevent the Minister from making an arrangement with a Minister of a State or Territory for:
  - (a) the making available to a State or Territory law enforcement agency of that State or Territory, for purposes mentioned in subsections (1), (3) and (5), of things seized under this Part and originals and copies of documents produced under Division 4B; and
  - (b) the disposal by the agency of such things, originals and copies when they are no longer of use to that agency for those purposes.

Note: This subsection does not empower the Minister to make such an arrangement.

*Definition*

- (7) In this section:

***State or Territory law enforcement agency*** means:

- (a) the police force or police service of a State or Territory; or
- (b) the New South Wales Crime Commission constituted by the *New South Wales Crime Commission Act 1985* of New South Wales; or
- (c) the Independent Commission Against Corruption constituted by the *Independent Commission Against Corruption Act 1988* of New South Wales; or
- (d) the Police Integrity Commission constituted by the *Police Integrity Commission Act 1996* of New South Wales; or
- (e) the Office of Police Integrity continued by the *Police Integrity Act 2008* of Victoria; or
- (f) the Crime and Misconduct Commission of Queensland; or
- (g) the Corruption and Crime Commission established by the *Corruption and Crime Commission Act 2003* of Western Australia.

### **3ZQV Operating seized electronic equipment**

- (1) This section applies to electronic equipment seized under this Part or moved under section 3K.
- (2) The electronic equipment may be operated at any location after it has been seized or moved, for the purpose of determining whether data that is evidential material is held on or accessible from the electronic equipment, and obtaining access to such data.
- (3) The data referred to in subsection (2) includes, but is not limited to, the following:
  - (a) data held on the electronic equipment, including data held on the electronic equipment when operated under this section that was not held on the electronic equipment at the time the electronic equipment was seized;
  - (b) data not held on the electronic equipment but accessible by using it, including data that was not accessible at the time the electronic equipment was seized.
- (4) If the electronic equipment was seized under a warrant or moved under section 3K, the electronic equipment may be operated before or after the expiry of the warrant.
- (5) This section does not limit the operation of other provisions of this Part that relate to dealing with items seized under this Part or moved under section 3K.

Note: For example, this section does not affect the operation of the time limits in section 3K on examination or processing of a thing moved under that section.

### **3ZQW Compensation for damage to electronic equipment**

- (1) This section applies if:
  - (a) as a result of equipment being operated as mentioned in section 3ZQV:
    - (i) damage is caused to the equipment; or
    - (ii) damage is caused to data recorded on the equipment or data access to which was obtained from the operation of the equipment; or
    - (iii) programs associated with the use of the equipment, or with the use of the data, are damaged or corrupted; and
  - (b) the damage or corruption occurs because:
    - (i) insufficient care was exercised in selecting the person who was to operate the equipment; or
    - (ii) insufficient care was exercised by the person operating the equipment.

(2) The Commonwealth must pay the owner of the equipment, or the user of the data or programs, such reasonable compensation for the damage or corruption as the Commonwealth and the owner or user agree on.

(3) However, if the owner or user and the Commonwealth fail to agree, the owner or user may institute proceedings in a court of competent jurisdiction for such reasonable amount of compensation as the court determines.

(4) In determining the amount of compensation payable, regard is to be had to whether any appropriate warning or guidance was provided, before the equipment was operated, on the operation of the equipment.

(5) Compensation is payable out of money appropriated by the Parliament.

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

*damage*, in relation to data, includes damage by erasure of data or addition of other data.

## **Subdivision B—Returning things seized and documents produced**

### **3ZQX When things seized or documents produced under Division 2, 4 or 4B must be returned**

*When things seized under Division 2 or 4 must be returned*

(1) If the Commissioner is satisfied that a thing seized under Division 2 or 4 is not required (or is no longer required) for a purpose mentioned in section 3ZQU or for other judicial or administrative review proceedings, the Commissioner must take reasonable steps to return the thing to the person from whom it was seized or to the owner if that person is not entitled to possess it.

(2) However, the Commissioner does not have to take those steps if:

(aa) either:

(i) the thing may be retained because of an order under subsection 3ZQZB(3), or any other order under that subsection has been made in relation to the thing; or

(ii) the Commissioner has applied for such an order and the application has not been determined; or

(a) the thing may otherwise be retained, destroyed or disposed of under a law, or an order of a court or tribunal, of the Commonwealth or of a State or a Territory; or

(b) the thing is forfeited or forfeitable to the Commonwealth or is the subject of a dispute as to ownership.

*When documents produced under Division 4B must be returned*

- (3) If the Commissioner is satisfied that a document produced under Division 4B is not required (or is no longer required) for a purpose mentioned in section 3ZQU or for other judicial or administrative review proceedings, the Commissioner must take reasonable steps to return the document to the person who produced the document or to the owner if that person is not entitled to possess it.
- (4) However, the Commissioner does not have to take those steps if:
  - (a) either:
    - (i) the document may be retained because of an order under subsection 3ZQZB(3), or any other order under that subsection has been made in relation to the document; or
    - (ii) the Commissioner has applied for such an order and the application has not been determined; or
  - (b) the document may otherwise be retained, destroyed or disposed of under a law, or an order of a court or tribunal, of the Commonwealth or of a State or a Territory; or
  - (c) the document is forfeited or forfeitable to the Commonwealth or is the subject of a dispute as to ownership.

**3ZQY When things seized under Division 3 must be returned**

- (1) If:
  - (a) the Commissioner is satisfied that a thing seized under Division 3 is not required (or is no longer required) for a purpose mentioned in section 3ZQU or for other judicial or administrative review proceedings; or
  - (b) the period of 60 days after the thing's seizure ends;

the Commissioner must take reasonable steps to return the thing to the person from whom it was seized or to the owner if that person is not entitled to possess it.

- (2) However, the Commissioner does not have to take those steps if:
  - (a) proceedings in respect of which the thing may afford evidence were instituted before the end of the 60 days and have not been completed (including an appeal to a court in relation to those proceedings); or
  - (b) either:

- (i) the thing may be retained because of an order under subsection 3ZQZB(2) or (3), or any other order under subsection 3ZQZB(3) has been made in relation to the thing; or
- (ii) the Commissioner has applied for such an order and the application has not been determined; or
- (c) the thing may otherwise be retained, destroyed or disposed of under a law, or an order of a court or tribunal, of the Commonwealth or of a State or a Territory; or
- (d) the thing is forfeited or forfeitable to the Commonwealth or is the subject of a dispute as to ownership.

**3ZQZA When things seized under Division 3A must be returned**

- (1) The Commissioner must take reasonable steps to return a thing seized under Division 3A if the owner requests the return of the thing.
- (2) However, the Commissioner does not have to take those steps if:
  - (a) the Commissioner suspects on reasonable grounds that if the thing is returned to the owner, the thing is likely to be used by the owner or another person in the commission of a terrorist act, a terrorism offence or a serious offence; or
  - (b) the Commissioner is satisfied that the thing is being used, or is required to be used, for a purpose mentioned in section 3ZQU or for other judicial or administrative review proceedings; or
  - (c) either:
    - (i) the thing may be retained because of an order under subsection 3ZQZB(2) or (3), or any other order under subsection 3ZQZB(3) has been made in relation to the thing; or
    - (ii) the Commissioner has applied for such an order and the application has not been determined; or
  - (d) the thing may otherwise be retained, destroyed or disposed of under a law, or order of a court or tribunal, of the Commonwealth or of a State or a Territory; or
  - (e) the thing is forfeited or forfeitable to the Commonwealth or is the subject of a dispute as to ownership.
- (3) Despite subsection (2), if:
  - (a) the owner of a thing requests the return of the thing:
    - (i) within 90 days after the date of the seizure notice served under section 3UF in relation to the thing; or



(ii) if subsection 3UF(2) applied in relation to the thing so that a seizure notice was not served—within 90 days after the day on which the thing was seized; and

(b) the thing has not been returned to the owner by the end of the 90th day;

the Commissioner must, before the end of the 95th day:

(c) take reasonable steps to return the thing to the owner; or

(d) apply to a magistrate for an order under section 3ZQZB.

**3ZQZB Magistrate may permit a thing seized or document produced under this Part to be retained, forfeited etc.**

(1) A magistrate may, on application by the Commissioner, make an order under subsection (2) or (3) in relation to a thing seized or a document produced under this Part.

*Use for purpose mentioned in section 3ZQU or for other judicial or administrative review proceedings*

(2) The magistrate may order that a thing seized under Division 3 or 3A be retained for the period specified in the order if the magistrate is satisfied that the thing is being used, or is required to be used, for a purpose mentioned in section 3ZQU or for other judicial or administrative review proceedings.

*Preventing use in committing terrorist act, terrorism offence or serious offence*

(3) The magistrate may make any of the orders referred to in subsection (4) if the magistrate is satisfied that there are reasonable grounds to suspect that, if a thing seized or document produced under this Part is returned to any of the following persons, it is likely to be used by that person or another person in the commission of a terrorist act, a terrorism offence or a serious offence:

(a) the owner of the thing or document;

(b) in the case of a thing—the person from whom the thing was seized;

(c) in the case of a document—the person who produced the document.

(4) The orders are as follows:

(a) an order that the thing or document may be retained for the period specified in the order;

- (b) an order that the thing or document is forfeited to the Commonwealth;
- (c) for a thing that is not a document—an order that:
  - (i) the thing be sold and the proceeds given to the owner of the thing; or
  - (ii) the thing be sold in some other way;
- (d) an order that the thing or document is to be destroyed or otherwise disposed of.

*Thing or document must be returned if magistrate not satisfied*

- (5) The magistrate must order that a thing or document be returned to the following person if the magistrate is not satisfied as mentioned in subsection (2) or (3):
- (a) in the case of a thing—the person from whom the thing was seized;
  - (b) in the case of a document—the person who produced the document;
  - (c) if the person referred to in paragraph (a) or (b) is not entitled to possess the thing or document—the owner of the thing or document.

*Persons with an interest in thing or document*

- (6) Before making an application under this section in relation to a thing or document, the Commissioner must:
- (a) take reasonable steps to discover who has an interest in the thing or document; and
  - (b) if it is practicable to do so, notify each person who the Commissioner believes to have such an interest of the proposed application.
- (7) The magistrate must allow a person who has an interest in the thing or document to appear and be heard in determining the application.

*Special rule for things seized under Division 3*

- (8) The Commissioner may only make an application under this section in relation to a thing seized under Division 3 if the application is made:
- (a) before the end of 60 days after the seizure; or

(b) before the end of a period previously specified in an order in relation to the thing under this section.

## **Division 5—General**

### **3ZR Conduct of ordinary searches and frisk searches**

An ordinary search or a frisk search of a person under this Part must, if practicable, be conducted by a person of the same sex as the person being searched.

### **3ZS Announcement before entry**

- (1) A constable must, before any person enters premises under a warrant or to arrest a person:
  - (a) announce that he or she is authorised to enter the premises; and
  - (b) give any person at the premises an opportunity to allow entry to the premises.
- (2) A constable is not required to comply with subsection (1) if he or she believes on reasonable grounds that immediate entry to the premises is required to ensure:
  - (a) the safety of a person (including a constable); or
  - (b) that the effective execution of the warrant or the arrest is not frustrated.

### **3ZT Offence for making false statements in warrants**

A person must not make, in an application for a warrant, a statement that the person knows to be false or misleading in a material particular.

Penalty: Imprisonment for 2 years.

### **3ZU Offences relating to telephone warrants**

A person must not:

- (a) state in a document that purports to be a form of warrant under section 3R the name of an issuing officer unless that officer issued the warrant; or
- (b) state on a form of warrant under that section a matter that, to the person's knowledge, departs in a material particular from the form authorised by the issuing officer; or
- (c) purport to execute, or present to a person, a document that purports to be a form of warrant under that section that the person knows:
  - (i) has not been approved by an issuing officer under that section; or
  - (ii) to depart in a material particular from the terms authorised by an issuing officer under that section; or
- (d) give to an issuing officer a form of warrant under that section that is not the form of warrant that the person purported to execute.

Penalty: Imprisonment for 2 years.

### **3ZW Delegation by Commissioner**

- (1) The Commissioner may delegate to a constable any or all of the Commissioner's powers, functions or duties under this Part.
- (2) The Commissioner may delegate to a Commonwealth officer any or all of the Commissioner's powers, functions or duties under Division 4C of this Part if the Commissioner is satisfied on reasonable grounds that the officer is able to properly exercise those powers, functions or duties.

### **3ZX Law relating to legal professional privilege not affected**

This Part does not affect the law relating to legal professional privilege.