Australia

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 01 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": 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 "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; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; 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	**Art. 476.1 of Criminal Code Act 1995 (Act n°12 of 1995) of Australia** **Definitions** (1) In this Part: **access to data held in a computer** means: (a) the display of the data by the computer or any other output of the data from the computer; or (b) the copying or moving of the data to any other place in the computer or to a data storage device; or (c) in the case of a program—the execution of the program. **Commonwealth computer** means a computer owned, leased or operated by a Commonwealth entity. **data** includes: (a) information in any form; or (b) any program (or part of a program). **data held in a computer** includes: (a) data held in any removable data storage device for the time being held in a computer; or (b) data held in a data storage device on a computer network of which the computer forms a part. **data storage device** means a thing (for example, a disk or file server) containing, or designed to contain, data for use by a computer.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	electronic communication means a communication of information in any form by means of guided or unguided electromagnetic energy. **unauthorised access, modification or impairment** has the meaning given in section 476.2. (2) In this Part, a reference to: (a) access to data held in a computer; or (b) modification of data held in a computer; or (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.
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	
Article 2 – Illegal access 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 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.	**Art. 476.2 of Criminal Code Act 1995 (Act n°12 of 1995) of Australia** **Meaning of unauthorised access, modification or impairment** (1) In this Part: (a) access to data held in a computer; or (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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 Territory; iii. the enforcement of a law of the Commonwealth or of a State or Territory; iv. the protection of public safety; v. the personal affairs of any person; vi. trade secrets; vii. records of a financial institution; or viii. commercial Information the disclosure of which could cause advantage or disadvantage to any person is guilty of an offence

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Penalty: Imprisonment for 2 years 3. A person who: 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; 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 c. continues to examine that data; is guilty of an offence. Penalty for a contravention of this subsection: **Imprisonment for 2 years**
Article 3 – Illegal interception 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.	**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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 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. (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. (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	intercepted, and the action has ceased before it is practicable for an application for a Part 2-5 warrant to be made. (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. (8) Subsections (4), (5), (6) and (7) only apply where the agency concerned is: (a) the Australian Federal Police; or (b) the Police Force of a State. (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. 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. (10) Subsection (9) has effect only to the extent necessary: (a) to enable an application to be made for the purposes of subsection (6); and (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 (c) to enable this Act to operate in relation to a Part 2-5 warrant issued on such an application.
Article 4 – Data interference 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.	**Art. 477.1 (1/ii) 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: (ii) any unauthorised modification of data held in a computer; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 is guilty of an offence. **Section 76D of Crimes Act 1914 of Australia** 1.A person who, by means of a facility operated or provided by the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Commonwealth or by a carrier, intentionally and without authority obtains access to data stored in a computer, is guilty of an offence. **Section 76E(a) of Crimes Act 1914 of Australia** 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: a.destroys, erases or alters data stored in, or inserts data into a computer; is guilty of an offence
Article 5 – System interference 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	**Part VIA, Section 76C(b) of Crimes Act 1914 of Australia** A person who intentionally and without authority or lawful excuse: b.interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer; is guilty of an offence. **Section 76E (b) of Crimes Act 1914 of Australia** 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: b.destroys, erases or alters data stored in, or inserts data into a computer; is guilty of an offence.
Article 6 – Misuse of devices 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: a the production, sale, procurement for use, import, distribution or otherwise making available of: 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; 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,	**For Art. 6(1/a/ii)- Art. 478.3(1) of Criminal Code Act 1995 (Act n°12 of 1995) of Australia.** **Possession or control of data with intent to commit a computer offence** (1) A person is guilty of an offence if: (a) the person has possession or control of data; and (b) the person has that possession or control with the intention that the data be used, by the person or another person, in: (i) committing an offence against Division 477; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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; 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. (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; and (b) the response is in connection with the operations of a Commonwealth entity. Penalty: Imprisonment for 10 years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 intention of: (i) dishonestly inducing another person in the other person's capacity as a public official to accept it as genuine; and (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 (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 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 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 knows that a document is a false document and uses it with the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	intention of: (i) dishonestly inducing another person to accept it as genuine; and (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 (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 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 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 cause a computer, a machine or an electronic device to respond to the document as if the document were genuine; and gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function; and (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 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 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 knows that a document is a false document and has it in his or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	her possession 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. **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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 the knowledge of the first-mentioned person, is false or misleading in a material particular; and (c) the first-mentioned person does so with the intention of: (i) obtaining a gain from another person; or (ii) causing a loss to another person; and (d) 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. **145.6 Geographical jurisdiction** Section15.4 (extended geographical jurisdiction—category D) applies to each offence against this Division.
Article 8 – Computer-related fraud 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: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system,	**Part 7.3—Fraudulent conduct** **Division 133—Preliminary** **133.1 Definitions** In this Part: ***account*** means an account (including a loan account, a credit card account or a similar account) with a bank or other financial institution.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	***deception*** means an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes: (a) a deception as to the intentions of the person using the deception or any other person; and (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. **Division 134—Obtaining property or a financial advantage by deception** **134.1 Obtaining property by deception** (1) A person is guilty of an offence if: (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 (b) the other person is a Commonwealth entity. Penalty: Imprisonment for 5 years. (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. (5) A person is guilty of an offence if: (a) the person dishonestly causes a loss, or dishonestly causes a risk of loss, to another 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 other person is a Commonwealth entity. Penalty: Imprisonment for 5 years. (6) Absolute liability applies to the paragraph (5)(c) element of the offence. Influencing a Commonwealth public official (7) A person is guilty of an offence if: (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 (b) the public official is a Commonwealth public official; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) the duties are duties as a Commonwealth public official. Penalty: Imprisonment for 5 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. **135.2 Obtaining financial advantage** (1) 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 himself or herself from another person; and (ab) the person knows or believes that he or she is not eligible to receive that financial advantage; and (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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	135.2 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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. **135.5 Geographical jurisdiction** Section 15.4 (extended geographical jurisdiction—category D) applies to each offence against this Division.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 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: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a	**For. Art. 9(1)-** **Sect. 474.19 of Criminal Code Act 1995 of Australia.** **Using a carriage service for child pornography material** (1)A person is guilty of an offence if: (a) the person: (i) uses a carriage service to access material; or (ii) uses a carriage service to cause material to be transmitted to the person; or (iii) uses a carriage service to transmit material; or (iv) uses a carriage service to make material available; or (v) uses a carriage service to publish or otherwise distribute material; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 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. 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.	(b) the material is child pornography material. *Penalty:* Imprisonment for 10 years. (2)To avoid doubt, the following are the fault elements for the physical elements of an offence against subsection (1): (a) intention is the fault element for the conduct referred to in paragraph (1)(a); (b) recklessness is the fault element for the circumstances referred to in paragraph (1)(b). Note: For the meaning of *intention* and *recklessness* see sections 5.2 and 5.4. (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. **Sect. 474.20 of Criminal Code Act 1995 of Australia.** **Possessing, controlling, producing, supplying or obtaining child 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).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 (ii) potential prohibited content (within the meaning of that Schedule); in the performance of the Authority's functions under that Schedule; or (b) manufacturing or developing, or updating, content filtering technology (including software) in accordance with: (i) a recognised alternative access-prevention arrangement (within the meaning of clause 40 of Schedule 5 to the *Broadcasting Services Act 1992*); or (ii) a designated alternative access-prevention arrangement (within the meaning of clause 60 of that Schedule). Note: A defendant bears an evidential burden in relation to the matter in this subsection, see subsection 13.3(3).
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 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	**For Art. 10(1)- Sec. 47G of Copyright Act 1968 of Australia.** **Unauthorised use of copies or information** (1) If: (a) a reproduction or adaptation of a literary work that is a computer program is made under a prescribed provision; and (b) the reproduction or adaptation, or any information derived from it, is,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 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 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.	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; the prescribed provision does not apply, and is taken never to have applied, to the making of the reproduction or adaptation. (2) For the purposes of this section, sections 47B, 47C, 47D, 47E and 47F are prescribed provisions. **For Art. 1(2)- Sec. 91 of Copyright Act 1968 of Australia**. **Television broadcasts and sound broadcasts in which copyright subsists** Subject to this Act, copyright subsists in a television broadcast or sound broadcast made from a place in Australia: (a) under the authority of a licence or a class licence under the *Broadcasting Services Act 1992* ; or (b) by the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation. **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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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** Indictable offence (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 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. **Section 132 AM Copyright Act 1968 of Australia, Advertising supply of infringing copy** Summary offence (1) A person commits an offence if: (a) the person, by any means, publishes, or causes to be published, an

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	advertisement for the supply in Australia of a copy (whether from within or outside Australia) of a work or other subject-matter; and (b) the copy is, or will be, an infringing copy. Penalty: 30 penalty units or imprisonment for 6 months, or both. Location of supply of copy by communication resulting in creation of copy (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. **Section 132 AN Copyright Act 1968 of Australia, Causing work to be performed publicly** Indictable offence (1) 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. (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* .

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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*). Defence--encryption research (4) Subsection (1) does not apply to the person if: (a) the person circumvents the access control technological protection measure to enable: (i) the person; or (ii) if the person is a body corporate--an employee of 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 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 (c) the person or employee is:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 (d) the person or employee: (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 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 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--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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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*). 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).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 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. 2 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, 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.	**For Art. 11(2)** **Art. 477.1 (8) of Criminal Code Act 1995 (Act n°12 of 1995) of Australia** **Unauthorised access, modification or impairment with intent to commit a serious offence** *No offence of attempt* (8) It is not an offence to attempt to commit an offence against this section. **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*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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. (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. (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. (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. (8) Subsections (4), (5), (6) and (7) only apply where the agency concerned is: (a) the Australian Federal Police; or (b) the Police Force of a State. (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	would not constitute a serious offence apart from this subsection. 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. (10) Subsection (9) has effect only to the extent necessary: (a) to enable an application to be made for the purposes of subsection (6); and (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 (c) to enable this Act to operate in relation to a Part 2-5 warrant issued on such an application.
Article 12 – Corporate liability 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: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 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. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Part 2.5—Corporate criminal responsibility** **Division 12** **12.1 General principles** **(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.** **(2) A body corporate may be found guilty of any offence, including one punishable by imprisonment.** Note: Section 4B of the *Crimes Act 1914* enables a fine to be imposed for offences that only specify imprisonment as a penalty. **12.2 Physical elements** If a physical element of an offence is committed by an employee, agent or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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. **12.3 Fault elements other than negligence** (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. (2) The means by which such an authorisation or permission may be established include: (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 (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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: (a) negligence is a fault element in relation to a physical element of an offence; and (b) no individual employee, agent or officer of the body corporate has that fault element; 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). (3) Negligence may be evidenced by the fact that the prohibited conduct was substantially attributable to: (a) inadequate corporate management, control or supervision of the conduct of one or more of its employees, agents or officers; or (b) failure to provide adequate systems for conveying relevant information to relevant persons in the body corporate. **12.5 Mistake of fact (strict liability)** (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: (a) the employee, agent or officer of the body corporate who carried out the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 (b) the body corporate proves that it exercised due diligence to prevent the conduct. (2) A failure to exercise due diligence may be evidenced by the fact that the prohibited conduct was substantially attributable to: (a) inadequate corporate management, control or supervision of the conduct of one or more of its employees, agents or officers; or (b) failure to provide adequate systems for conveying relevant information to relevant persons in the body corporate. **12.6 Intervening conduct or event** 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.
Article 13 – Sanctions and measures 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. 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.	Australia's domestic offences establish appropriate penalties, including imprisonment. The penalty for each offence is contained within the specific offence provision.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 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. 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:	Australian law currently provides for all of the powers required by the Convention (powers are contained in Articles 14 – 21 inclusive). Australia anticipates pursuing this reservation. Domestic Australia law restricts real-time collection of traffic data to criminal offences with a minimum penalty threshold of 3 years imprisonment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 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. 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: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is 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	
Article 15 – Conditions and safeguards 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	See TIA act as well as the Mutual Assistance In Criminal Matters Act 1987 (MA Act)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* 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.	
Article 16 – Expedited preservation of stored computer data 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 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. 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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Subsections 313 (3) of the Telecommunication Act** (3) A carrier or carriage service provider must, in connection with: (a) the operation by the carrier or provider of telecommunications networks or facilities; or (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: (c) enforcing the criminal law and laws imposing pecuniary penalties; (d) protecting the public revenue; (e) safeguarding national security. **See the text attached on general search and seizure powers of Part 1AA of the Crimes Act 1914 (Crimes Act).** **Provisons of Cybercrime Legislation Amendment Act (No. 120, 2012) provide for direct implemnentation of preservation provisons as required by the Budapest Convention on Cybercrime.**
Article 17 – Expedited preservation and partial disclosure of traffic	**Section 180of TIA Act Authorisations for access to prospective**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
data 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: 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 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**information or documents** (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* 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 (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 (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 (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. (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 (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 (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. Note: Section 184 deals with notification of revocations. **Provisons of Cybercrime Legislation Amendment Act (No. 120, 2012)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	provide for direct implemnentation of preservation provisons as required by the Budapest Convention on Cybercrime.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: 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 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 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: a the type of communication service used, the technical provisions taken thereto and the period of service; 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; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**For Art. 18(1/a)- Art. 3LB(2) of Crimes Act 1914 of Australia.** **3LB Accessing data held on other premises—notification to occupier of that premises** (2) A notification under subsection (1) must include sufficient information to allow the occupier of the other premises to contact the executing officer. **For Art. 18(1/a)- Subsection 24, Art. 201(1) (1 Note) of Customs Act 1901 of Australia** **24 Subsection 201(1)** Repeal the subsection, substitute: (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: (a) the data might constitute evidential material; and (b) the equipment can be operated without damaging it. 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. (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: (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)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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
Article 19 – Search and seizure of stored computer data 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; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 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	**For Art. 19(1)- Art. 3LA(a) of Crimes Act 1914 of Australia** **Person with knowledge of a computer or a computer system to assist access etc.** (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; **For Art. 19(3/a)- Art. 3LA(b) of Crimes Act 1914 of Australia** **3LB Accessing data held on other premises—notification to occupier of that premises** (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. **For Art.19(4)- Art. 3LA(3) of Crimes Act 1914 of Australia.** **Person with knowledge of a computer or a computer system to assist access etc.** (3) A person commits an offence if the person fails to comply with the order. **For Art.19(1)- Subsection 24, Art. 201(1) (1) of Customs Act 1901 of Australia.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**24 Subsection 201(1)** Repeal the subsection, substitute: (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: (a) the data might constitute evidential material; and (b) the equipment can be operated without damaging it. **For Art. 19 (3/b)- Subsection 24, Art. 201(1) (1A/a) of Customs Act 1901 of Australia.** (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: (a) copy the data to a disk, tape or other associated device brought to the premises; or **subsections 313 (3) of the Telecommunication Act** (3) A carrier or carriage service provider must, in connection with: (a) the operation by the carrier or provider of telecommunications networks or facilities; or (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: (c) enforcing the criminal law and laws imposing pecuniary penalties; (d) protecting the public revenue; (e) safeguarding national security.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary 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	**Section 180of TIA Act Authorisations for access to prospective information or documents** (1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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, traffic data, in real-time, associated with 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 traffic data associated with specified communications transmitted 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.	Prospective authorisation (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 (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 (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. (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 (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 (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. Note: Section 184 deals with notification of revocations.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 21 – Interception of content data 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.	**section 63 of the TIA Act No dealing in intercepted information or interception warrant information** (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.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 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 b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed	**Section 4 and 4A of the TIA Act** SECT 4 Application This Act binds the Crown in right of the Commonwealth, of a State and of the Northern Territory. SECT 4A Application of the Criminal Code Chapter 2 of the *Criminal Code* applies to all offences against this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
outside the territorial jurisdiction of any State. 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. 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. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 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.	Note: Chapter 2 of the *Criminal Code* sets out the general principles of criminal responsibility. **Section 132 AB of the Copyright Act.** SECT 132AB Geographical application (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 *Criminal Code* .
Chapter III – International co-operation	
Article 24 – Extradition 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. 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. 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 concluded between or among them. 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	**For Art. 24(5) - Part II, Art. 12 of Extradition Act 1988 of Australia** **Art. 12- Provisional arrest warrants** (1)Where: (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 (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; the magistrate shall issue a warrant, in the statutory form, for the arrest of the person. (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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 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. 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. 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. 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	(3)Where: (a) the Attorney-General has received the report under subsection (2) or has otherwise become aware of the issue of the warrant; (b) the person has not been arrested under the warrant; and (c) either: (i) the Attorney-General decides not to issue a notice under subsection 16(1) in relation to the person; or (ii) the Attorney-General considers for any other reason that the warrant should be cancelled; the Attorney-General shall, by notice in writing in the statutory form, direct a magistrate to cancel the warrant.
Article 25 – General principles relating to mutual assistance 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. 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.	**For Art. 25(4)- Sec. 8 of Mutual Assistance in Criminal Matters Act 1987 of Australia Refusal of assistance** (1) A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Attorney-General: (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior 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. 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.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 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. 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. b The central authorities shall communicate directly with each other; 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;	**For. Art. 27(4-6)- Sec. 8 of Mutual Assistance in Criminal Matters Act 1987 of Australia** **.** **For Art. 25(4)- Sec. 8 of Mutual Assistance in Criminal Matters Act 1987 of Australia Refusal of assistance** (1) A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Attorney-General: (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 (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 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	(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 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 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	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 following information: (a) the name of the authority concerned with the criminal matter to which the request relates; (b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; (c) a description of the purpose of the request and of the nature of the assistance being sought; (d) any information that may assist in giving effect to the request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	However, a failure to comply with this subsection is not a ground for refusing the request. (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. (4) If a foreign country makes a request to a court in Australia for international assistance in a criminal matter: (a) the court must refer the request to the Attorney-General; and (b) the request is then taken, for the purposes of this Act, to have been made to the Attorney-General.
Article 28 – Confidentiality and limitation on use 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. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could 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.	**Schedule 4—Telecommunications data Confidentiality, Cybercrime Legislation Amendment Act (No. 120, 2012)**
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	**Schedule 2—Amendments relating to Mutual Assistance, Cybercrime Legislation Amendment Act (No. 120, 2012)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Schedule 2—Amendments relating to Mutual Assistance, Cybercrime Legislation Amendment Act (No. 120, 2012)**
Article 31 – Mutual assistance regarding accessing of stored computer data 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. 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. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Schedule 2—Amendments relating to Mutual Assistance, Cybercrime Legislation Amendment Act (No. 120, 2012)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or 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.	
Article 33 – Mutual assistance in the real-time collection of traffic data 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. 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.	
Article 34 – Mutual assistance regarding the interception of content data 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.	
Article 35 – 24/7 Network 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: a the provision of technical advice;	**Declarations contained in a Note verbale from the Australian Department of Foreign Affairs and Trade deposited with the instrument of accession on 30 November 2012 – Or. Engl** Article 35 - 24/7 Network: AOCC Watchfloor Operations Australian Federal police GPO Box 401

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 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. 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. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	Canberra ACT 2601 Australia
Article 42 – Reservations 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.	**Reservations contained in the instrument of accession deposited on 30 November 2012 – Or. Engl.– Or. fr.** In accordance with Article 42 and Article 14, paragraph 3.a, of the Convention, Australia reserves the right to apply the measures referred to in Article 20 (Real-time collection of traffic data) only to offences that are punishable by imprisonment for at least 3 years and any other 'serious offences' as defined under domestic law governing the collection and recording of traffic data in real time and the interception of content data. Under Australian law, domestic agencies may only gain access to traffic data collected and recorded in real time in relation to offences that are punishable by imprisonment for at least 3 years and other 'serious offences'. Domestic agencies may only gain access to intercepted content data in relation to 'serious offences'. Period covered: 01/03/2013 - Articles concerned : 14 **Reservations contained in the instrument of accession deposited on 30 November 2012 – Or. Engl.– Or. fr.** In accordance with Article 42 and Article 22, paragraph 2, of the Convention, Australia reserves the right not to apply the jurisdiction rules laid down in Article 22, paragraph 1.b-d, to offences established in accordance with Article 7

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(Computer-related forgery), Article 8 (Computer-related fraud) and Article 9 (Offences related to child pornography). The Parliament of the Commonwealth of Australia does not enjoy a plenary power to make laws establishing offences for computer-related forgery, computer-related fraud or offences related to child pornography. The Parliament of the Commonwealth of Australia has established offences for computer-related forgery, computer-related fraud and offences related to child pornography, committed on board ships flying Australian flags, on board aircraft registered under Australian law, or by Australian nationals outside Australia, where the offending conduct involves some subject matter with respect to which it has legislative power. In addition to those offences, the Australian States and Territories have also established offences in accordance with Articles 7, 8 and 9 when commited on their territory. In accordance with Article 42 and Article 22, paragraph 2, of the Convention, Australia further reserves the right not to apply the jurisdiction rules laid down in Article 22, paragraphs 1.b-d, to offences established in accordance with Article 10 (Offences related to infringements of copyright and related rights). Autralian law does not presently provide jurisdiction over acts constituting infringements of copyright and related rights committed on board ships flying Australian flags, on board aircraft registered under Australian law, or by Australian nationals outside Australia. Period covered: 01/03/2013 - Articles concerned : 22

Back to the Table of Contents