ALAI 2001 National Report
Session IC
Australia

Prepared by David Lindsay, Research Fellow, Centre for Media, Communications and Information Technology of Law, Faculty of Law, The University of Melbourne

ALAI 2001 Congress, New York, June 13-17
Adjuncts and Alternatives to Copyright

Situating legal protections for copyright-related technological measures in the broader legal landscape:

ANTI-CIRCUMVENTION PROTECTION OUTSIDE COPYRIGHT

1. Types of Circumvention

a. Gaining access to a technologically protected computer system or to protected material without authorisation.

In Australia, unlawful access to computers, or material stored on computers, is prohibited by criminal laws that establish offences for computer crimes. The criminal provisions were introduced in the 1980s in response to social concerns that unlawful access to data was, in itself, harmful.[1] Australia is a federation, with separate criminal laws established by the Commonwealth, on the one hand, and by the various States and Territories, on the other. There is considerable variation among Australian jurisdictions in relation to the criminal provisions prohibiting unlawful access to computers or to computer data. As part of a project to develop a national model criminal code, the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General released a report on computer-related criminal offences in January 2001.[2] The recommendations of the report are designed to harmonise Commonwealth, State and Territory computer crime laws with proposed changes to the law of theft and fraud. The report proposes a number of computer offences directed mainly to computer misuse preparatory to the commission of another crime, or computer misuse which is comparable to the offence of criminal damage, whether by unauthorised modification of data or by defeating security systems.

Liability for unauthorised access to secret information stored on a computer may also be established under the equitable doctrine of breach of confidence, although legal authority for this form of liability is not entirely clear.

---

[1] See Commonwealth Attorney-General's Department, *Computer Crime,* Discussion Paper No 12 (AGPS, Canberra, 1988); Tasmanian Law Reform Commission, *Computer Misuse,* Report No 47 (Tasmanian Government Printers, Hobart, 1986); Queensland Department of Justice, *Green Paper on Computer-Related Crime* (Queensland Department of Justice, Brisbane, 1987).

[2] Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Report on Model Criminal Code, Chapter 4, Damage and Computer Offences,* January 2001, available at http://www.law.gov.au/publications/Model_Criminal_Code/DamageReport.pdf (hereafter, the *Model Criminal Code Report).*

(i) Criminal offences for unauthorised access

Commonwealth

At the Commonwealth level, unauthorised access to data stored on a computer is prohibited under Part VIA of the *Crimes Act 1914* (Cth), which creates a number of offences relating to computers.[3] The scope of Part VIA is limited to offences in relation to data stored in a Commonwealth computer, data stored on behalf of the Commonwealth or access gained by means of Commonwealth facilities or facilities operated by a telecommunications carrier.

The main offence relating to unlawful access is contained in section 76B, which prohibits the intentional unauthorised access to data stored in a Commonwealth computer or data stored on behalf of the Commonwealth.[4] "Commonwealth computer" is defined to mean a computer or computer system that is "owned, leased or operated by the Commonwealth".[5] "Data" is defined to include "information, a computer program or part of a computer program".[6] "Data stored on behalf of the Commonwealth" is to be interpreted as including a reference to:

(i) data stored in the computer at the direction or request of the Commonwealth; and
(ii) data supplied by the Commonwealth that is stored in the computer under, or in the course of performing, a contract with the Commonwealth.[7]

In addition to the offence of unauthorised access, section 76B establishes three aggravated forms of the offence.[8]

The offences created by section 76B are mirrored by section 76D, which prohibits the intentional unauthorised access to data stored in a computer by means of a Commonwealth facility or a facility operated by a telecommunications carrier.[9] A telecommunications "carrier" is defined widely by reference to a series of complex definitions in the *Telecommunications Act 1997* (Cth).[10] In effect, the provision prohibits the intentional unauthorised access to data stored in a computer by means of the telecommunications system. Like section 76B, section 76D establishes three aggravated forms of the offence.

The Commonwealth offences operate concurrently with State and Territory computer crime laws.[11]

States and Territories

Specific offences relating to unlawful access to computers are established by criminal provisions in New South Wales, Tasmania, Victoria and the Australian Capital Territory. There are differences in the precise wording of the unlawful access offences. In South Australia, Western Australia and Queensland, offences are established only in relation to computers that are protected by access restrictions, such as an access code. In the Northern Territory, some forms of unauthorised access may be caught by an offence of unlawfully obtaining confidential information from a computer.

---

[3] Part VIA of the *Crimes Act 1914* (Cth) was introduced in 1989 by the *Crimes Legislation Amendment Act 1989* (Cth).
[4] *Crimes Act 1914* (Cth) s 76B(1).
[5] *Crimes Act 1914* (Cth) s 76A(1), definition of "Commonwealth computer".
[6] *Crimes Act 1914* (Cth) s 76A(1), definition of "data".
[7] *Crimes Act 1914* (Cth) s 76A(2).
[8] *Crimes Act 1914* (Cth) ss 76B(2), (3). The aggravated forms of unauthorised access establish offences for access with wrongful intent, access to classified data and the continued examination of classified data.
[9] *Crimes Act 1914* (Cth) s 76D(1).
[10] *Crimes Act 1914* (Cth) s 76A (definition of "carrier"); *Telecommunications Act 1997* (Cth) ss 7 (definitions of "carrier", "carriage service provider"); 16, 87.
[11] *Crimes Act 1914* (Cth) s 76F.

In New South Wales, section 309 of the *Crimes Act 1900* (NSW) establishes a criminal offence for the intentional access to a program or data stored in a computer without authority or lawful excuse.[12] Like the Commonwealth legislation, section 309 creates three aggravated forms of the offence.[13] The Australian Capital Territory offence of unlawful access is similar to the New South Wales offence. Section 135J of the *Crimes Act 1900* (ACT) prohibits intentionally obtaining access to data stored in a computer without lawful authority or excuse. There are no aggravated offences in the Australian Capital Territory.

In Victoria, section 9A of the *Summary Offences Act 1966* (Vic) establishes the offence of computer trespass for gaining access to, or entering, a computer system without lawful authority. A similar offence is created under the Tasmanian *Criminal Code.* Section 257D of the Criminal Code (Tas) creates an offence for intentionally gaining access to a computer or computer system, without lawful excuse.

In South Australia, rather than prohibiting unauthorised access *per se,* an offence is established for operating a "restricted-access" computer system without proper authorisation.[14] A "restricted-access" computer system is defined as a computer system in which the use of a "particular code of electronic impulses" is necessary to obtain access and in which use of the code is confined to particular authorised persons.[15] The Western Australian legislation is similarly limited to "restricted-access" computer systems.[16] Unlike South Australia, however, in Western Australia there is an offence for gaining access to information stored in a "restricted-access" system without proper authorisation, in addition to the offence of operating a "restricted-access" system without authorisation.[17] In Queensland, an offence of "computer hacking" is established under section 408D of the *Criminal Code Act 1899* (Qld). The Queensland offence prohibits a person from using a "restricted computer" without the consent of the computer's "controller", meaning a person who has the right to control the computer.[18] A "restricted computer" is defined essentially as a computer for which a device, code or sequence of electronic impulses is necessary to gain access and in relation to which access is restricted to persons authorised by the computer's "controller".[19]

In the Northern Territory there is no specific provision dealing with unauthorised access. There is, however, a general offence for unlawfully abstracting confidential information from a repository of information, including a computer, with an intent to cause loss, to publish the information, or to obtain a benefit from the information.[20]

The *Model Criminal Code Report* recommended replacing the existing Commonwealth, State and Territory offences with a new summary offence of unauthorised access to data. The proposed new offence would be similar to the South Australian, Queensland and western Australian offences, in that it would not apply to unauthorised access *per se,* but would be limited to data held in a computer which is protected by a computerised access control system.

(ii) Breach of confidence

The equitable action for breach of confidence is established if: information is confidential; the information is communicated in circumstances importing an obligation of confidence; and there has been an

---

[12] *Crimes Act 1900* (NSW) s 309(1); see also s 308 (definitions of "data" and "program").
[13] *Crimes Act 1900* (NSW) ss 309(2), (3), (4).
[14] *Summary Offences Act 1953* (SA) s 44(1).
[15] *Summary Offences Act 1953* (SA) s 44(3).
[16] Criminal Code (WA) s 440A. A "restricted-access" computer system is defined by s 440A(1) of the *Code.*
[17] Criminal Code (WA) s 440A(2).
[18] *Criminal Code Act 1899* (Qld) ss 408D(1), (5) (definition of "controller").
[19] *Criminal Code Act 1899* (Qld) s 408D(5) (definition of "restricted computer").
[20] Criminal Code Act (NT) s 222.

unauthorised use of the information to the detriment of the person communicating it.[21] In some decisions a breach of confidence seems to have been established where information has been obtained surreptitiously, even though the information was not communicated in confidence.[22] This suggests that unauthorised access to information stored on a computer may amount to a breach of confidence, provided that the information is sufficiently secret and there has been an unauthorised use of the information. Information is likely to be regarded as confidential if sufficient steps are taken to control access.[23] Nevertheless, the mere encryption of information does not automatically render information confidential, especially if the information is accessible to anyone with the skills to decrypt the information.[24] Moreover, the mere fact of encryption does not necessarily amount to a communication importing an obligation of confidence, especially if the information has not been accessed surreptitiously.[25] On the other hand, if the circumstances in which the information is accessed are such that a reasonable person would regard the information as confidential, then surreptitious access is likely to be a breach of confidence.[26] Information that is generally accessible will not usually have the necessary quality of confidence merely because it is protected by access protection technology, unless there are additional protection measures, such as firewalls protecting an intranet.

b. Receiving protected data or material without authorisation or without paying the due remuneration.

In Australia, there are no laws that apply specifically to receiving protected data, or material without authorisation, or without paying the due remuneration.

In certain circumstances, however, a person who receives secret information may be liable for a breach of confidence. Recipients of information acquired in breach of confidence may be liable for using or disclosing the information if they have actual or constructive notice of the breach.[27] Liability arises from the time the recipient knows, or has reason to know, of the breach of confidence.[28]

c. Gaining access to a technologically protected computer system or to protected material by supplying a false name or password.

Supplying a false name or false password may, in certain circumstances, amount to a criminal offence of forgery, or of fraud (obtaining property by deception). There are significant differences in the operation of the various applicable Commonwealth, State and Territory criminal provisions. The main legal issue has been whether the offences are applicable in circumstances in which there is no deception of a human being, but merely the entry of false data into a machine.

---

[21] *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41; *Moorgate Tobacco Co Ltd v Philip Morris Ltd* (1984) 156 CLR 414.

[22] See *Franklin v Giddens* [1978] Qd R 72. Under English law there are apparently conflicting authorities. In *Malone v Metropolitan Police Commissioner* [1979] 2 All ER 620, it was held that police who obtained information by means of a lawful telephone tap were not liable for breach of confidence. In *Francome v Mirror Group Newspapers Ltd* [1984] 2 All ER 408, however, it was held that an unlawful telephone tap by a newspaper was a breach of confidence.

[23] For example, some English decisions have held that there may be a breach of confidence where photographs have been surreptitiously obtained despite security arrangements: *Creation Records Ltd v News Group Newspapers Ltd* (1997) 39 IPR 1 (Ch); *Shelley Films Ltd v Rex Features Ltd* [1994] EMLR 134 (Ch).

[24] *Mars UK Ltd v Teknowledge Ltd* (1999) 46 IPR 248.

[25] *Ibid.*

[26] For the reasonable person test see: *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41.

[27] *Fraser v Evans* [1969] 1 All ER 8; *Talbot v General Television Corporation Pty Ltd* [1980] VR 224; *Dart Industries Inc v David Bryar & Associates Pty Ltd* (1997) 38 IPR 389.

[28] *Nicrotherm Electrical Co Pty Ltd v Percy* [1956] RPC 272; *Printers & Finishers Ltd v Holloway* [1965] RPC 239.

Commonwealth

Section 29B of the *Crimes Act 1914* (Cth) establishes an offence for imposing a false representation upon the Commonwealth, or any public authority under the Commonwealth, with a view to obtaining money or any other benefit or advantage. The offence of imposition may be committed even though the representation has been made to a machine and has not come to the knowledge of a human agent.[29] In other words, the offence is complete upon the making of a false representation. Supplying a false name or false password may therefore constitute an offence under section 29B provided that:

1. the representation is imposed on the Commonwealth, or a Commonwealth public authority; and
2. the representation is imposed with a view to obtaining money or any other benefit or advantage.

Forgery offences under State and Territory laws

Supplying a false name or false password to a computer does not fall within the traditional offence of forgery.[30] This is because the traditional offence required both the making of a document in tangible form and the deception of a human being. Legislative amendments have relaxed these requirements in New South Wales, Victoria and the Australian Capital Territory.

Section 300 of the *Crimes Act 1900* (NSW) establishes offences for making or using a false instrument with the intention of inducing a person to accept the instrument as genuine and, as a result, acting to his or her prejudice or to the prejudice of another person. An "instrument" is broadly defined to include any "device on or in which information is recorded or stored by mechanical, electronic or other means".[31] The reference to inducing a person to accept the instrument as genuine is to be interpreted as including inducing a response from a machine that will prejudice a person.[32] Section 83A of the *Crimes Act 1958* (Vic) establishes a similar offence.[33] Like the New South Wales provision, a reference to inducing a person to accept a false document as genuine is to be interpreted as including a reference to causing a machine to respond to the document as if it were a genuine document.[34] Section 135C of the *Crimes Act 1900* (ACT) is to the same effect.[35] Each of these provisions may apply to supplying a false name or password to a computer, provided that doing so results in some prejudice to a person.

In South Australia, a "catch-all" provision makes it an offence to forge "any instrument or matter".[36] It is possible that this broad provision may apply to the supply of a false name or password.

Fraud (obtaining property by deception) under State and Territory laws

The traditional criminal offence of fraud, or obtaining property by deception, requires the deception of a human being.[37] This requirement has been modified in New South Wales and Victoria.

Section 178BA of the *Crimes Act 1900* (NSW) establishes an offence for dishonestly obtaining by deception any money, or valuable thing, or financial advantage. "Deception" is defined to include causing

---

[29] *R v Baxter* (1988) 1 Qd R 537.
[30] *R v Gold and Shifreen* [1988] AC 1063 (holding that the user segment of a computer system was not a "false instrument").
[31] *Crimes Act 1900* (NSW) s 299(1)(c).
[32] *Crimes Act 1900* (NSW) s 303.
[33] *Crimes Act 1958* (Vic) s 83A(1).
[34] *Crimes Act 1958* (Vic) s 83A(9).
[35] *Crimes Act 1990* (ACT) ss 135C, 135B(2), 93 (definition of "instrument").
[36] *Criminal Law Consolidation Act 1935* (SA) s 235.
[37] *Director of Public Prosecutions v Ray* [1973] 3 All ER 131 at 137 per Lord Morris; *Davies v Flackett* [1972] Crim LR 708; *Kennison v Daire* (1986) 60 ALJR 249; *R v Evenett* [1987] 2 Qd R 753.

a computer system or machine to make a response that the defendant is not authorised to cause the computer or machine to make.[38]

Section 81 of the *Crimes Act 1958* (Vic) establishes an offence of obtaining property from a person by deception, with the intention of permanently depriving the person of the property, and section 82 establishes an offence of obtaining financial advantage by deception. Like the New South Wales provision, "deception" is defined to include causing a computer system or machine to make a response that the defendant is not authorised to cause the computer or machine to make.[39] The term "financial advantage" may encompass a diversity of advantages, as the two words are to be given their plain meanings.[40]

The New South Wales and Victorian offences may apply to the supply of a false name or password, provided that the deception is practiced for the required purpose. Although the other States and Territories have criminal offences analogous to the offence of obtaining property by deception, the relevant provisions have not been extended to include entering false information into a computer system or a machine.

d. Gaining access to a technologically protected computer system or to protected material by supplying a false Internet Protocol (IP) address

Supplying a false IP address may, in certain circumstances, amount to a criminal offence of forgery, or of fraud (obtaining property by deception). The relevant legal provisions, and the issues involved with applying the provisions, are explained in paragraph 1c immediately above. In general terms, these provisions may apply to supplying a false IP address, provided the false information is supplied for the requisite purpose of obtaining property, or some financial advantage (depending upon the precise wording of the provision).

e. Gaining access to technologically protected material by supplying false payment information

Gaining access to protected material by supplying false payment information may amount to a number of criminal offences, depending upon the circumstances. If the false information is submitted to a computer, it may amount to the criminal offence of obtaining by deception under New South Wales or Victorian law. The offence of obtaining by deception is explained at paragraph 1c above. If the computer is operated by the Commonwealth, or a Commonwealth public authority, supplying false payment information may breach section 29B of the *Crimes Act 1914* (Cth). This offence is also explained at paragraph 1c above. If a person is deceived, the supply of false payment information may constitute a number of State or Territory offences relating to dishonest acquisition.[41]

f. Decrypting without authorisation encrypted content

Part VAA of the *Copyright Act 1968* (Cth) deals with the unauthorised decryption of "encoded broadcasts". The relevant provisions are explained at paragraph 3 below. Australian laws do not otherwise expressly prohibit unauthorised decryption. Nevertheless, unauthorised decryption may, in certain circumstances, amount to unauthorised access to a computer system, or to data stored on a computer. Commonwealth, State and Territory criminal laws prohibiting unlawful access are dealt with at paragraph 1a(i) above. Moreover, it is possible that, in certain circumstances, unauthorised decryption may constitute an offence prohibiting the unlawful alteration of data.[42] The application of laws prohibiting unlawful alteration to the unauthorised decryption of material is untested. Finally, in certain

[38] *Crimes Act 1900* (NSW) s 178BA(2).
[39] *Crimes Act 1958* (Vic) ss 81(4), 82(2).
[40] *Fisher v Bennett* (1987) 85 FLR 469; *R v Walsh* (1990) 52 A Crim R 80.
[41] For example, in *R v Lambie* [1981] 3 WLR 88 it was held that presenting a credit card after substantially exceeding a credit limit might amount to obtaining by deception.
[42] *Crimes Act 1914* (Cth) s 76C; *Crimes Act 1900* (NSW) s 310; Criminal Code (Tas) s 257C; *Crimes Act 1900* (ACT) s 135K; Criminal Code Act (NT) s 276.

circumstances, unauthorised decryption may amount to a breach of confidence. As explained at paragraph 1a(ii), however, mere encryption of information does not automatically mean that the information is confidential.

g. Overriding a limit on the number of simultaneous users allowed access or on the allowed time of access

In Australia, liability for overriding limitations on the number of users, or on the allowed time of access, depends primarily upon whether there has been a breach of contract. This may well involve consideration of unresolved legal issues, such as whether a "click-through" agreement constitutes a binding contract. The legal enforceability of "click-through" agreements is dealt with further at paragraph 8b1 below. In the absence of a contractual relationship, recourse must be had to other forms of liability. For example, if confidential information is disclosed for a limited purpose, access to the information for another purpose may amount to a breach of confidence.[43] Furthermore, where there is an express or implied limitation on the conditions of access, if access is obtained otherwise than in accordance with the limitation there may be a contravention of one of the criminal provisions that prohibit unauthorised access.[44] Criminal laws prohibiting unauthorised access are dealt with at paragraph 1a(i) above.

h. Overriding a limit on the number of copies an authorised user is permitted to make, or a technologically enforced prohibition against making *any* copies?

In Australia, liability for overriding a limit on the number of copies that an authorised user may make depends primarily on contract law. As explained at paragraph 1g above, making unauthorised copies may, in appropriate circumstances, amount to a breach of confidence or contravene a criminal provision that prohibits unauthorised access. Similarly, enforcement of copy protection technologies depends mainly on contract law, but may amount to a breach of confidence or contravene a criminal provision that prohibits unauthorised access.

2. <u>General tort law rules of direct or secondary liability</u>

a. Under your country's general tort law principles, could a person be held liable for having engaged in an act of circumvention or for having manufactured or distributed a circumvention device? What would be the conditions for liability?

Under Australian law, it would be difficult for tort liability to be established for an act of circumvention. In most cases of circumvention, the elements of an intentional tort in relation to goods, such as trespass to goods, will not be made out. The intentional torts are unlikely to apply, as it is necessary to establish some interference or dealing with "goods". Circumvention will usually be for the purpose of accessing information. Information is not conventionally regarded as a "good" and, consequently, mere unauthorised access cannot constitute an intentional tort in relation to goods, such as trespass to goods.[45]

Establishing tort liability for the manufacture or distribution of a circumvention device may also present difficulties. It is possible that an action for negligence could be brought against a manufacturer or distributor. In general terms, negligence will be made out if the plaintiff establishes that there is a duty of care, a breach of the duty and damages resulting from the breach.[46] The liability of a manufacturer or distributor will depend principally upon whether a duty of care is owed to a person who suffers loss as a result of the manufacture or distribution of a circumvention device. The damage resulting from the manufacture or distribution of a circumvention device is likely to be "pure economic loss". In Australia,

---

[43] See, for example, *Smith, Kline & French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health* (1991) 20 IPR 643.
[44] *Director of Public Prosecutions v Murdoch* [1993] 1 VR 406.
[45] For the subject matter of an action for conversion see: *Doodeward v Spence* (1908) 6 CLR 406.
[46] *Donoghue v Stevenson* [1932] AC 562.

there is no general exclusionary principle in negligence that prevents recovery of damages for economic loss that is not consequential upon injury to person or property.[47] At the same time, there is no unifying principle for determining liability for negligence in cases of "pure economic loss". Instead, Australian courts have adopted an incremental approach to determining liability, taking into account a number of "policy" considerations.[48] Holding a manufacturer or distributor of a circumvention device liable in negligence for loss resulting from use of the device would involve extending liability in accordance with this "incremental approach". Given the current state of the law, it is difficult to predict the outcome of an action in negligence for the manufacture or distribution of a circumvention device.

b. Has your country's case law already applied tort law to prohibit or to enjoin the act of circumventing or the manufacture or distribution of a circumvention device? Are knowledge or intent required? How have knowledge or intent been defined? Is the liability of manufacturers and distributors of devices direct, or based on secondary liability (contributory or vicarious)?

Australian courts have not applied tort law to the act of circumventing, or to the manufacture or distribution of a circumvention device. As explained above, the application of Australian tort law to these activities would involve an extension of current legal principles.

3. Broadcasting law, cable and satellite regulations, protection of encrypted services or broadcasts, protection of conditional access services

a. Are encrypted services or broadcasts (eg pay-TV signals, etc) legally protected in your country? Is the regulation civil, administrative, criminal or public? What is the rationale for this regulation?

(i) Are encrypted broadcasts legally protected?

Encrypted broadcasting services are protected under Part VAA of the *Copyright Act 1968* (Cth), a new addition to Australian copyright law that was inserted by the *Copyright Amendment (Digital Agenda) Act 2000* (Cth). The protection of encrypted broadcasts in Australia does not focus on the private act of decrypting encrypted broadcasting services. Rather, the focus of part VAA is on making, importing, commercially dealing with, making available online or commercially using "broadcast decoding devices".

(ii) Is the regulation civil, administrative, criminal or public?

Part VAA establishes civil rights of action and criminal offences for certain dealings with "broadcast decoding devices".

(iii) What is the rationale for this regulation?

The *Second Reading Speech* to the legislation that introduced Part VAA stated that the provisions in that Part "will enable subscription broadcasters to control the reception of their encoded broadcasts".[49] The legislation was subsequently amended to extend to encoded broadcasts delivered by commercial or national broadcasting services. Part VAA is therefore intended to enable broadcasters to control access to "encoded broadcasts".

---

[47] *Caltex Oil (Australia) Pty Ltd v The Dredge "Willemstad"* (1976) 136 CLR 529; *Perre v Apand Pty Ltd* (1999) 73 ALJR 1190.

[48] *Perre v Apand Pty Ltd* (1999) 73 ALJR 1190.

[49] Hon. Darryl Williams, Attorney-General, Copyright Amendment (Digital Agenda) Bill 1999, *Second Reading Speech,* Commonwealth of Australia, *Parliamentary Debates,* House of Representatives, 2 September 1999, p 2751.

Part VAA does not prohibit the private, non-commercial use of "broadcast decoding devices". The *Revised Explanatory Memorandum* to the Copyright Amendment (Digital Agenda) Bill 2000 (Cth) explained the reasons for this approach in the following terms:

> … it is the Government's view that the main threat to subscription broadcasters is not the single act of unauthorised reception by individuals, but rather the preparatory acts carried out by commercial companies, and the unauthorised use of such devices to promote commercial activities.[50]

The provisions regulating the use of "broadcast decoding devices" adopt the same general approach as the provisions in new Division 2A of Part V of the *Copyright Act 1968* (Cth), which were introduced to prohibit the circumvention of technological measures for protecting copyright.

b. In such legislation, is the decryption, descrambling or any other form of unauthorised interception of encrypted services or broadcasts prohibited? Under what conditions? What are the rationale and purpose for such prohibition? What are the services or programs at issue? Is protection available only if the broadcast or transmission requires payment? (ie, no protection for free broadcasts of transmissions?) Who may bring a claim? What remedies are available?

(i) Prohibited use of broadcast decoding devices

Section 135ANA of the *Copyright Act 1968* (Cth) establishes a civil right of action for the unauthorised commercial use of a "broadcast decoding device". Under Part VAA of the *Copyright Act 1968* (Cth), a "broadcast decoding device" is defined to mean:

> … a device (including a computer program) that is designed or adapted to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster by circumventing, or facilitating the circumvention of, the technical means or arrangements that protect access in an intelligible form to the broadcast.[51]

An "encoded broadcast" is defined to mean either of two kinds of broadcasts. The first kind of "encoded broadcast" is one that is:

> … made available only to persons who have the prior authorisation of the broadcaster and only on payment by such persons of subscription fees (whether periodically or otherwise).[52]

The second kind of "encoded broadcast" is a television broadcast (other than the first kind of "encoded broadcast") that is delivered by a commercial or national broadcasting service and to which access in an intelligible form is protected by a technical measure or arrangement (including a computer program).[53]

---

[50] Copyright Amendment (Digital Agenda) Bill 2000 (Cth), *Revised Explanatory Memorandum,* Part VAA, Item 240.

[51] *Copyright Act 1968* (Cth) s 135AL (definition of "broadcast decoding device").

[52] *Copyright Act 1968* (Cth) s 135AL (definition of "encoded broadcast" (a)).

[53] *Copyright Act 1968* (Cth) s 135AL (definition of "encoded broadcast"(b)). "Commercial broadcasting services" are essentially "free-to-air" broadcasting services that appear to be intended to appeal to the general public and that are usually funded by advertising revenue: *Broadcasting Services Act 1992* (Cth) s 14. "National broadcasting services" are essentially broadcasting services, other than subscription services, that are provided by the government-funded broadcasters, the Australian Broadcasting Corporation or the Special Broadcasting Service: *Broadcasting Services Act 1992* (Cth) s 13.

(ii) Elements of action for unauthorised commercial use of broadcast decoding device

Under section 135ANA, a broadcaster has a civil action for the unauthorised "commercial" use of "broadcast decoding devices" if each of the following four conditions are satisfied:

1. the broadcaster[54] makes an "encoded broadcast";
2. a person uses (or authorises the use of) a broadcast decoding device to gain access to an encoded broadcast without the authorisation of the broadcaster;
3. the person uses (or authorises the use of) the device for the purposes of a trade or business; and
4. the person knew, or ought reasonably to have known, that the broadcaster had not authorised access to the broadcast by use of the device.[55]

(iii) Rationale and purpose of prohibition

As explained at 3a(iii) above, the *Second Reading Speech* to the legislation that introduced Part VAA stated that the provisions in that Part were essentially intended to enable broadcasters to control the reception of "encoded broadcasts". This appears to be the main objective of section 135ANA.

Although the main purpose of Part VAA is to allow broadcasters to control access to "encoded broadcasts", it may be significant that the provisions are included as part of Australian copyright law, not part of broadcasting law. A second possible purpose for the prohibition in section 135ANA was suggested in the *Revised Explanatory Memorandum* to the Copyright Amendment (Digital Agenda) Bill 2000 (Cth), which stated that the provision was intended to:

> …protect the commercial interests of copyright owners and focus the remedy on public and commercial activities rather than use by individuals.[56]

Therefore, like the general provisions relating to the use of anti-circumvention devices introduced by the *Copyright Amendment (Digital Agenda) Act 2000* (Cth),[57] the action for unauthorised use of a "broadcast decoding device" is also apparently intended to supplement the rights of copyright owners.

A potential obstacle to this interpretation of the purpose of section 135ANA is that the civil right of action is vested in the "broadcaster", not in the owner or licensee of copyright in the broadcast. A possible explanation for this is that, in Australia, copyright in a broadcast does not confer rights in relation to reception of a broadcast, only to transmission. It therefore seems that the prohibition on commercial use of a "broadcast decoding device" in section 135ANA is aimed both at allowing broadcasters to control reception of "encoded broadcasts" and supplementing the rights of owners of copyright in broadcast transmissions.

(iv) Services to which the prohibition applies

The civil action for unauthorised use of a "broadcast decoding device" applies to "encoded broadcasts". An "encoded broadcast" is either:

---

[54] For the purposes of Part VAA, a "broadcaster" is defined as "a person who makes an encoded broadcast": *Copyright Act 1968* (Cth) s 135AL (definition of "broadcaster"). The person who makes a broadcast is the person who provides the broadcasting service by which the broadcast is delivered: *Copyright Act 1968* (Cth) s 22(5).

[55] *Copyright Act 1968* (Cth) s 135ANA(1).

[56] Copyright Amendment (Digital Agenda) Bill 2000 (Cth), *Revised Explanatory Memorandum,* Clause 135ANA, Para 256. The *Revised Explanatory Memorandum* also stated that section 135ANA "is intended to include a remedy against the use of a decoding device to allow reception in a premises such as a hotel or pub even though no payment is required from patrons to watch the broadcast".

[57] *Copyright Act 1968* (Cth), Part V, Division 2A.

1. a broadcast[58] that is made available only to persons who have the prior authorisation of the broadcaster and only on payment of subscription fees; or
2. a television broadcast (other than the first kind of "encoded broadcast") that is delivered by a commercial or national broadcasting service, access to which in an intelligible form is protected by a technical measure or arrangement.[59]

(v) Is protection available only if the broadcast or transmission requires payment?

In addition to services available only on payment of subscription fees, an action may apply in relation to encoded "free-to-air" commercial or national television broadcasting services. Thus, the action will apply to a commercial or national television broadcasting service if access to the service in an intelligible form is protected by a technical measure or arrangement (including a computer program).[60]

(vi) Who may bring a claim?

The civil action for unauthorised commercial use of a broadcast decoding device may be brought by a "broadcaster".[61] A "broadcaster" is the person who makes the "encoded broadcast", which means the person who provides the broadcasting service by means of which the encoded broadcast is delivered.[62]

(vii) What remedies are available?

The main remedies available for an action for unauthorised commercial use of a "broadcast decoding device" are an injunction, and either damages or an account of profits.[63] In certain circumstances, the courts may also award additional damages.[64] In awarding additional damages, the court must have regard to the flagrancy of the unauthorised use and any benefit shown to have accrued to the defendant. In an action for unauthorised use the court may also direct that the "broadcast decoding device" be destroyed, or otherwise dealt with, including delivery up to the broadcaster.[65]

c. Is the distribution of devices that enable or facilitate circumvention illicit? What are the criteria for considering a device to be illicit? For example, is there a requirement of knowledge or intent to engage in or facilitate illicit circumvention? What commercial/private activities related to that device are prohibited (manufacture, distribution, sale, possession, etc)? How does the law address devices that potentially have licit and illicit purposes? Who may bring a claim? What remedies are available?

(i) Distribution of "broadcast decoding devices"

Section 135AN of the *Copyright Act 1968* (Cth) establishes a civil action in relation to certain dealings with "broadcast decoding devices". The action applies in relation to the following activities (hereafter referred to as "prohibited commercial activities"):

---

[58] A "broadcast" is defined to mean "a communication to the public delivered by a broadcasting service within the meaning of the *Broadcasting Services Act 1992* (Cth)": *Copyright Act 1968* (Cth) s 10(1) (definition of "broadcast").
[59] *Copyright Act 1968* (Cth) s 135AL (definition of "encoded broadcast").
[60] *Ibid.*
[61] *Copyright Act 1968* (Cth) s 135ANA(3).
[62] *Copyright Act 1968* (Cth) ss 135AL, 22(5).
[63] *Copyright Act 1968* (Cth) s 135ANA(4).
[64] *Copyright Act 1968* (Cth) s 135ANA(5).
[65] *Copyright Act 1968* (Cth) s 135ANA(6).

1. making a "broadcast decoding device";
2. selling, letting for hire, or offering or exposing for sale or hire, a "broadcast decoding device";
3. distributing a "broadcast decoding device" for the purpose of trade, or for any purpose that will affect prejudicially the broadcaster;
4. exhibiting a "broadcast decoding device" in public by way of trade;
5. importing a "broadcast decoding device" for any of the above commercial purposes;
6. making a "broadcast decoding device" available online to an extent that will affect prejudicially the broadcaster.[66]

Section 135AS establishes criminal offences in relation to the above "prohibited commercial activities". There is no criminal offence for the use of a "broadcast decoding device".

The distribution of "broadcast decoding devices" is therefore unlawful provided that the distribution is for a commercial purpose, or a purpose that will otherwise affect the broadcaster prejudicially. Moreover, making a "broadcast decoding device" available online is unlawful if doing so will "affect prejudicially" the broadcaster.

(ii) What are the criteria for considering a device to be illicit?

Under section 135AN of the *Copyright Act 1968* (Cth), three elements must be established for there to be a civil action in relation to a "broadcast decoding device". Accordingly, a civil action in relation to a commercial dealing with a "broadcast decoding device" will apply if:

1. a broadcaster makes an "encoded broadcast";[67]
2. the defendant commits a "prohibited commercial activity" in relation to a "broadcast decoding device"; and
3. the defendant knew, or ought reasonably to have known, that the device would be used for gaining unauthorised access to an encoded broadcast.[68]

Thus, a broadcaster may have a civil action in relation to the commercial distribution of a "broadcast decoding device" provided the broadcaster makes an "encoded broadcast" and the defendant knew, or ought reasonably to have known, that the device would be used to gain unauthorised access to the broadcast.

Under section 135AS of the *Copyright Act 1968* (Cth), a criminal offence is committed in relation to a "broadcast decoding device" if:

1. the defendant commits a "prohibited commercial activity" in relation to the device; and
2. the defendant knows, or is reckless as to whether, the device will be used to gain unauthorised access to an "encoded broadcast".[69]

The commercial distribution of a "broadcast decoding device" will therefore constitute a criminal offence if the defendant knows, or is reckless as to whether, the device will be used to gain unauthorised access to an "encoded broadcast".

(iii) Is there a requirement of knowledge or intent to engage in or facilitate illicit circumvention?

For a civil action to arise, the defendant must have actual or constructive knowledge that a "broadcast decoding device" will be used to gain unauthorised access to an "encoded broadcast".[70]

---

[66] *Copyright Act 1968* (Cth) s 135AN(1)(b).
[67] For the definition of "encoded broadcast" see paragraph 3b above
[68] *Copyright Act 1968* (Cth) s 135AN(1).
[69] *Copyright Act 1968* (Cth) s 135AS(1).
[70] *Copyright Act 1968* (Cth) s 135AN(1)(c).

For a criminal offence to be committed, the defendant must know, or be reckless as to whether, the device will be used to gain unauthorised access to an "encoded broadcast".[71]

(iv) What commercial/private activities related to that device are prohibited (manufacture, distribution, sale, possession, etc)?

Civil and criminal actions apply in relation to the following commercial activities:

1. making a "broadcast decoding device";
2. selling, letting for hire, or offering or exposing for sale or hire, a "broadcast decoding device";
3. distributing a "broadcast decoding device" for the purpose of trade, or for any purpose that will affect prejudicially the broadcaster;
4. exhibiting a "broadcast decoding device" in public by way of trade;
5. importing a "broadcast decoding device" for any of the above commercial purposes;
6. making a "broadcast decoding device" available online to an extent that will affect prejudicially the broadcaster.[72]

As explained at paragraph 3b(ii) above, a civil action may apply in relation to the use of a "broadcast decoding device" if the use is for the purposes of a trade or business.[73]

Part VAA of the *Copyright Act 1968* (Cth) does not prohibit the private, non-commercial use of a "broadcast decoding device".

(v) How does the law address devices that potentially have licit and illicit purposes?

Section 135AL of the *Copyright Act 1968* (Cth) defines a "broadcast decoding device" as a device "that is designed or adapted" to gain unauthorised access to a broadcast by circumventing technical means of protection. The extent to which a device may be used for potentially lawful purposes is therefore largely irrelevant to the definition of a "broadcast decoding device".

Part VA of the *Copyright Act 1968* (Cth) distinguishes between potentially lawful and unlawful purposes of "broadcast decoding devices" by restricting civil and criminal actions to certain unlawful activities, and requiring a mental element for both civil and criminal actions.

First, a civil or criminal action arises only if the defendant commits certain "prohibited commercial activities" in relation to a "broadcast decoding device", including making, selling, hiring, commercially distributing or exhibiting, or importing the device, or making the device available online. A civil action for using a device is available only in relation to use of the device for the purposes of a trade or business.

Secondly, an action will arise only if the defendant has the requisite mental element. Thus, a civil action is available in relation to a "prohibited commercial activity" only if the defendant knew, or ought reasonably to have known, that the device would be used to gain unauthorised access to an "encoded broadcast". Similarly, an action for the unlawful commercial use of a device arises only if the defendant knew, or ought reasonably to have known, that the broadcaster had not authorised the defendant to gain access to the broadcast by using the device. A criminal offence is committed in relation to a "prohibited commercial activity" only if the defendant knows, or is reckless as to whether, the device will be used to gain unauthorised access to an "encoded broadcast".

[71] *Copyright Act 1968* (Cth) s 135AS(1).
[72] *Copyright Act 1968* (Cth) ss 135AN(1)(b), 135(1)(a)-(f).
[73] *Copyright Act 1968* (Cth) s 135ANA(1).

(vi) Who may bring a claim?

A civil action for "prohibited commercial activities" (including commercial distribution) in relation to a "broadcast decoding device" may be brought by a "broadcaster".[74] A "broadcaster" is the person who makes the "encoded broadcast", which means the person who provides the broadcasting service by means of which the encoded broadcast is delivered.[75]

(vi) What remedies are available?

The main remedies available for an action for "prohibited commercial activities" in relation to a "broadcast decoding device" are an injunction, and either damages or an account of profits.[76] In certain circumstances, the courts may also award additional damages.[77] In awarding additional damages, the court must have regard to the flagrancy of the unauthorised use and any benefit shown to have accrued to the defendant. In an action for unauthorised use the court may also direct that the "broadcast decoding device" be destroyed, or otherwise dealt with, including delivery up to the broadcaster.[78]

In a criminal prosecution, regardless of whether the defendant is convicted, the court may order the destruction of a "broadcast decoding device", or that the device be otherwise dealt with.[79]

d. Are there circumstances in which circumvention or decryption is authorised or exempted from the prohibition? How have courts in your country applied the prohibitions (or exceptions) to circumventing technological protections for broadcasts and transmissions?

(i) Are there circumstances in which circumvention or decryption is authorised or exempted from the prohibition?

The prohibitions in relation to "broadcast decoding devices" apply only in relation to "prohibited commercial activities" or to the use of a device for the purposes of a trade or business. Part VAA of the *Copyright Act 1968* (Cth) does not prohibit the private, non-commercial use of a "broadcast decoding device".

The provisions establishing civil and criminal actions in relation to "broadcast decoding devices" expressly exempt activities that are "lawfully done for the purposes of law enforcement or national security".[80] To fall within the exemption, the actions must be undertaken by or on behalf of the Commonwealth or a State or Territory, or a Commonwealth, State or Territory authority.

(ii) How have courts in your country applied the prohibitions (or exceptions) to circumventing technological protections for broadcasts and transmissions?

Australian courts have not yet applied the prohibitions or exceptions relating to the circumvention of "encoded broadcasts" contained in Part VAA of the *Copyright Act 1968* (Cth).

e. Do you consider these legal provisions as adequate and effective?

The most significant limitation on the prohibitions in Part VAA of the *Copyright Act 1968* (Cth) is that they do not directly prohibit private, non-commercial uses of "broadcast decoding devices". Prior to the legislation passing Parliament, a report on the legislation by the House of Representatives Standing

[74] *Copyright Act 1968* (Cth) s 135AN(3).
[75] *Copyright Act 1968* (Cth) ss 135AL, 22(5).
[76] *Copyright Act 1968* (Cth) s 135AN(4).
[77] *Copyright Act 1968* (Cth) s 135AN(5).
[78] *Copyright Act 1968* (Cth) s 135AN(6).
[79] *Copyright Act 1968* (Cth) s 135AU.
[80] *Copyright Act 1968* (Cth) ss 135AN(2), 135ANA(2), 135AS(2).

Committee on Legal and Constitutional Affairs concluded that Part VAA should be strengthened by including a criminal offence for dishonestly receiving a broadcast with intent to avoid payment of an applicable charge.[81] The Standing Committee considered that the possibility of a criminal sanction would provide an important deterrent against personal use of unauthorised decoding devices. The Standing Committee's recommendations in favour of an additional criminal offence were not incorporated in the final legislation. It remains to be seen whether the existing provisions on commercial activities relating to "broadcast decoding devices" are sufficient to deter the private use of devices to circumvent "encoded broadcasts". If private circumvention becomes widespread in Australia, it may be that the legislation will need to be amended in line with the Standing Committee's recommendations.

f. "Conditional access" services

1. Is there a similar protection in your country? In which legal regime (broadcasting law or other)?

To a certain extent, Part VAA of the *Copyright Act 1968* (Cth) performs functions similar to the European *Directive on the legal protection of services based on, or consisting of, conditional access.*[82] Thus, the *Revised Explanatory Memorandum* to the Copyright Amendment (Digital Agenda) Bill 2000 (Cth) stated that "elements" of Part VAA were "drawn from the *European Council Directive on the legal protection of services based on, or consisting of, conditional access".*[83] Nevertheless, Part VAA does not apply to all services encompassed by the *Conditional Access Directive,* its operation being limited to "encoded broadcasts".

2. If yes, what is the rationale for protection?

As explained at paragraph 3a(iii) above, Part VAA of the *Copyright Act 1968* (Cth) is intended to enable broadcasters to control reception of "encoded broadcasts". As explained at paragraph 3b(iii) above, Part VAA may also be intended to supplement the rights of owners of copyright in a broadcast.

Which services are covered?

Part VAA applies to "encoded broadcasts". As explained at paragraph 3b(iv) above, there are two kinds of "encoded broadcast":

1. a broadcast that is made available only to persons who have the prior authorisation of the broadcaster and only on payment of subscription fees; and
2. a television broadcast (other than the first kind of encoded broadcast) delivered by a commercial or national broadcasting service, access to which in an intelligible form is protected by a technical measure or arrangement (including a computer program).[84]

The *Copyright Act 1968* (Cth) defines a "broadcast" to mean "a communication to the public delivered by a broadcasting service within the meaning of the *Broadcasting Services Act 1992* (Cth)".[85] Under section 6 of the *Broadcasting Services Act 1992* (Cth), a "broadcasting service" is defined as:

---

[81] House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on Copyright Amendment (Digital Agenda) Bill 1999* (November 1999, Canberra), Recommendation 22, para 5.15, p 85.

[82] *Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the Legal Protection of Services Based On, or Consisting of, Conditional Access,* [1998])J L320/54 ("the *Conditional Access Directive").*

[83] Copyright Amendment (Digital Agenda) Bill 2000 (Cth), *Revised Explanatory Memorandum,* Part VAA, para 240.

[84] *Copyright Act 1968* (Cth) s 135AL (definition of "encoded broadcast").

[85] *Copyright Act 1968* (Cth) s 10(1) (definition of "broadcast").

> … a service that delivers television programs or radio programs to persons having equipment appropriate for receiving that service, whether the delivery uses the radiofrequency spectrum, cable, optical fibre, satellite or any other means or a combination of those means, but does not include:
>
> (a) a service (including a teletext service) that provides no more than data, or no more than text (with or without associated still images); or
> (b) a service that makes programs available on demand on a point-to-point basis, including a dial-up service; or
> (c) a service, or a class of services, that the Minister determines, by notice in the *Gazette,* not to fall within this definition.[86]

To clarify the position of Internet streaming, the Minister has made a determination under paragraph (c) of the definition of a "broadcasting service".[87] The determination provides that the following kind of service does not fall within the definition:

> a service that makes available television programs or radio programs using the internet, other than a service that delivers television programs or radio programs using the broadcasting services bands.

An "encoded broadcast" under Part VAA therefore does not include "Information Society Services" such as video or audio-on-demand (excluded under paragraph (b) of the definition of a "broadcasting service"); on-line access to a database (excluded under paragraph (a) of the definition of a "broadcasting service"); or video or audio Internet streaming (excluded by the Ministerial determination under paragraph (c) of the definition of a "broadcasting service").

What are the requirements for protection?

A civil action is available in relation to a service protected under Part VAA if the following requirements are met:

1. a broadcaster makes an "encoded broadcast";
2. the defendant commercially uses, or commits a "prohibited commercial activity" in relation to, a "broadcast decoding device"; and
3. the defendant knows, or has constructive knowledge, that use of the device is unauthorised, or that the device would be used to obtain unauthorised access.

The elements of civil actions under Part VAA are explained in more detail at paragraphs 3b and 3c above.

Is the circumvention of the conditional access measure and/or the circumvention device prohibited?

Section 135ANA of the *Copyright Act 1968* (Cth) establishes a civil action for the unauthorised "commercial" use of a "broadcast decoding device." This section therefore operates to prohibit "circumvention" for a commercial purpose. Section 135ANA is explained in more detail at paragraph 3b above.

Section 135AN of the *Copyright Act 1968* (Cth) establishes civil actions for "prohibited commercial activities" committed in relation to "broadcast decoding devices". Section 135AS of the *Copyright Act 1968* (Cth) establishes criminal offences for "prohibited commercial activities" committed in relation to "broadcast decoding devices". These provisions are directed at preventing the manufacture, distribution

---

[86] *Broadcasting Services Act 1992* (Cth) s 6 (definition of "broadcasting service").
[87] *Determination under paragraph (c) of the definition of "broadcasting service" (No 1 of 2000),* Notified in *Gaz GN38* of 27 September 2000.

and sale of circumvention devices ("broadcast decoding devices") rather than the actual circumvention of "encoded broadcasts". Sections 135AN and 135AS are explained in more detail at paragraph 3c above.

Which activities related to circumvention devices are prohibited?

Section 135ANA prohibits the use of a "broadcast decoding device" for the purposes of a trade or business.

Sections 135AN and 135AS prohibit the following activities:

1. making a "broadcast decoding device";
2. selling, letting for hire, or offering or exposing for sale or hire, a "broadcast decoding device";
3. distributing a "broadcast decoding device" for the purpose of trade, or for any purpose that will affect prejudicially the broadcaster;
4. exhibiting a "broadcast decoding device" in public by way of trade;
5. importing a "broadcast decoding device" for any of the above commercial purposes;
6. making a "broadcast decoding device" available online to an extent that will affect prejudicially the broadcaster.

3. "Information Society Services"

Does your legislation on conditional access concern information society services as well? In other words, could your conditional access legislation be applied to services provided through the Internet or other networks?

As explained at paragraph 3f2 above, Part VAA of the *Copyright Act 1968* (Cth) does not apply to "information society services". This is principally because the definition of an "encoded broadcast" in Part VAA is linked to the definition of a "broadcasting service" under the *Broadcasting Services Act 1992* (Cth). The definition of a "broadcasting service" excludes on-demand video and audio services (under paragraph (b) of the definition) and services delivered by means of the Internet (under a Ministerial determination pursuant to paragraph (c) of the definition).

4. <u>Telecommunications Law</u>

a. Telecommunications law sometimes prohibits unauthorised interception of any wire or electronic communication. This could serve as a basis for a claim against decryption or any other unauthorised means of getting access to data when transmitted over telecommunication networks. Does your country's telecommunications law include such a prohibition?

Under Australian law, the unlawful interception of communications by means of a telecommunications system is dealt with by the *Telecommunications (Interception) Act 1979* (Cth). The *Telecommunications (Interception) Act 1979* (Cth) also prohibits unlawful dealing with intercepted information. The disclosure of the contents of communications carried by a telecommunications system by "eligible persons", including carriers, is dealt with under Part 13 of the *Telecommunications Act 1997* (Cth). A number of criminal offences, including offences relating to interception devices, are established by Part VIIB of the *Crimes Act 1914* (Cth).

1. Which acts are concerned (interception, disclosure, unauthorised access, reception, etc)?

Unlawful interception of telecommunications

Section 7 of the *Telecommunications (Interception) Act 1979* (Cth) is the main provision dealing with the unlawful interception of telecommunications services in Australia. Section 7 prohibits a person from:

1. intercepting;
2. authorising, suffering or permitting another person to intercept; or
3. doing any act or thing that will enable him or her or another person to intercept;

a communication passing over a telecommunications system.[88]

Section 6 of the *Telecommunications (Interception) Act 1979* (Cth) provides that "interception" of a communication "consists of listening to or recording, by any means, such a communication in its passage over … (a) … telecommunications system without the knowledge of the person making the communication".[89]

A "communication" is defined to include "conversation and a message, and any part of a conversation or message".[90] A "telecommunications system" is essentially defined to mean "a telecommunications network that is within Australia".[91] A "telecommunications network" is defined as a "system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or series of systems, for carrying communications solely by means of radiocommunication".[92] This means that the *Telecommunications (Interception) Act 1979* (Cth) does not deal with communications solely by means of the radio-frequency spectrum.[93] As most mobile communications use fixed links in addition to the radio-frequency spectrum, interception of such communications falls within the prohibition.[94]

The unlicensed operation of radiocommunications devices and the unlawful possession of radiocommunications devices is dealt with under the *Radiocommunications Act 1992* (Cth).[95] Furthermore, section 197 of the *Radiocommunications Act 1992* (Cth) creates an offence for knowingly or recklessly causing interference to radiocommunications.

There are conflicting authorities in relation to whether the recording of a communication after it has passed through a telecommunications system, for example by a recording device external to a telephone handset, amounts to a prohibited interception.[96] For example, a recording made by a microphone that was not physically connected to a telephone handset has been held not to be an unlawful interception.[97] Recording private communications, other than communications passing over a telecommunications system, is

---

[88] *Telecommunications (Interception) Act 1979* (Cth) s 7(1).
[89] *Telecommunications (Interception) Act 1979* (Cth) s 6(1). In relation to an interception, "record" is defined to mean: "(i) a record or copy, whether in writing or otherwise, of the whole or a part of the communication, being a record or copy made by means of the interception; or (ii) a record or copy, whether in writing or otherwise, of the whole or a part of a record or copy that is, by virtue of any other application or applications of this definition, a record obtained by the interception": *Telecommunications (Interception) Act 1979* (Cth) s 5 (definition of "record").
[90] *Telecommunications (Interception) Act 1979* (Cth) s 5 (definition of "communication").
[91] *Telecommunications (Interception) Act 1979* (Cth) s 5 (definition of "telecommunications system").
[92] *Telecommunications (Interception) Act 1979* (Cth) s 5 (definition of "telecommunications network").
[93] *Radiocommunications Act 1992* (Cth) ss 6, 8.
[94] *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222.
[95] *Radiocommunications Act 1992* (Cth) ss 46, 47.
[96] *R v Migliorini* (1981) 38 ALR 356; *R v Curran and Torney* [1983] 2 VR 1333; *R v Oliver* (1985) 57 ALR 543; *Clyne v Bowman* (1987) 11 NSWLR 341.
[97] *R v Oliver* (1985) 57 ALR 543.

prohibited under State and Territory "listening devices" legislation.[98] The State and Territory laws do not apply to the interception of telecommunications.[99]

Unlawful "dealing" with intercepted information

Section 63 of the *Telecommunications (Interception) Act 1979* (Cth) prohibits unlawful dealing with intercepted information. It prohibits a person from:

1. communicating to another person, making use of, or making a record of; or
2. giving in evidence in a proceeding;

information obtained by the lawful or unlawful interception of a communication passing over a telecommunications system.[100] "Communicate", in relation to information, is defined to include "divulge".[101]

This provision therefore prohibits a broad range of activities in relation to intercepted information, unless the activities fall within one of the exceptions established under the interception legislation. It clearly extends to disclosure of intercepted information, but does not expressly prohibit reception of intercepted material.

Disclosure by carriers, carriage service providers and persons in the telecommunications business of information acquired in connection with carrying telecommunications

Part 13 of the *Telecommunications Act 1997* (Cth) deals with the disclosure of the contents of communications carried by carriers and carriage service providers by "eligible persons". Section 276 prohibits an "eligible person" from disclosing or using any information or document that relates to the contents or substance of a communication that has been carried, or is being carried, by a carrier or carriage service provider.[102] An "eligible person" is a carrier, a carriage service provider, an employee of a carrier or carriage service provider, or a telecommunications contractor or employee of a telecommunications contractor.[103]

The telecommunications legislation defines the terms, "carrier" and "carriage service provider", by means of a complex series of interlocking definitions. A "carrier" is essentially a person who owns the elements of a telecommunications network that are used to supply telecommunications services to the public.[104] A "carriage service provider" is essentially a person who supplies a telecommunications service to the public by means of telecommunications networks operated by carriers.[105] Section 276 operates to prohibit the use or disclosure of information acquired by an "eligible person" in connection with the person's business or employment.[106] A number of exceptions to the prohibitions on disclosure, or use, of intercepted information by "eligible persons" are established under Part 13.[107]

---

[98] *Listening Devices Act 1992* (ACT); *Listening Devices Act 1990* (NT); *Listening Devices Act 1984* (NSW); *Invasion of Privacy Act 1971* (Qld); *Listening Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Listening Devices Act 1978* (WA).
[99] *Miller v Miller* (1979) 141 CLR 269 at 275-76; *R v Curran* [1983] 2 VR 133; *R v McHardie* [1983] 2 NSWLR 733; *Edelsten v Investigating Committee of NSW* (1986) 7 NSWLR 222.
[100] *Telecommunications (Interception) Act 1979* (Cth) ss 63(1), 6E(1) (definition of "lawfully obtained information").
[101] *Telecommunications (Interception) Act 1979* (Cth) s 5 (definition of "communicate").
[102] *Telecommunications Act 1997* (Cth) s 276(1)(a).
[103] *Telecommunications Act 1997* (Cth) s 271.
[104] *Telecommunications Act 1997* (Cth) ss 7, 42, 26-29, 7 (definition of "carriage service").
[105] *Telecommunications Act 1997* (Cth) ss 87, 16, 7 (definition of "carriage service").
[106] *Telecommunications Act 1997* (Cth) s 276(1)(b).
[107] *Telecommunications Act 1997* (Cth) Part 13, Division 3, Subdivision A.

Wrongful delivery of communications

Section 85ZD of the *Crimes Act 1914* (Cth) establishes a criminal offence in relation to the "wrongful delivery" of a communication over a telecommunications system. It prohibits a person from knowingly, or recklessly, causing a communication in the course of telecommunications carriage to be received by a person (or service) other than the person (or service) to whom it is directed. The provision applies to communications being carried by a carrier or carriage service provider, but does not apply to communications solely by means of the radio-frequency spectrum.[108]

Does the law cover interception devices as well?

Criminal offences in relation to telecommunications interception devices are established under Part VIIB of the *Crimes Act 1914* (Cth).

Section 85ZKB of the *Crimes Act 1914* (Cth) makes it a criminal offence to manufacture; advertise, display or offer for sale; sell; or possess an interception device.[109] An interception device is an apparatus or device that the person knows is capable of unlawfully intercepting a communication under section 7(1) of the *Telecommunications (Interception) Act 1979* (Cth), but does not include an apparatus or device designed principally for receiving messages transmitted by radiocommunications.[110]

In addition to section 85ZKB, section 85ZKA of the *Crimes Act 1914* (Cth) makes it an offence to manufacture; advertise, display or offer for sale; sell; or possess an unauthorised call-switching device. Section 85ZK makes it an offence to connect equipment to a telecommunications network, or to use equipment connected to a telecommunications network, to commit a criminal offence. Furthermore, section 85ZG establishes offences in relation to interference with a facility operated by a carrier that hinders the normal operation of a telecommunications carriage service; or the use or operation of an apparatus or device that hinders the normal operation of a carriage service.

2. Does the content have to be encrypted or otherwise protected so as to benefit from protection?

No. Australian laws dealing with the interception of telecommunications do not establish separate rules in relation to encrypted or protected communications.

3. What are the circumstances where interception is authorised or where interception devices are legitimate (eg, when they comply with some technical standards)?

Permitted interceptions under the Telecommunications (Interception) Act 1979 (Cth)

The following interceptions are permitted under the *Telecommunications (Interception) Act 1979* (Cth):

1. interception under a warrant issued in accordance with the *Telecommunications (Interception) Act 1979* (Cth);
2. interception by an officer of the Australian Security Intelligence Organisation (ASIO) in the performance of duties in relation to discovering a "listening device";

[108] *Crimes Act 1914* (Cth) ss 85ZD, 85ZB (definitions of "carrier", "communication" and "communication in the course of telecommunications carriage"). "Carrier" and "carriage service provider" are given complex definitions under the *Telecommunications Act 1997* (Cth).
[109] *Crimes Act 1914* (Cth) s 85ZKB(1).
[110] *Crimes Act 1914* (Cth) s 85ZKB(1A).

3. interception by an employee of a carrier, or other person, in the course of duties relating to the installation, operation or maintenance of a telecommunications system;
4. interception by an employee of a carrier in the course of duties relating to identifying or tracing a person who may have contravened Part VIIB of the *Crimes Act 1914* (Cth);
5. interception by a person lawfully engaged in the installation, connection or maintenance of equipment used, or to be used, for the interception of communications under warrants; and
6. interception by a member of the police force, or an employee of a carrier, pursuant to a request by a member of the police force for the purpose of tracing the location of a caller making an emergency call relating to a likely death or serious injury.[111]

Permitted "interception devices" under section 85ZKB of the Crimes Act 1914 (Cth)

As explained above, section 85ZKB of the *Crimes Act 1914* (Cth) makes it a criminal offence to manufacture; advertise, display or offer for sale; sell; or possess an interception device. An offence is not committed in the following circumstances:

1. the device could not reasonably be regarded as having been designed for the purpose of unlawfully intercepting a communication passing over a telecommunications system under section 7 of the *Telecommunications (Interception) Act 1979* (Cth);
2. the device is in the possession of a person in the course of a person's duties relating to the lawful interception of communications passing over a telecommunications system;
3. the device is manufactured, advertised, displayed, sold, or in the possession of a person, for a purpose related to the lawful interception of a communication;
4. the device is manufactured for a purpose related to interception in the course of a person's duties of lawfully intercepting communications;
5. the device is manufactured, sold, or in possession of a person, for export from Australia;
6. the use of the device is legally permitted under specified legislation, including the *Australian Federal Police Act 1979* (Cth) and the *Australian Security Intelligence Organization Act 1979* (Cth); and
7. the possession of the device is related to a person's duties of investigating or prosecuting offences under the *Telecommunications (Interception) Act 1979* (Cth) or Part VIIB of the *Crimes Act 1914* (Cth).[112]

4. Who may bring a claim? What remedies are available?

Unlawful interceptions under the Telecommunications (Interception) Act 1979 (Cth)

Section 107A of the *Telecommunications (Interception) Act 1979* (Cth) provides for civil actions in relation to unlawful interceptions, or other breaches of section 7(1) of that Act.

A civil action under section 107A may only be commenced by an "aggrieved person".[113] An "aggrieved person" is a person who was either a party to the intercepted communication, or a person on behalf of whom the intercepted communication was made.[114]

In a civil action brought under section 107A, a court may make such orders as it considers appropriate, including a declaration that the interception was unlawful, an order for damages, an injunction and an account of profits.[115] An order for damages may include an award for punitive damages.[116]

---

[111] *Telecommunications (Interception) Act 1979* (Cth) ss 7(2), 30.
[112] *Crimes Act 1914* (Cth) s 85ZKB(2); Crimes Regulations 1990 (Cth), reg 7.
[113] *Telecommunications (Interception) Act 1979* (Cth) s 107A(3).
[114] *Telecommunications (Interception) Act 1979* (Cth) s 107A(2).
[115] *Telecommunications (Interception) Act 1979* (Cth) ss 107A(2), (7).
[116] *Telecommunications (Interception) Act 1979* (Cth) s 107A(10).

In addition to the civil remedies, contravention of sections 7 (unlawful interception) or 63 (unlawful dealing with intercepted information) of the *Telecommunications (Interception) Act 1979* (Cth) are criminal offences.[117] If a court convicts a person of an offence in relation to unlawful interception, or unlawful dealing in intercepted information, it may, upon an application by an "aggrieved person", grant any remedy it considers appropriate.[118]

Unlawful activities in relation to "interception devices" under section 85ZKB of the Crimes Act 1914 (Cth)

A contravention of section 85ZKB of the *Crimes Act 1914* (Cth) is a criminal offence, with a maximum penalty of imprisonment for 5 years.[119]

b. Telecommunications Law might also impose mandatory technical standards to be applied to telecommunications reception devices. This could lead to prohibiting devices enabling the unauthorised reception of communications. What about the telecommunications law in your country?

Part 21 of the *Telecommunications Act 1997* (Cth) deals with the technical regulation of telecommunications "customer equipment". Technical standards may be either mandatory or voluntary. The Australian Communications Authority (ACA) is responsible for setting mandatory standards. The ACA may only make a technical standard in relation to customer equipment if it is necessary or convenient to protect the integrity of a telecommunications network, protect personal health and safety, facilitate access to emergency services or enabling interoperability of customer equipment for the purpose of the supply of a standard telephone service.[120] Self-declaration based on an appropriate level of testing, a labelling regime, sample auditing, and prescribed penalties forms the basis of the compliance regime. There are currently no express provisions in ACA technical standards dealing with the unauthorised reception or interception of communications.

The ACA also has the responsibility for determining technical standards for devices that use the radio-frequency spectrum under the *Radiocommunications Act 1992* (Cth).[121] The ACA may only make such radiocommunications standards as are necessary or convenient to contain interference, or protect personal health or safety.[122] No current ACA standards specifically prohibit devices that enable the interception or reception of radiocommunications. Nevertheless, under s 190 of the *Radiocommunications Act 1992* (Cth), the ACA may declare certain devices that are likely to interfere with radiocommunications, or adversely affect health or safety, to be "prohibited devices". The ACA has declared "mobile telephone jammers" to be "prohibited devices".[123] The operation, supply or possession of a "prohibited device" is a criminal offence.[124]

5. Computer crime

a. In your country, is there legislation related to computer crime? Can circumvention of technological measures and/or unauthorised access to computer systems, networks or data be prosecuted under such statutes? What is the rationale of criminalizing such offences?

---

[117] *Telecommunications (Interception) Act 1979* (Cth) s 107.
[118] *Telecommunications (Interception) Act 1979* (Cth) ss 107A(5), (6).
[119] *Crimes Act 1914* (Cth) s 85ZKB(1).
[120] *Telecommunications Act 1997* (Cth) s 376.
[121] *Radiocommunications Act 1992* (Cth) s 162.
[122] *Radiocommunications Act 1992* (Cth) s 162(3).
[123] Australian Communications Authority, *Declaration under section 190 of the Radiocommunications Act 1992,* 4 March 1999.
[124] *Radiocommunications Act 1992* (Cth) s 189.

In Australia, there is Commonwealth, State and Territory legislation relating to computer crime. There are considerable differences between the various Commonwealth, State and Territory laws. Nevertheless, the respective criminal laws all include provisions that, in some way, prohibit unauthorised access to data stored in a computer, or to a computer system. The relevant offences are explained at paragraph 1a(i) above. As explained, the recently released *Model Criminal Code Report* included significant recommendations for changing and harmonising Australian computer crime laws.

A number of rationales have been given for criminalising unauthorised access. In the late 1980s, Commonwealth, State and Territory legislatures adopted the view that unauthorised access to computers or computer systems represented "anti-social behaviour" and should be criminalised as a deterrent. For example, a 1988 Commonwealth discussion paper on *Computer Crime* concluded that unauthorised access should be criminalised, largely because it might be a prelude to more serious activities, such as fraud, theft or corruption of data.[125] The *Second Reading Speech* to the Commonwealth computer crimes legislation maintained that unauthorised access should be prohibited because information stored in computers is more vulnerable than paper records.[126] In Victoria, the computer crimes legislation originally did not criminalise unauthorised access as such. The legislation was amended, however, during passage to include an offence for "computer trespass". The *Second Reading Speech* stated that unauthorised access should be prohibited so as to discourage "antisocial behaviour and to maintain the confidence of the community in the integrity and privacy of computerised storage of data".[127] The *Model Criminal Code Report* suggested that the existing Australian offences relating to unauthorised access displayed "a certain confusion about the objectives sought to be achieved".[128] The report concluded that the primary objective of criminal laws relating to unauthorised access is to ensure the integrity of computer systems and networks.[129] The report recommended that a proposed offence in relation to unauthorised access be limited to data held in a computer that is protected by a computerised access control system. The main reason given for this conclusion is that the criminal law does not establish liability for the mere unauthorised use of property belonging to another.

b. What is the definition of the offence? Is the way of getting unauthorised access defined: eg providing a false password, decrypting, cracking the technical protection, etc?

The following Commonwealth, State and Territory offences apply to unauthorised access:

Commonwealth

- Unauthorised access to data stored in a Commonwealth computer or data stored on behalf of the Commonwealth: *Crimes Act 1914* (Cth) s 76B.
- Unauthorised access to data stored in a computer by means of a Commonwealth facility or a facility operated by a telecommunications carrier: *Crimes Act 1914* (Cth) s 76D.

New South Wales

- Obtaining access to a program or data stored in a computer without authority or lawful excuse: *Crimes Act 1900* (NSW) s 309.

---

[125] Commonwealth Attorney-General's Department, *Computer Crime,* Discussion Paper No 12 (AGPS, Canberra, 1988).
[126] Hon. Lionel Bowen, Attorney-General, Crimes Legislation Amendment Bill 1989, *Second Reading Speech,* Commonwealth of Australia, *Parliamentary Debates,* House of Representatives, 11 May 1989, p 2543.
[127] Hon. Andrew McCutcheon, Attorney-General, Crimes (Computers) Bill 1988, *Second Reading Speech,* Victoria, *Parliamentary Debates,* Legislative Assembly, 13 April 1988, p 1331.
[128] *Model Criminal Code Report,* p 189.
[129] *Ibid.* p 187.

Queensland

- Using a "restricted computer" without the consent of the computer's "controller": *Criminal Code Act 1899* (Qld) s 408D.

South Australia

- Operating a "restricted-access" computer system without proper authorisation: *Summary Offences Act 1953* (SA) s 44.

Tasmania

- Gaining access to a computer or computer system without lawful excuse: Criminal Code (Tas) s 257D.

Victoria

- Gaining access to, or entering, a computer system without lawful authority: *Summary Offences Act 1966* (Vic) s 9A.

Western Australia

- Operating a "restricted-access" computer system without proper authorisation: Criminal Code (WA) s 440A.
- Gaining access to information stored in a "restricted-access" system without proper authorisation: Criminal Code (WA) s 440A.

Australian Capital Territory

- Obtaining access to data stored in a computer without lawful authority or excuse: *Crimes Act 1900* (ACT) s 135J

The provisions establishing criminal offences are dealt with in more detail at paragraph 1a(i) above.

None of the above criminal provisions specifically defines the means of obtaining unlawful access. Nevertheless, in Queensland, South Australia and Western Australia the relevant offences prohibit the use of "restricted-access" computer systems or a "restricted computer". It would appear that, in these jurisdictions, the prohibitions are aimed mainly at circumvention of "restricted-access" technologies, for example, the circumvention of password protection.

c. Can the manufacture or distribution of devices enabling the carrying out of these offences be prosecuted as well (such devices are sometimes called "hacker tools")? If not, could the seller or manufacturer of circumvention devices be prosecuted as an accomplice? What are the penalties for the offence?

Commonwealth, State and Territory computer crime laws do not include offences relating to the manufacture or distribution of circumvention devices. As explained at paragraph 3c above, the manufacture and distribution of "broadcast decoding devices" is prohibited under Part VAA of the *Copyright Act 1968* (Cth). Moreover, as explained at paragraph 4a above, section 85ZKB of the *Crimes Act 1914* (Cth) prohibits manufacturing, or otherwise commercially dealing with, "interception devices".

Under Australian law, it is possible that a seller or manufacturer of a circumvention device may be prosecuted for a criminal offence relating to unlawful access as an accessory before the fact. To establish liability as an accessory, it must be proved that the seller or manufacturer intended to aid, abet, counsel or procure the commission of the offence, the intention being based on knowledge of the "essential matters"

constituting the offence.[130] Provided the defendant has the requisite intention, there is clear authority that supplying tools for the commission of an offence may render a person liable as an accessory.[131] If there is an intention to commit an offence, and an agreement to do so, it is also possible that a seller or manufacturer may be liable for criminal conspiracy.

The penalties for Commonwealth, State and Territory offences relating to unauthorised access include imprisonment and fines.

d. Is knowledge or malicious intent required to constitute the violation?

Liability for unauthorised access under Commonwealth, State and Territory criminal laws requires proof of an intention to commit the unlawful act.[132] "Malice" is not an element of the offence.

e. Has computer crime legislation already been applied by your country's courts to the unauthorised access to protected information or transmissions, or to the circumvention of technological protection measures?

Commonwealth, State and Territory computer crime legislation has been applied to unauthorised access.[133] Most cases in which a prosecution has been brought have involved either activities in addition to mere unauthorised access, or unauthorised access by employees.

f. In the absence of specific provisions on computer crime, could unauthorised access and/or the circumvention of technological measures be considered to violate other penal laws (eg offences such as theft, fraud, breaking and entering, forgery, etc)? Are there some examples in the case law?

Commonwealth, State and Territory computer crime laws were enacted because existing criminal laws were considered inadequate. Thus, unauthorised access does not amount to theft, as information stored on a computer is not "property" and therefore cannot be the subject matter of a prosecution for theft or larceny.[134] As explained at paragraph 1c above, in certain circumstances, unauthorised access, accompanied by additional elements, may constitute the Commonwealth offence of imposing a false representation with a view to obtaining money,[135] or State or Territory offences for forgery[136] or obtaining property by deception.[137] If the unauthorised access is associated with the destruction or alteration of data, it may give rise to an Stare or Territory offence relating to damage to property.[138]

---

[130] *R v Giorgianni* (1985) 156 CLR 473.
[131] *R v Bainbridge* [1960] 1 QB 120.
[132] In the absence of specific statutory language, there is a legal presumption that "intent" is an element of all criminal offences: *R v He Kaw Teh* (1985) 15 A Crim R 203.
[133] See, for example, *Snell v Pryce* (Unreported, Supreme Court of Northern Territory, 1989); *Rook v Maynard* (1993) 2 Tas R 97; *Rook v Maynard [No 2]* (1994) 123 ALR 677; *Director of Public Prosecutions v Murdoch* [1993] 1 VR 406.
[134] See, for example, *Oxford v Moss* (1978) 68 Cr App R 183; *R v Stewart* (1988) 41 CCC (3d) 481.
[135] *Crimes Act 1914* (Cth) s 29B.
[136] *Crimes Act 1900* (NSW) s 300; *Crimes Act 1958* (Vic) s 83A; *Crimes Act 1900* (ACT) s 135C.
[137] *Crimes Act 1900* (NSW) s 178BA; *Crimes Act 1958* (Vic) s 81.
[138] See, for example, *Crimes Act 1900* (NSW) s 195; *Criminal Code Act 1899* (Qld) s 469; *Criminal Law Consolidation Act 1935* (SA) s 85A; *Crimes Act 1958* (Vic) s 197; *Cox v Riley* (1986) 83 Cr App R 54; *Samuel v Stubbs* [1972] 2 SASR 200; *R v Zischke* [1983] Qd R 240.

6. Unfair competition law or unfair commercial practices

a. In your country, in the absence of specific prohibitions on circumvention or unauthorised access, has the distribution of circumvention devices or descramblers been prohibited through the application of unfair competition law? Under what circumstances?

In Australia, there is no general action for "unfair competition".[139] Consequently, the distribution of circumvention devices or descramblers cannot be prohibited under this head of law in Australia.

b. What are the advantages, disadvantages and boundaries of the recourse to unfair competition law as far as circumvention activities or devices are concerned? Do you consider this protection as sufficient and effective?

See answer to question 6a, immediately above.

7. Protection of technological measures as such

Technical means of protection might be in themselves protected by a proprietary right, eg by a copyright (for instance if the technological measure consists of software), patent or trade secrets. In such a case, circumventing the software or the technical system or developing circumvention devices could effect an unauthorised reproduction of the software (namely reverse engineering) or a disclosure of the trade secret.

a. In your country, what legal regime of exclusive or related rights might apply to the technological measure? Under what conditions? Do you know any case law in that field?

In Australia, technological measures for protecting material might be protected by copyright law, patent law, *sui generis* legislation protecting semi-conductor chips or the equitable doctrine of breach of confidence.

Copyright

A technological protection measure that consists of computer software may be protected as a "computer program" under the *Copyright Act 1968* (Cth). A "computer program" is protected as a "literary work" under Australian copyright law. Under section 10(1) of the *Copyright Act 1968* (Cth), a "computer program" is defined to mean:

> … a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

Provided software falls within this definition, and satisfies the other legal requirements for the subsistence of copyright, including "originality", the measure will be protected under Australian copyright law.

The decision of the Australian High Court in *Autodesk Inc v Dyason*[140] illustrates how existing principles of Australian copyright law may apply to a technological protection measure. That case concerned copyright protection in a technological protection measure, known as a "dongle". The "dongle" (known as the "AutoCAD lock") was a device without which a computer program (known as "AutoCAD") could not operate. The "dongle" operated by transmitting responses to challenges received from the AutoCAD program. A part of the AutoCAd program (known as "Widget C") compared the responses with the correct responses contained in a "look-up table". If the correct response was not received, the AutoCAD

[139] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479; *Moorgate Tobacco v Philip Morris* (1984) 56 ALR 193.
[140] (1992) 173 CLR 331. See also *Autodesk Inc v Dyason (No 2)* (1993) 176 CLR 300.

program would not operate. The defendant produced a circumvention device (known as the "Auto Key lock") by reverse engineering the "dongle". The High Court held that the circumvention device infringed copyright in the Widget C program because, by reproducing the "look-up table", it reproduced a "substantial part" of the Widget C program. The High Court held that the "look-up table" was a substantial part because it was "essential" or "critical" to the operation of the Widget C program. Subsequently, however, in *Data Access Corporation v Powerflex Services Pty Ltd,*[141] the High Court rejected this approach to determining whether something was a "substantial part" of a computer program. In that case, the High Court held that, in order for something to be part of a computer program it must intend to express "an algorithmic or logical relationship between the function desired to be performed and the physical capabilities" of the computer.[142] Moreover, in determining whether something is a "substantial part" of a program, it is the "originality" of the part that must be looked at, and not whether it is essential to the operation of a program. On the other hand, the *Data Access* decision makes it clear that a string of data, such as a "look-up table", might be protected as a "compilation" under Australian copyright law. Depending upon the precise circumstances, it remains possible for a technological protection measure to be protected as a "computer program" or as a "compilation" under the *Copyright Act 1968* (Cth).

Patent

A technological protection measure may be protected under the *Patents Act 1990* (Cth). Whereas copyright protects the form of expression of systems or methods, patent law protects the function of a computer program or device.[143] To qualify for patent protection, the technological measure must be a "manner of manufacture" within section 18 of the *Patents Act 1990* (Cth). Computer software will constitute a "manner of manufacture" if the program involves the production of "an end result which is an artificially created state of affairs of utility in the field of economic endeavour".[144] Australian courts have adopted a relatively liberal approach to patent protection of computer software. Provided that the legislative requirements for patentability (including novelty, inventiveness and utility) are satisfied, a technological protection measure consisting of software is likely to be patentable.

Integrated circuit protection

A technological protection measure embodied in an integrated circuit (or "chip") may be protected under the *Circuit Layouts Act 1989* (Cth). That legislation establishes a *sui generis* regime for "circuit layouts". A "circuit layout" is defined to mean:

> … a representation, fixed in any material form, of the three-dimensional location of the active and passive elements and interconnections making up an integrated circuit.[145]

The legislation gives the "maker" of a circuit layout exclusive rights to copy the layout, to make a "chip" in accordance with the layout and to commercially exploit the layout.[146]

Breach of confidence

A technological measure may also be protected under the equitable doctrine of breach of confidence. As explained at paragraph 1a(ii) above, an equitable action for breach of confidence will be established if: information is confidential; the information is communicated in circumstances importing an obligation of confidence; and there has been an unauthorised use of the information to the detriment of the person

---

[141] (1999) 45 IPR 353.
[142] (1999) 45 IPR 353 at 374.
[143] *Data Access Corporation v Powerflex Services Pty Ltd* (1999) 45 IPR 353 at 360.
[144] *CCOM Pty Ltd v Jiejing Pty Ltd* (1994) 28 IPR 481 at 514. See also *NRDC v Commissioner of Patents* (1959) 102 CLR 252; *IBM Corporation v Commissioner of Patents* (1991) 22 IPR 417.
[145] *Circuit Layouts Act 1989* (Cth) s 5 (definition of "circuit layout").
[146] *Circuit Layouts Act 1989* (Cth) s 17.

communicating it.[147] Moreover, where information has been obtained surreptitiously, there would appear to be a breach of confidence, even where the information has not been communicated in confidence.

b. What exceptions related to these legal regimes could be applied to legitimate the circumvention act or device?

Under legal regimes that may apply to protect technological measures, reverse engineering may be permitted in specific circumstances.

Copyright

The *Copyright Act 1968* (Cth) permits the reproduction of computer programs for the following purposes:

- the normal use of a program;[148]
- studying the ideas behind the program and the way in which it functions;[149]
- in order to make back-up copies of the program;[150]
- in order to make interoperable programs or products;[151]
- to correct errors that prevent the program from operating;[152]
- testing the security of the program, or of a computer system or network of which the program is a part;[153] and
- investigating, or correcting, a security flaw in, or the vulnerability to unauthorised access of, program, or of a computer system or network of which the program is a part.[154]

A technological measure that is protected by copyright may therefore be copied provided that the reproduction is for one of the above permitted purposes. If the reproduction is used, or dealt with, for a purpose that is not permitted, then the exception will not apply.[155] Circumventing a protection measure that consists of computer software may therefore escape copyright infringement if it involves the reproduction of the program for one if the above permitted purposes. The most likely exceptions to be relied upon are the exceptions relating to security testing.

Integrated circuit protection

Reverse engineering of protected circuit layouts is expressly permitted under section 23 of the *Circuit Layouts Act 1989* (Cth). Section 23 provides that exclusive rights in circuit layouts are not infringed by making copies of layouts for the purpose of evaluating or analysing the layout.

Breach of confidence

Reverse engineering of a technological protection measure does not necessarily give rise to an action for breach of confidence. In *Mars UK Ltd v Teknowledge Ltd,*[156] it was held that mere encryption does not render information confidential. It was also held that mere encryption does not mean that the encrypted information is imparted in circumstances importing an obligation of confidence. Thus, if a person buys a machine that contains encrypted information, and has the skills to decrypt the information, he or she may

[147] *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41; *Moorgate Tobacco Co Ltd v Philip Morris Ltd* (1984) 156 CLR 414.
[148] *Copyright Act 1968* (Cth) s 47B(1).
[149] *Copyright Act 1968* (Cth) s 47B(3).
[150] *Copyright Act 1968* (Cth) s 47C.
[151] *Copyright Act 1968* (Cth) s 47D.
[152] *Copyright Act 1968* (Cth) s 47E.
[153] *Copyright Act 1968* (Cth) s 47F(1)(b)(i).
[154] *Copyright Act 1968* (Cth) s 47F(1)(b)(ii).
[155] *Copyright Act 1968* (Cth) s 47G.
[156] (1999) 46 IPR 248.

do so without giving rise to an action for breach of confidence. The extent to which the reasoning in this decision may be applied to circumstances in which the decrypted information is not embodied in a machine purchased by the defendant is somewhat uncertain.

8. Other protections

a. Can you think of any other means of protecting technological measures against circumvention in your country? In which legal areas and by which mechanisms (eg. privacy law, property right, "trespass", "conversion," …)?

Other means of protecting technological measures under Australian law are quite limited.

Privacy

Until recently, Australian privacy law related only to the protection and management of personal information collected or held by public sector agencies. Thus, in the two States that have enacted privacy legislation, New South Wales and Victoria, protection is limited to information held by the public sector.[157] Nevertheless, the Commonwealth has recently enacted new privacy legislation that will apply to the private sector from the end of 2001.[158] The new legislation establishes National Privacy Principles (NPPs) that will apply to the collection, use, security and disclosure of personal information by most private sector organisations. The NPPs establish base line standards for privacy. It is, nevertheless, intended that organisations will develop their own privacy codes of practice and complaints handling mechanisms. Complaints relating to breaches of the NPPs will be enforced by determinations made by the Privacy Commissioner following investigations, and supported by court orders. Circumvention of a technological protection measure may breach the NPPs if it involves the unlawful collection of personal information, or the unauthorised collection of "sensitive information".

Misleading or deceptive conduct

Section 52 of the *Trade Practices Act 1974* (Cth) prohibits corporations from engaging in misleading or deceptive conduct in trade or commerce. The courts have interpreted misleading or deceptive conduct to mean conduct that leads the person to whom it is directed into error, or is likely to cause an error.[159] Some activities directed at circumventing technological protection measures – such as supplying false passwords or false names - may breach section 52, provided that the relevant activities constitute conduct in "trade or commerce". The courts consider most activities conducted by a business to be conduct in "trade or commerce". [160]

Trespass and conversion

Under Australian law, remote circumvention of technological protection measures cannot give rise to an action for trespass to goods or conversion. This is because information is not a "good".

b. In particular, do you think that, in your country, contract law can offer an effective prohibition against circumvention?

1. For example, a contract obliging each user not to circumvent can be embedded in the technological measure itself when it enables the on-line licensing of or access to transmissions (including content). Would such a contract be enforceable in your country?

---

[157] *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2000* (Vic).
[158] *Privacy Amendment (Private Sector) Act 2000* (Cth).
[159] *Weitman v Katies Ltd* (1977) 29 FLR 336; *Puxu v Parkdale Furniture* (1979) 27 ALR 387.
[160] *Concrete Constructions Pty Ltd v Nelson* (1990) 169 CLR 594.

The enforceability of "click-wrap" or "click-through" agreements is somewhat uncertain under Australian contract law. In order for there to be a legally binding contract there must generally be an offer, acceptance of the offer, valuable consideration passing from the promisee to the promisor and an intention to create legal relations. There is no Australian case law definitively establishing the legal validity of "click-wrap" or "click-through" agreements. In particular, it is unclear whether the conduct of "clicking" to obtain access to online content is sufficient to establish the existence of a binding contract.[161] Australian courts look to the objective intentions of the parties, meaning the interpretation placed upon the actions and words of the parties by a reasonable person, to determine the existence of a binding agreement.[162] The Commonwealth, and some States, have enacted legislation that ensures that transactions are not invalidated merely because they have been effected by means of electronic communications.[163]

2. Or contracts might be negotiated between content providers and the computer or consumer electronic manufacture industries in order to oblige them either to design devices that answer to technological measures or not to develop devices that are able to circumvent them. Are such negotiations in progress in your country?

In Australia, there currently appear to be no negotiations between content providers and the manufacturing industry relating to the design or development of circumvention devices.

9. Limitations, exceptions, fundamental rights, third parties' and public interest

a. Are there any general limiting principles that could apply to the various legal regimes we have addressed in this report (eg. freedom of expression, freedom of information, public interest, consumer protection, abuse of right, etc)?

Australia does not have a Bill of Rights. There is, nevertheless, an implied freedom of political communication, derived from the system of representative democracy established by the Australian Constitution.[164] Users wishing to obtain access to material protected by a technological measure would not be assisted by the limited Australian doctrine of freedom of speech.

The common law "public interest" defence applies to actions for breach of confidence.[165] In Australia, the scope of this defence is unclear.[166] The most that can be said is that, if the circumvention of a technological measure amounts to a breach of confidence, there may be a defence if it can be established that disclosure is in the "public interest". The defence is more likely to apply in relation to the disclosure of government information, in which case the government may bear the onus of establishing that non-disclosure is in the public interest.[167]

---

[161] The fact that a human may not be aware that a user has "clicked" to obtain access is no barrier to there being a binding contract: *Thornton v Shoe Lane Parking* [1072] QB 163.
[162] See, for example, *Taylor v Johnson* (1983) 151 CLR 422.
[163] *Electronic Transactions Act 1999* (Cth); *Electronic Transactions Act 2000* (NSW); *Electronic Transactions Act 2000* (Tas). Other Australian States and Territories intend to introduce analogous legislation.
[164] *Lange v Australian Broadcasting Corporation* (1997) 145 ALR 96.
[165] *Commonwealth of Australia v John Fairfax & Sons Ltd* (1980) 32 ALR 485; *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd* (1987) 10 IPR 153.
[166] See, for example, *Corrs Pavey Whiting & Byrne v Collector of Customs for the State of Victoria* (1987) 10 IPR 53.
[167] *Esso Australia Resources Ltd v Plowman (Minister for Resources)* (1995) 128 ALR 391 at 402-3 per Mason CJ.

b. What are the concerns of computer and consumer electronic industries related to prohibitions of circumvention devices? Have these concerns been taken into account in the legal provisions addressed above?

Sections of the computer and consumer electronics industries expressed concerns in relation to prohibitions on circumvention devices in the policy debate concerning the introduction of provisions in Australian copyright law that prohibit the manufacture and distribution of circumvention devices.[168] In particular, concerns were expressed that prohibitions on the use or manufacture of circumvention devices would inhibit security testing and other legitimate activities of system administrators.[169] A House of Representatives Standing Committee responded to these concerns by recommending that the legislation be amended to include a specific exemption for system administrators.[170] The recommendation was not accepted as the exceptions included in the Bill were considered to satisfactorily deal with industry concerns. The exceptions allow for the decompilation of computer programs for the purposes of interoperability, error correction or security testing.[171]

In general, concerns of the computer and consumer electronics industries do not seem to have been expressly taken into account in the legal regimes addressed in this survey.

10. Potential application of the protections surveyed in Questions 1-9 to copyrighted works

a. In your country, could copyright holders avail themselves of some or all of these extra-copyright legal provisions or mechanisms, either to prevent the act of circumvention of technological measures, or to prohibit trafficking in circumvention devices? If so, which ones?

Owners or licensees of copyright are able to bring an action in relation to the circumvention of technological measures, or trafficking in circumvention devices, if they have legal standing to bring a civil action under an "extra-copyright" legal regime dealt with in this survey. Copyright owners or licensees may be able to bring a civil action under the following regimes:

- *Breach of confidence*

At paragraph 1a(ii) above it was explained that unauthorised access to information stored on a computer may give rise to an equitable action for breach of confidence. The remedies available for a breach of confidence include an injunction, account of profits and damages.

- *Unauthorised commercial use or dealings with "broadcast decoding devices"*

At paragraph 3 above it was explained that a "broadcaster" may bring a civil action in relation to the unauthorised commercial use or commercial dealing with a "broadcast decoding device" under Part VAA of the *Copyright Act 1968* (Cth). The civil remedies available for a breach of Part VAA are an injunction, account of profits and damages. A copyright owner or licensee may bring an action under Part VAA in relation to circumvention if the owner or licensee is a "broadcaster" and there has been a commercial use or dealing with a "broadcast decoding device".

---

[168] *Copyright Act 1968* (Cth) s 116A.
[169] House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on Copyright Amendment (Digital Agenda) Bill 1999* (December 1999) paras [4.40], [4.60]-[4.66], [4.68].
[170] *Ibid,* Recommendation 16, para [4.72].
[171] *Copyright Act 1968* (Cth) ss 116A(7), 47D, 47E, 47F.

- *Unlawful interception of telecommunications*

At paragraph 4 above it was explained that a civil action is available in relation to an unlawful interception of telecommunications service under the *Telecommunications (Interception) Act 1979* (Cth). An action for unlawful interception may be brought by an "aggrieved person", meaning a person who was a party to the intercepted communication, or a person on behalf of whom the intercepted communication was made.[172] The remedies available for an unlawful interception include an injunction, a declaration, damages and an account of profits.

- *Contract*

In the event of a binding contract between a copyright owner or licensee and a person who circumvents a technological measure there may be an action for breach of contract. Uncertainties relating to whether or not "click-wrap" or "click-through" agreements are legally binding contracts are dealt with at paragraph 8b1 above.

In addition to the above extra-copyright legal regimes, the circumvention of a technological measure may be a breach of copyright if it involves the reproduction of a substantial part of a "computer program" or of a "compilation". As explained at paragraph 7a above, in *Autodesk Inc v Dyason*[173] the High Court held that "reverse engineering" a device for circumventing a technological protection measure constituted an infringement of copyright in a computer program.

b. Could the alternative means of protection for technological measures available in your country be added or used simultaneously with copyright-related anti-circumvention provisions?

Division 2A of Part V of the *Copyright Act 1968* (Cth) prohibits certain commercial dealings with copyright circumvention devices and circumvention services, including making, selling, commercially distributing and importing circumvention devices. Civil actions may be brought by the copyright owner or an exclusive licensee in relation to contravention of Division 2A of Part V. There is nothing in Division 2A of Part V of the *Copyright Act 1968* (Cth) to prevent a person from bringing a civil action under any of the "extra-copyright" regimes set out above in addition to an action under the copyright anti-circumvention provisions. For example, in appropriate circumstances, a copyright owner could bring an action for breach of confidence or for breach of contract, in addition to an action under Division 2A of Part V of the *Copyright Act 1968* (Cth).

c. What would be the pros and cons of recourse to extra-copyright protections against circumvention of access to copyrighted works or circumvention of technological protections of rights of the author? Do these protections call for reassessment of the need for copyright-specific protections?

Division 2A of Part V of the *Copyright Act 1968* (Cth) does not prohibit the use of a circumvention device or service. The main advantage of an action under an "extra-copyright" regime – such as an action for breach of confidence, for breach of contract or for unlawful interception – is that it may apply to the act of circumventing a technological measure. Similarly, the laws relating to computer crimes, dealt with at paragraphs 1a(i) and 5 above, may apply to the act of using a circumvention device or service. From the perspective of the owner of copyright, there are two main disadvantages with recourse to "extra-copyright" legal regimes. First, the application of established legal principles to the circumvention of copyright material is somewhat unclear and may involve an extension of existing legal principles. This is particularly the case in relation to non-legislative forms of liability, such as the equitable action for breach of confidence and contract law. For example, the availability of an action for breach of confidence for unauthorised access to a computer is not entirely clear. Moreover, the application of contract law to the

[172] *Telecommunications (Interception) Act 1979* (Cth) s 107A.
[173] (1992) 173 CLR 331.

circumvention of technological measures is an area of great uncertainty, especially in relation to so-called "click-through" agreements. Secondly, the "extra-copyright" regimes may not apply to all circumvention-related activities. This is because legal regimes outside of copyright law are not expressly designed to protect copyright, but have quite different policy objectives. For example, Part VAA of the *Copyright Act 1968* (Cth) appears primarily designed to protect "encoded broadcasts", while the *Telecommunications (Interception) Act 1979* (Cth) is designed to prevent the interception of telecommunications services and not the circumvention of technological protection measures. Moreover, from a policy perspective, the "extra-copyright" regimes may not reflect the balances between the interests of copyright owners and users that Australian copyright law attempts to establish. The uncertainty relating to the application of "extra-copyright" regimes, the gaps in protection resulting from the limited scope of such regimes and the extent to which the regimes are directed at quite different policy objectives suggests that they cannot replace copyright-specific protections. Thus, in Australia, although the "extra-copyright" regimes may sometimes supplement the anti-circumvention provisions of the *Copyright Act 1968* (Cth), the existence of alternative legal remedies would not appear to call into question the need for copyright-specific anti-circumvention laws.

d. If recourse to extra-copyright protections is available, could your country implement the WIPO treaty obligations without copyright-specific anti-circumvention legislation? In your view, would this be a desirable approach? If not, to what discrepancies or failures in the existing law would copyright-related anti-circumvention provisions need to respond?

Article 11 of the *WIPO Copyright Treaty* provides, in relevant part, that:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures.

The language of this provision was adopted as a compromise, after the United States had unsuccessfully supported a stronger provision directed at making unlawful the importation, manufacture or distribution of devices whose primary purpose or effect was to circumvent copyright. Article 11 is much less specific than the draft provision supported by the United States.

It is clear that, in the absence of copyright-specific anti-circumvention legislation, Australian law provides some legal protection for technological measures and some remedies against circumvention of technological measures. To determine whether the extra-copyright regimes are capable of meeting obligations under Article 11 it is necessary to determine whether or not the extra-copyright protection is "adequate" and the remedies "effective". The standards established under Article 11 are vague. Given the uncertainties associated with the application of the extra-copyright legal regimes and the gaps in protection, it is doubtful whether Article 11 could be implemented without copyright-specific legislation. The introduction of Division 2A of Part 5 of the *Copyright Act 1968* (Cth), which establishes a copyright-specific regime in relation to circumvention devices and electronic rights management information, would appear to confirm this view.

The introduction of copyright-specific anti-circumvention legislation is a more desirable means of implementing Article 11 than reliance on existing extra-copyright legal regimes. The extra-copyright regimes consist of a patchwork of specific laws designed for specific policy objectives. There are considerable uncertainties in relation to the application of these regimes to the circumvention of copyright protection technologies. While the regimes may provide some protection, the protection is certainly not comprehensive. Moreover, there are significant discrepancies in the operation of the various extra-copyright laws. For example, there are considerable differences among the various Australian jurisdictions in the criminal laws that apply to unauthorised access to data stored on a computer, or to computer systems. This suggests that there may be a need to introduce greater consistency to Australian extra-copyright anti-circumvention regimes. In any case, a legal regime designed specifically to deter circumvention of copyright protection technologies would appear preferable to reliance upon regimes designed to promote quite different policy objectives.

Any other observations?

This survey of Australian extra-copyright anti-circumvention laws reveals that there a complex patchwork of laws that may apply to the circumvention of technological measures. The operation of most of these regimes involves significant uncertainties. Furthermore, there are considerable inconsistencies relating to the operation of the various legal regimes. For example, the differences between Commonwealth, State and Territory laws that deal with computer crimes are a cause for concern. Moreover, the policy objectives of the various regimes have not always been specified with sufficient precision. For example, it is somewhat unclear whether the regime introduced to protect "encoded broadcasts" under Part VAA of the *Copyright Act 1968* (Cth) is intended primarily to allow broadcasters to control the reception of encrypted broadcasts or to support the rights of owners of copyright in broadcast transmissions. As technological measures for protecting access to information stored on computer systems become more important, and as attempts to circumvent access controls generate more social concern, there may be a need to review the various Australian anti-circumvention regimes. Such a review could assist in more precisely defining the policy objectives of anti-circumvention regimes and introducing greater consistency between the various regimes.

Links to Legislation

Legislation referred to in this report may be obtained at the following URLs.

Commonwealth

Broadcasting Services Act 1992 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/.
Circuit Layouts Act 1989 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/cla1989203/.
Copyright Act 1968 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/.
Crimes Act 1914 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/.
Electronic Transactions Act 1999 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/eta1999256/.
Patents Act 1990 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/pa1990109/.
Privacy Act 1988 (Cth) (incorporating *Privacy Amendment (Private Sector) Act 2000* (Cth)), http://www.privacy.gov.au/publications/privacy88.pdf.
Radiocommunications Act 1992 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/ra1992218/.
Telecommunications Act 1997 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.
Telecommunications (Interception) Act 1979 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/ta1979350/.

New South Wales

Crimes Act 1900 (NSW), http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/.
Electronic Transactions Act 2000 (NSW), http://www.austlii.edu.au/au/legis/nsw/consol_act/eta2000256/.

Queensland

Criminal Code Act 1899 (Qld), http://www.austlii.edu.au/au/legis/qld/consol_act/cca1899115/.

South Australia

Criminal Law Consolidation Act 1935 (SA), http://www.austlii.edu.au/au/legis/sa/consol_act/clca1935262/.
Summary Offences Act 1953 (SA), http://www.austlii.edu.au/au/legis/sa/consol_act/soa1953189/.

Tasmania

Criminal Code (Tas), http://www.austlii.edu.au/au/legis/tas/consol_act/cca1924115/s13.html/.

Victoria

Summary Offences Act 1966 (Vic), http://www.austlii.edu.au/au/legis/vic/consol_act/soa1966189/.

Western Australia

Criminal Code (WA), http://www.austlii.edu.au/au/legis/wa/consol_act/ccaca1913252/sch1.html/.

Australian Capital Territory

Crimes Act 1900 (ACT), http://www.austlii.edu.au/au/legis/act/consol_act/ca190082/.

Northern Territory

Criminal Code Act (NT), http://www.austlii.edu.au/au/legis/nt/consol_act/cca115.html/.