Privacy Protection for Internet E-mail in Australia

Kent Davey, L LB(Hons) B Sc LL M
Australian Government Solicitor
(Part 3 of 3 parts)

This article is based on a thesis submitted in partial fulfilment of the requirements of the degree of Master of Laws of the University of Melbourne. The author would like to thank Associate Professor Mark Sneddon of the University for his comments on earlier drafts of the thesis.

CHAPTER 8—E-MAIL AND THE PROTECTION OF COMMUNICATIONS INFORMATION UNDER TELECOMMUNICATIONS LEGISLATION

Introduction

The Telecommunications Act 1997 (Cth)[1] expressly protects communications by restricting the disclosures and uses which carriers, service providers, telecommunications contractors and their employees may make of communications information. The extension of this restriction to carriers themselves removes a major limitation on the protection previously afforded to communications by the Telecommunications Act 1991 (Cth). In the view of the former Privacy Commissioner interferences with privacy are more likely to be attributable to the actions of carriers than to the actions of their employees.[2] The Telecommunications Act 1997 also affords greater protection for communications by making provision for the development of industry codes and standards.

The Sections of this Chapter cover the following areas relating to the privacy protection afforded to Internet e-mail by the Telecommunications Act 1997. Section A looks at the primary offence under the Act relating to the disclosure and use of communications information. Section B examines the secondary offence under the Act relating to the disclosure advise of such information. Section C comments on the record-keeping requirements imposed on carriers and service providers by the Act. Section D discusses the development of telecommunications industry codes and standards. Section E proposes amendments to the Act to provide adequate protection for communications information.

A. Primary Offence Relating to the Disclosure and Use of Communications Information by Carriers, Service Providers, Telecommunications Contractors and their Employees

It is an offence under the Telecommunications Act 1997 for a carrier, service provider, telecommunications contractor[3] or an employee of such a person to disclose or use any communications information which comes to their knowledge or into their possession in connection with the person's business.[4] Communications information is information that relates to:

(i) the contents of a communication that has been carried by a carrier or service provider;

(ii) the contents of a communication that is being carried by a carrier or service provider (including a communication that has been collected or received but has not been delivered);

(iii) telecommunications services supplied or intended to be supplied to another person by a carrier or service provider; or

(iv) the affairs or personal particulars of another person.[5]

The relevant issues to be considered in determining whether a carrier, service provider, telecommunications contractor or an employee of such a person commits an offence by disclosing or using communications information obtained by snooping on Internet e-mail are:

(1) Whether e-mail is a 'communication'?

(2) What constitutes the 'disclosure' and 'use' of information?

(3) Whether any disclosure and use exceptions apply?

1. Whether E-mail is a 'Communication'?

The Telecommunications Act 1997 broadly defines a 'communication' to include any communication whether between persons and/or things and whether in the form of speech music or other sounds, data, text, visual images, signals or any other form or combination of forms.[6] E-mail is a 'communication' as it may consist of text, images, sound and/or animation.

Communications information relating to another person's affairs which is contained in e-mail is protected under the Telecommunications Act 1997. The Act also protects communications information relating to the contents of e-mail which:

(a) has been transmitted by a carrier or service provider and which is stored in the mailbox of the intended recipient or on an intermediate computer;

(b) is being transmitted by a carrier or service provider over the Internet; or

(c) has been received by a carrier or service provider for transmission by it over the

Internet.

2. *What Constitutes the 'Disclosure' and 'Use' of Information?*

The word 'disclosure' is not defined in the Telecommunications Act 1997. The word 'disclose' is defined in the Macquarie Dictionary (2nd ed) to mean 'to make known; reveal'. Information would be 'disclosed' by a person where the person makes known or reveals the information to a third person.

The word 'use' is also not defined in the Telecommunications Act 1997. The word 'use' is defined in the Macquarie Dictionary (2nd ed) to mean 'to avail oneself of; apply to one's own purposes'. A person would use information where the person applies the information to their own purposes. However, information may not be considered to 'used' for the purposes of the Act where it is only viewed on a computer screen.

In relation to an alleged contravention of the Data Protection Act 1984 (UK) the House of Lords held that as the word 'use' was not defined in the Act it must be given its natural and ordinary meaning of '"make use of" or "employ for a purpose"'.[7] The House of Lords expressed the view that the retrieval of information so that it appeared on a computer screen would not of itself be 'using' the information retrieved but would simply be transferring the information into a different form.[8]

If Australian courts follow the approach taken by the House of Lords then it may be necessary for a person to do more than view e-mail on a computer screen for information to have been 'used'. It may prove to be 'extremely difficult if not impossible' to establish that someone has 'used' information for the purpose of committing an offence under the Telecommunications Act 1997.[9] However, the viewing of e-mail on a computer screen may involve gaining unauthorised access to the message. Chapter 9 considers the application of Commonwealth, State and Territory legislation to the situation where a person gains unauthorised access to e-mail stored on a computer.

3. *Whether any Disclosure and Use Exceptions Apply?*

There are numerous exceptions under the Telecommunications Act 1997 which allow carriers, service providers, telecommunications contractors and their employees to disclose and use communications information without committing an offence under the Act. These exceptions include the substance of the exceptions contained in the Telecommunications Act 1991 together with additional exceptions. The exceptions contained in the Telecommunications Act 1991 were based on the IPPs contained in the Privacy Act and provisions contained in repealed telecommunications legislation.[10] As a result of the exceptions being based on the IPPs the privacy protection provided for communications information by the Telecommunications Act 1997 is similarly inadequate.

A carrier, service provider, telecommunications contractor or an employee of such a person may disclose and use communications information in the performance of their duties without committing an offence.[11] The scope of the duties of a person may be very wide being limited only by the activities which a carrier or service provider chooses to undertake. The duties which would justify the disclosure or use of communications information by such a person should be clearly identified.

Communications information may be disclosed and used by a carrier, service provider, telecommunications contractor or an employee of such a person where the disclosure or use is:

(a) required or authorised by or under law;[12] or

(b) reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.[13]

These exceptions should be made more specific by requiring that communications information may only be disclosed and used for a lawful purpose in the public interest. This requirement would involve the weighing of privacy interests against public interests which has been discussed in Chapter 3. The laws enforcement of which would justify the disclosure and use of information should be clearly identified. Additionally, the expression 'protection of the public revenue' should be clarified. Chapter 6 considered these exceptions in relation to the IPPs contained in the Privacy Act.

The disclosure and use of communications information by a carrier, service provider, telecommunications contractor or an employee of such a person is permitted where:

(a) the information relates to another person's affairs and the individual concerned is reasonably likely to have been aware that such information is usually disclosed or used in the circumstances or has consented to the disclosure or use in the circumstances;[14] or

(b) the information relates to the contents or substance of a communication made by another person and it might reasonably be expected that the sender and recipient would have consented to the disclosure or use.[15]

These exceptions permit unreasonable intrusions upon the privacy of users and should be removed. If the disclosure or use is not covered by any other exception the consent of the individual concerned should be obtained by the carrier, service provider or telecommunications contractor concerned.

Communications information may be disclosed and used by a carrier, service provider, telecommunications contractor or an employee of such a person where the disclosure or use is made for the purpose of another carrier or service provider carrying on its business and the information relates to a customer of one of the

carriers or service providers. The disclosure or use of the information must be for a purpose which is connected with the supply of a telecommunications service to the customer by the other carrier or service provider.[16] This exception provides greater privacy protection for communications information being narrower than the corresponding exception contain in the Telecommunications Act 1991.

Other exceptions allow carriers, service providers, telecommunications contractors and their employees to disclose and use communications information where:

(a) the disclosure is made by a witness summoned to give evidence;[17]

(b) the disclosure is made to the Australian Security Intelligence Organization ('ASIO') in connection with the performance of its functions;[18]

(c) the disclosure is made to the Australian Communications Authority ('ACA') or Australian Competition and Consumer Commission ('ACCC') to assist it to carry out its functions or powers;[19]

(d) the disclosure is made to the Telecommunications Industry Ombudsman ('TIO') to assist in the consideration of a complaint;[20]

(e) the information relates to information contained in an integrated public number database and the disclosure or use is made for purposes connected with the provision of directory assistance services, publication or maintenance of a directory of public numbers or dealing with a call to an emergency service number;[21]

(f) the disclosure is made to a member of an emergency service for the purpose of dealing with a call to an emergency service number;[22]

(g) the information relates to another person's affairs and the disclosure or use is reasonably necessary to prevent a serious or imminent threat to the life or health of a person;[23] or

(h) the disclosure or use is made for the purpose of the preservation of human life at sea.[24]

The disclosure of communications information under these exceptions may be justified on the basis that public interests in disclosure are likely to outweigh privacy interests in confidentiality to a substantial degree in the circumstances.

B. Secondary Offence Relating to the Disclosure and Use of Communications Information by Carriers, Service Providers, Telecommunications Contractors and their Employees

A significant policy change is the creation of a secondary offence under the Telecommunications Act 1997 which prohibits a person to whom communications information has been disclosed for a particular purpose under a specified exception disclosing or using it for any other purpose.[25] The exceptions specified relate to the performance of a person's duties,[26] authorisation by or under law,[27] law enforcement and protection of the public revenue,[28] assisting the ACA ACCC or TIO,[29] a threat to a person's life or health,[30] preservation of human life at sea[31] and the business needs of other carriers or service providers.[32]

In order to protect the privacy of users the secondary offence should also apply when communications information is disclosed under the exceptions relating to the awareness and consent of the individual concerned and the reasonable expectation of the sender and recipient of a communication. The Explanatory Memorandum to the Telecommunications Bill 1996 gives no indication of the reasons why these exceptions were not also included as specified exceptions. The use or disclosure of communications information for a purpose other than that for which it was disclosed under any of these exceptions may unreasonably intrude upon the privacy of users.

C. Requirement for Carriers and Service Providers to Keep Records of Disclosures of Communications Information

The Telecommunications Act 1997 requires carriers and service providers to keep records of disclosures of communications information which they make under any exception other than specified exceptions. The exceptions specified relate to the performance of a person's duties, assisting ASIO, the integrated public number database, the reasonable expectation of the sender and recipient of a communication and the business needs of other carriers or service providers.[33]

The requirement to keep records of disclosures should also apply to the exceptions relating to ASIO and the integrated public number database in order to protect the privacy of users. Again the Explanatory Memorandum to the Telecommunications Bill 1996 gives no indication of the reasons why the requirement to keep records does not also apply to these exceptions. If record-keeping requirements are not imposed on carriers and service providers in relation to their disclosures under these exceptions their accountability for such disclosures will be unnecessarily limited.

The Telecommunications Act 1997 imposes an obligation on carriers and service providers to report annually to the ACA on the disclosures to which the record-keeping requirements apply.[34] The Privacy Commissioner is given the function of monitoring compliance by carriers and service providers with these record-keeping requirements.[35]

D. Development of Telecommunications Industry Codes and Standards

The Federal Government intends that telecommunications should be regulated in a manner that promotes the greatest practicable use of industry self-regulation.[36] Part 6 of the Telecommunications Act 1997 provides the framework for increased industry self-regulation by the development of industry codes and

standards.[37] Privacy matters that industry codes and standards may deal with include:

(i) the protection of personal information; and

(ii) the monitoring or recording of communications.[38]

An industry code or standard should be developed for the purpose of protecting Internet e-mail from snooping by carriers, service providers and telecommunications contractors. Such a code or standard should provide guidance as to when the collection of communications information by snooping on the Internet and the use, disclosure and retention of such information will be necessary for a lawful purpose in the public interest.

The Federal Government intends that bodies and associations which represent sections of the telecommunications industry should develop industry codes applicable to activities of participants in the respective sections of the industry.[39] An industry code developed by carriers and service providers may be registered with the ACA if a draft has been published inviting submissions from carriers, service providers and the public, the ACCC does not object to the code, the TIO has been consulted and, where the code deals with privacy matters, the Privacy Commissioner has been consulted.[40] Compliance with industry codes will be voluntary in the first instance.[41] However, the ACA may direct a person contravening an industry code to comply with it.[42] A person must comply with such a direction by the ACA.[43]

The ACA may determine an industry standard if it is satisfied that the industry standard is necessary or convenient and that an industry code has not been developed or is deficient.[44] The ACA will be required to consult with the Privacy Commissioner before determining an industry standard which deals with privacy matters.[45] Compliance with an industry standard will be compulsory.[46]

E. Amendments to Telecommunications Legislation Required to Provide Adequate Protection for Communications Information

Several amendments are required to be made to the Telecommunications Act 1997 to provide adequate protection for communications information. The Act should be amended to include provisions relating to the collection of only the minimum amount of communications information, the protection of such information with reasonable security safeguards and the destruction of such information after it is no longer required.

The Telecommunications Act 1997 should only permit the collection by carriers, service providers and telecommunications contractors of the minimum amount of communications information relating to another person's affairs necessary for a lawful purpose in the public interest. This requirement would involve weighing privacy interests against public interests which has been examined in Chapter 3. The requirement to collect only the minimum amount of such information would accord with the Collection Limitation Principle contained in the Australian Privacy Charter ('APC').[47] It would be an unreasonable intrusion upon the personal affairs of the user concerned if more information relating to their personal affairs than necessary was collected by a carrier, service provider or telecommunications contractor as such information would be unnecessarily stored.

Carriers, service providers and telecommunications contractors should be required under the Telecommunications Act 1997 to protect communications information relating to another person's affairs which is in their possession or control with reasonable security safeguards against loss, unauthorised access, use, modification or disclosure and other misuse. Such a requirement would be consistent with IPP 4 contained in the Privacy Act and the security principles contained in the OECD Data Protection Guidelines[48] and APC. Chapter 6 has examined the application of IPP 4. The security principles contained in the OECD Data Protection Guidelines and APC have been considered in Chapter 4.

There also should be a requirement under the Telecommunications Act 1997 for carriers, service providers and telecommunications contractors to destroy communications information relating to another person's affairs which is in their possession or control after it is no longer required for a lawful purpose in the public interest. This requirement would also involve the weighing of privacy interests against public interests which has been considered in Chapter 3. The requirement to destroy such information after it is no longer required for a lawful purpose would accord with the Retention Limitation Principle contained in the APC. The privacy of users will be unreasonably intruded upon where carriers, service providers and telecommunications contractors retain such information for longer than required for a lawful purpose in the public interest as it may be unnecessarily used or disclosed.

Conclusion

The Telecommunications Act 1997 has wider application and provides greater protection for communications information than the Telecommunications Act 1991. The provisions for the protection of communications information contained in the Telecommunications Act 1997 apply to carriers, service providers, telecommunications contractors and their employees. However, the Telecommunications Act 1997 re-enacts the substance of the exceptions contained in the Telecommunications Act 1991 concerning the disclosure and use of communications information which were based on the IPPs contained in the Privacy Act. As a result the privacy protection provided for communications information by the Telecommunications Act 1997 is inadequate. The amendments outlined above should be made to the Telecommunications Act 1997 to

provide adequate protection for communications information.

The secondary offence under the Telecommunications Act 1997 which prohibits a person to whom communications information has been disclosed for a particular purpose under a specified exception from using or disclosing the information for any other purpose provides increased privacy protection for such information. The accountability of carriers and service providers for their disclosures of communications information under specified exceptions is greater as they are required to keep records of such disclosures and report to the ACA with the Privacy Commissioner having the function of monitoring compliance. However, the Act should also have imposed requirements on carriers, service providers and telecommunications contractors to collect only the minimum amount of communications information relating to another person's affairs necessary for a lawful purpose in the public interest, to protect such information in their possession or control with reasonable security safeguards and to destroy such information after it is no longer required for a lawful purpose in the public interest. As these requirements have not been addressed in the Act itself then hopefully they will be implemented in industry codes and standards developed under the Act.

Improved privacy protection for communications information will result from the development under the Telecommunications Act 1997 of industry codes and standards which deal with privacy matters. An industry code or standard should be developed to protect e-mail from carriers, service providers and telecommunications contractors snooping on the Internet. Such a code or standard for e-mail should provide guidance as to when the collection of communications information by snooping on the Internet and the use, disclosure and retention of such information will be necessary for a lawful purpose in the public interest. Importantly, the Privacy Commissioner must be consulted where an industry code or standard deals with privacy matters. The development of industry codes and standards dealing with privacy matters will promote greater awareness of privacy issues within the telecommunications industry in general with the effect that greater recognition will be given to privacy interests by carriers, service providers and telecommunications contractors.

1 The Act is part of a package of legislation which repealed the Telecommunications Act 1991 (Cth) and replaced it with a new regulatory framework which commenced on 1 July 1997. The package of legislation includes the Telecommunications (Transitional Provisions and Consequential Amendments) Act 1997 (Cth), Trade Practices Amendment (Telecommunications) Act 1997 (Cth) and Australian Communications Authority Act 1997 (Cth).

2 'Dial "P" For Privacy', *Choice*, June 1994, 16.

3 A 'telecommunications contractor' is a person who performs services for or on behalf of a carrier or service provider other than as an employee: Telecommunications Act 1997 s 274.

4 Ibid s 276.

5 Ibid.

6 Ibid s 7.

7 *R v Browne* [1996] 1 All ER 545, 548.

8 Ibid.

9 Sheila McGregor and Lesley Sutton, 'Improper "use" of Data' (1995) 14(3) *Communications Law Bulletin* 14, 15.

10 Australian Telecommunications Corporation Act 1989 (Cth) s 97; AUSSAT Act 1984 (Cth) s 16; Overseas Telecommunications Act 1946 (Cth) s 33A.

11 Telecommunications Act 1997 s 279.

12 Ibid s 280.

13 Ibid s 282.

14 Ibid s 289.

15 Ibid s 290.

16 Ibid s 291.

17 Ibid s 281.

18 Ibid s 283.

19 Ibid s 284(1)-(2).

20 Ibid s 284(3).

21 Ibid s 285

22 Ibid s 286.

23 Ibid s 287.

24 Ibid s 288.

25 Ibid Part 13, Division 4.

26 Ibid s 296.

27 Ibid s 297.

28 Ibid s 298.

29 Ibid s 299.

30 Ibid s 300.

31 Ibid s 301.

32 Ibid s 302.

33 Ibid s 306.

34 Ibid s 308.

35 Ibid s 309.

36 Telecommunications Act 1997 s 4.

37 Telecommunications Bill 1996 Second Reading Speech 4-5.

38 Telecommunications Act 1997 s 113(3)(f).

39 Ibid s 112.

40 Ibid s 117.

41 Telecommunications Bill 1996 Explanatory Memorandum Volume 1, 68-9.

42 Telecommunications Act 1997 s 121(1).

43 Ibid s 121(2).

44 Ibid ss 123-5.

45 Ibid s 134.

46 Ibid s 128.

47 Australian Privacy Charter Council, *Australian Privacy Charter*, December 1994.

48 Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980) ('OECD Data Protection Guidelines').

CHAPTER 9—GAINING UNAUTHORISED ACCESS TO E-MAIL STORED ON A COMPUTER

Introduction

Commonwealth, State and Territory legislation provides indirect privacy protection for Internet e-mail by prohibiting persons gaining unauthorised access to data stored on computers in certain circumstances. However, a significant difficulty with the legislation is that it lacks uniformity with the effect that snooping on e-mail may or may not constitute an offence depending on the applicable legislation of the relevant jurisdiction. Another difficulty with the application of the legislation is that many of the terms such as 'access', 'computer', 'lawful authority' and 'lawful excuse' are not defined with the result that the exact scope of the offences remains uncertain.

The Sections of this Chapter examine the circumstances in which Commonwealth, State and Territory legislation prohibits persons gaining access to Internet e-mail stored on a computer. Section A considers legislation relating to gaining access to a computer without lawful authority or excuse. Section B discusses legislation concerning gaining access to data stored on a computer without authority or lawful excuse. Section C looks at

legislation relating to the operation of a restricted-access computer without authority. Section D discusses legislation concerning unlawfully abstracting confidential information from a computer. Section E proposes the creation of an offence to prevent persons snooping on the Internet gaining unauthorised access to encrypted e-mail.

A. Gaining Access to a Computer Without Lawful Authority or Lawful Excuse

A person commits an offence under the Summary Offences Act 1966 (Vic) ('Victorian Act') and Criminal Code (Tas) ('Tasmanian Code') where he or she gains access to a computer without lawful authority and lawful excuse respectively.[1] The Criminal Code broadly defines 'gain access' to include 'communicate with a computer'.[2]

In *DPP v Murdoch*[3] the Victorian Supreme Court discussed the circumstances in which an employee enters a computer without authority. The defendant was a computer operator employed by a bank in its information systems department. Without authority he entered a command to take the bank's automatic teller machine 'off host' for the purpose of overdrawing his Visa credit card account with the bank. In considering whether the defendant had committed an offence under the Victorian Act Hayne J stated:

'In the case of a hacker it will be clear that he has no authority to enter the system. In the case of an employee the question will be whether that employee had authority to effect the entry with which he stands charged. If he has a general and unlimited permission to enter the system then no offence is proved. If however there are limits upon the permission given to him to enter that system, it will be necessary to ask was the entry within the scope of that permission? If it was, then no offence was committed; if it was not, then he has entered the system without lawful authority to do so.'[4]

A hacker snooping on the Internet who gains unauthorised access to a computer would commit an offence under the Victorian Act and Tasmanian Code. However, system administrators who have unlimited access privileges to a computer on which e-mail is stored would not commit an offence by gaining access to the computer to snoop on messages. This is a significant restriction on the protection afforded to e-mail by all Commonwealth, State and Territory legislation which prohibits persons gaining unauthorised access to data stored on computers.

B. Gaining Access to Data Stored on a Computer Without Authority or Lawful Excuse

An offence is committed under the Crimes Act 1914 (Cth) ('Commonwealth Act') and Crimes Act 1900 (ACT) ('ACT Act') where a person intentionally gains access to data stored on a computer without authority and lawful excuse respectively.[5] Similarly, a person commits an offence under the Crimes Act 1900 (NSW) ('NSW Act') where he or she intentionally gains access to data stored on a computer without authority or lawful excuse.[6] The Acts define 'data' to include information.[7] E-mail would constitute 'data' as it may consist of text, images, sound and/or animation.

An offence would be committed under the ACT and NSW Acts where a hacker snooping on the Internet gains unauthorised access to e-mail stored on a computer. However, an additional requirement for an offence to be committed under the Commonwealth Act is that the data must be stored on a Commonwealth computer or on a computer on behalf of the Commonwealth or that access must be by means of a facility operated or provided by the Commonwealth, a carrier or service provider.[8] Where a hacker gains remote access through the Internet to e-mail stored on a computer without authority an offence would be committed under the Act as Internet access involves the use of a facility operated by a carrier or service provider.

It is a more serious offence under the Commonwealth and NSW Acts where a person gains access to data stored on a computer which he or she knows relates to another person's affairs or gains access to data stored on a computer and continues to examine it after he or she knows the data relates to another person's affairs.[9] A more serious offence is committed under these Acts where a hacker gains unauthorised access to e-mail stored on a computer which he or she knows contains information relating to another person's affairs.

C. Operating a Restricted-Access Computer Without Proper Authorisation

A person commits an offence under the Summary Offences Act 1953 (SA) ('SA Act'), Criminal Code (WA) (' WA Code') and Criminal Code (Qld) ('Qld Code') where he or she operates a restricted-access computer system without proper authorisation.[10] A restricted-access computer system is a system which requires the use of a particular code of electronic impulses to obtain access where the person entitled to use the system has withheld knowledge of the code from all other persons or restricted knowledge of the code to particular persons.[11] Many host computers and intermediate computers are restricted-access computers in that a password is required to access the computer. A hacker snooping on Internet e-mail who operates a restricted access computer without authority would commit an offence under the SA Act and WA and Qld Codes.

D. Unlawful Abstraction of Confidential Information from a Computer

It is an offence under the Criminal Code (NT) ('NT Code') for a person to unlawfully abstract confidential information from a computer with intent to cause loss to a person, to disclose the information to a person who is not lawfully entitled to receive it or to use the information to obtain a benefit or advantage for himself or herself.[12] An offence would be committed where a hacker snoops on e-mail by abstracting confidential information from a computer without authority intending to cause loss,

disclose the contents of the message or use the message for his or her own benefit.

The offence under the NT Code would not apply where a person abstracts information which is not confidential from a computer. It has been suggested that an offence would not be committed where a person only views information on a computer screen without taking the information away in any abstracted form.[13]

E. Offence of Decrypting Encrypted E-mail Unless Authorised by Law or With the Consent of the Sender

An offence which prohibits persons decrypting encrypted e-mail would overcome the restrictive application of the Commonwealth, State and Territory legislation which prohibits persons gaining unauthorised access to data stored on computers. It is an offence under the Australian Postal Corporation Act 1989 (Cth) ('Australia Post Act') for a person to open an article while it is in the course of post under the control of Australia Post if the opening is not permitted by an exception.[14]

As Internet e-mail is gradually replacing postal mail an offence should be created which similarly prohibits system administrators, hackers and anyone else decrypting encrypted e-mail to access the contents of messages unless specifically authorised by law or with the consent of the sender of the message. Where the sender of e-mail has actively taken steps to protect the privacy of e-mail by encrypting the message it is appropriate to provide a higher standard of privacy protection by prohibiting decryption unless authorised by law as opposed to prohibiting decryption unless necessary for a lawful purpose in the public interest.

An exception applies under the Australia Post Act where an article cannot be delivered to the intended recipient because it is not properly addressed and cannot be returned to the sender because it does not properly show the sender's address.[15] In these circumstances an authorised examiner may open the article and examine its contents for the purpose of obtaining sufficient information to deliver the article to the intended recipient or return the article to the sender.[16] However, if encrypted e-mail bounces and is delivered to a system administrator an exception would not be required to permit him or her to decrypt the message for the purpose of delivering the message to the intended recipient or returning it to the sender. The system administrator may ascertain the e-mail addresses of the sender and recipient of a message which bounces from the unencrypted header of the message without having to decrypt the contents of the message.

Exceptions to the offence of decrypting encrypted e-mail would need to be created where privacy interests are outweighed by public interests to a substantial degree. The public interests may relate to law enforcement, national security, public revenue, public safety and rights and freedoms of others. The balancing of privacy interests and public interests has been considered in Chapter 3.

An offence which prohibits persons decrypting encrypted e-mail may be enacted by the Federal Government in reliance on the posts and telegraphs power contained in section 51(v) of the Commonwealth Constitution. An offence enacted in reliance on the posts and telegraphs power may apply uniformly throughout Australia. As the Internet reaches all Australian States and Territories uniformity throughout Australia is particularly desirable.

Conclusion

Commonwealth, State and Territory legislation which prohibits persons gaining unauthorised access to data stored on computers affords only restricted and uncertain privacy protection for Internet e-mail. The major restriction on the protection provided for e-mail by the legislation is that it does not prohibit system administrators with unlimited access privileges to a computer snooping on messages stored on the computer.

The restrictive application of the Commonwealth, State and Territory legislation relating to unauthorised computer access may be overcome by creating an offence which prohibits persons decrypting encrypted e-mail to access the contents of the message unless specifically authorised by law or with the consent of the sender of the message. It is appropriate to provide a higher standard of privacy protection for e-mail where the sender of the message has actively taken steps to protect the privacy of its contents. However, exceptions to the offence would need to be created where privacy interests are outweighed by public interests to a substantial degree.

1 Victorian Act s 9A; Tasmanian Code s 257D.
2 Tasmanian Code s 257A.
3 [1993] 1 VR 406.
4 Ibid 410.
5 Commonwealth Act ss 76B, 76D; ACT Act s 135J.
6 NSW Act s 309.
7 Commonwealth Act s 76A(1), NSW Act s 308(a), ACT Act s 135H(1).
8 Commonwealth Act ss 76A(1), 76B(1), 76D(1).
9 Ibid ss 76B(2)(b)(v), 76B(3), 76D(2)(b)(v), 76D(3); NSW Act ss 309(3)(e), 309(4).
10 SA Act s 44(1); WA Code s 440A(2); Qld Code s 408D(1).
11 SA Act s 44(3), WA Code s 440A(1); Qld Code s 408D(5).
12 NT Code s 222.
13 Greg Tucker, *Information Privacy Law in Australia* (1992) 145.
14 Australia Post Act ss 90M, 90N.
15 Ibid s 90Q(1).
16 Ibid s 90Q(2).

CHAPTER 10—E-MAIL AND THE EUROPEAN UNION'S DATA PROTECTION AND TELECOMMUNICATIONS PRIVACY DIRECTIVES

Introduction

It has been suggested that the Federal Government's decision to abandon its proposed co-regulatory approach for extending privacy protection to the private sector means that Australia is heading for a confrontation with the European Union with the risk of being isolated from international data flows.[1] The European Union's Data Protection Directive may restrict the flow of personal data from Member

States of the European Union to Australia if Australia's privacy laws are not reformed to provide an adequate level of protection for personal data.[2] The Directive expressly recognises that its provisions are intended to apply to e-mail containing personal data transmitted by means of an e-mail service.[3]

The Data Protection Directive requires Member States[4] to pass laws which provide protection for the privacy rights of individuals with respect to the processing of personal data and which restrict the transfer of personal data to third countries which do not ensure an adequate level of protection for such data. Member States must bring into force laws necessary to comply with the Directive by 25 October 1998.[5]

The European Union's Telecommunications Privacy Directive is intended to complement the Data Protection Directive by providing protection for the fundamental rights and freedoms of subscribers to publicly available telecommunications services.[6] In particular the Directive is intended to provide protection for the privacy rights of subscribers in relation to the processing of their personal data.[7] As with the Data Protection Directive Member States must bring into force laws necessary to comply with the Telecommunications Privacy Directive by 24 October 1998 with one exception. The exception concerns laws necessary to comply with Article 5 of the Directive relating to the confidentiality of communications which must be brought into force by Member States by 24 October 2000.[8]

The Sections of this Chapter examine the privacy protection provided for Internet e-mail by the Data Protection and Telecommunications Privacy Directives and consider the implications for the sending of e-mail to Australia. Section A considers the privacy protection required to be provided for e-mail under the Directives to give some indication of what may constitute an adequate level of protection for the purposes of the Data Protection Directive. Section B discusses whether the transfer of personal data to Australia would be restricted under the Data Protection Directive on the basis that Australia does not ensure an adequate level of protection for such data.

A. Application of the Data Protection and Telecommunications Privacy Directives to E-mail

The Data Protection and Telecommunications Privacy Directives apply to the processing of personal data. The Articles contained in the Data Protection Directive which are relevant to snooping on Internet e-mail relate to fair and lawful data processing, legitimate data processing and implementation of security measures. The Telecommunications Privacy Directive contains Articles relating to confidentiality of communications and implementation of security measures which similarly are relevant to snooping on Internet e-mail.

1. *Processing of Personal Data Under the Data Protection and Telecommunications Privacy Directives*

The Data Protection Directive applies to the processing of personal data wholly or partly by automatic means.[9] In contrast the Telecommunications Privacy Directive applies to the processing of personal data in connection with the provision of publicly available telecommunications services over public telecommunications networks in the European Community.[10]

'Personal data' is defined in the Data Protection Directive to mean 'any information relating to an identifiable natural person ("data subject")'.[11] The definition of 'personal data' is more restrictive than the definition of 'personal information' contained in the Privacy Act 1988 (Cth) ('Privacy Act') as it does not include an opinion about an individual. E-mail will contain 'personal data' where it contains information about a person whose identity is apparent or can be ascertained. E-mail may contain 'personal data' about a person other than the sender of the message. The circumstances in which e-mail contains 'personal information' have been discussed in Chapter 6.

The Data Protection Directive defines 'processing' to mean 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.[12] This extremely broad definition of 'processing' includes almost any dealing with e-mail whatsoever. Snooping on e-mail would constitute 'processing' personal data for the purposes of the Directive.

A 'telecommunications service' is defined in the Telecommunications Privacy Directive to mean a service 'whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks'.[13] 'Public telecommunications network' is defined in the Directive to mean 'transmission systems ... which permit the conveyance of signals between defined termination points by wire, by radio, by optical or other electromagnetic means, which are used in whole or in part, for the provision of publicly available telecommunications services'.[14] An Internet e-mail service supplied to the public would be a 'telecommunications service' as its provision involves the transmission of e-mail over the Internet by the conveyance of signals in the form of packets of data between the sender's and recipient's computers.

2. *Fair and Lawful Processing of Personal Data under the Data Protection Directive*

Article 6 of the Data Protection Directive requires Member States to ensure that personal data is processed lawfully and fairly.[15] Member States may need to prohibit the collection of personal data by snooping on e-mail on the basis that it is an unfair means of collecting such data. Under the Directive the controller is required

to ensure that personal data is processed lawfully and fairly.[16] However, the controller in respect of e-mail will normally be considered to be the person from whom the message originates rather than the person providing the Internet e-mail service.[17]

Where the controller in respect of e-mail is deemed to be the sender of the message this will severely limit the extent of any privacy protection required to be provided for e-mail under Article 6. The sender of e-mail may only be able to prevent someone snooping on it by encrypting its contents. It has been recognised that the Data Protection Directive is not designed to apply to the Internet as the aspects of transmission and network providers are not adequately addressed.[18]

3. *Legitimate Processing of Personal Data Under the Data Protection Directive*

Member States are obliged by Article 7 of the Data Protection Directive to ensure that personal data is only processed if the data subject has consented or processing is necessary:

(a) for the performance of a contract with the data subject;

(b) for the controller to comply with a legal obligation,

(c) to protect the data subject's vital interests;

(d) for the performance of a task in the public interest; or

(e) for legitimate interests pursued by the controller except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Member States may enact laws which permit carriers and service providers to snoop on e-mail for purposes such as network operation and network maintenance which may be considered to be tasks carried out in the public interest.

4. *Confidentiality of Communications Under the Telecommunications Privacy Directive*

In accordance with Article 5 of the Telecommunications Privacy Directive Member States must ensure the confidentiality of communications made by means of public telecommunications networks and publicly available telecommunications services. In particular Member States are required to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications by persons without the consent of users except where authorised by law.[19]

Member States are required by Article 5 to enact laws which prohibit persons snooping on Internet e-mail without the consent of users except where authorised by law. To a certain degree Article 5 overcomes the restrictive application of the Data Protection Directive resulting from the sender of e-mail normally being considered to be the controller.

5. *Implementation of Security Measures under the Data Protection Directive and Telecommunications Privacy Directives.*

Pursuant to Article 17 of the Data Protection Directive Member States must ensure that the controller implements appropriate technical and organisational measures to protect personal data against accidental loss and against unauthorised alteration, disclosure or access.[20] Where the controller in respect of e-mail is deemed to be the sender of the message this will significantly restrict the extent of privacy protection required to be afforded to e-mail under Article 17. Encryption is the main security measure that the sender of e-mail may use to prevent someone snooping on the Internet obtaining unauthorised access to the contents of the message.

In contrast Article 4 of the Telecommunications Privacy Directive requires the provider of a publicly available telecommunications service to implement appropriate technical and organisational measures to safeguard the security of the service.[21] If there is a particular risk of a breach of network security then the provider must inform subscribers of the risk and advise them of any possible remedies.[22] Significantly, Article 4 requires security safeguards to be implemented by providers of telecommunications services unlike Article 17 of the Data Protection Directive. Providers of Internet e-mail services may implement security measures such as password protection, secure networks and encryption where appropriate. The appropriateness of providing security safeguards has been considered in Chapter 3.

B. Prohibition Under the Data Protection Directive on the Transfer of Personal Data to Third Countries Which do not Ensure an Adequate Level of Protection

Article 25 of the Data Protection Directive requires Member States to prohibit the transfer of personal data to a third country where the data is undergoing processing or intended for processing after transfer unless the third country ensures an adequate level of protection. However, Article 26 of the Directive allows Member States to permit the transfer of personal data to third countries which do not ensure an adequate level of protection in certain circumstances.

1. *Assessing the Adequacy of the Level of Protection Afforded to Personal Data by Third Countries*

Pursuant to Article 25 the adequacy of the level of protection afforded to personal data by a third country is to be assessed in light of all the circumstances surrounding the transfer operation. In assessing the adequacy of the level of protection afforded by a third country:

'[P]articular consideration is to be given to the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and country of final destination, the rules of law, both

general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.'[23]

The laws enacted by Member States in order to comply with the Telecommunications Privacy Directive would be taken into account in assessing the adequacy of the level of protection afforded to personal data by a third country.

The fact that third countries are only required to ensure an adequate level of protection implies that personal data may be transferred to third countries which provide a lower standard of protection than that required to be provided by Member States under the Data Protection Directive. However, Member States may require third countries to provide a level of protection for personal data which is equivalent to the level of protection provided by their national provisions which they adopt pursuant to the Directive on the basis that transfers of personal data to third countries are to be without prejudice to their national provisions.[24]

It has been suggested that the Data Protection Directive may indirectly have the effect of prohibiting the transfer of personal data to Australia from countries other than Member States. Countries which pass laws to comply with the Directive may need to prohibit the transfer of personal data to Australia if Australia's laws do not ensure an adequate level of protection.[25]

The former Privacy Commissioner believed that for Australia to be assessed as a country with an adequate level of protection generally its privacy laws would need to be extended to cover the private sector and the States and Territories would need to pass similar legislation.[26] However, the Federal Attorney-General's Department has advised that the Federal Government could rely upon the external affairs power contained in section 51(xxix) of the Commonwealth Constitution to enact comprehensive privacy legislation for Australia. The legislation would give effect to Australia's international legal obligations under the International Covenant on Civil and Political Rights.[27] Although Australia may not be assessed as a country with an adequate level of protection generally, it may still be assessed with an adequate level in relation to sectors already covered by the Privacy Act.[28]

2. *Exceptions for the Transfer of Personal Data to a Third Country Which Does not Ensure an Adequate Level of Protection*

In accordance with Article 26 Member States may permit the transfer of personal data to a third country which does not ensure an adequate level of protection where:

(a) the data subject consents;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller;

(c) the transfer is necessary for the performance of a contract in the interests of the data subject;

(d) the transfer is necessary or legally required on important public interest grounds; or

(e) the transfer is necessary to protect the vital interests of the data subject.[29]

The sender of e-mail impliedly consents to the transfer to Australia of personal data contained in the message by the act of sending the message. However, Member States may need to prohibit e-mail being sent to Australia which contains personal data relating to a person other than the sender of the message unless the other person consents or the sending of the message is necessary for the performance of a contract or in the public interest.

Conclusion

In its Law and Justice Policy released prior to the last Federal Election the Federal Government stated that the Data Protection Directive 'will have the effect of excluding Australian entities from European community data flows unless our privacy laws are substantially improved by mid-1998.'[30] However, the Government's decision to abandon its co-regulatory approach for the extension of privacy protection to the private sector is inconsistent with its apparent intention to reform Australia's privacy laws.

The Telecommunications Privacy Directive requires Member States to enact laws which prohibit persons snooping on e-mail without the consent of users except where authorised by law. Member States may require Australia to provide a level of protection for personal data which is equivalent to the level of protection provided by the national provisions which they adopt pursuant to both the Data Protection and Telecommunications Privacy Directives. Unless Australia's privacy laws are reformed to prohibit persons snooping on e-mail without the consent of users except where authorised by law the Data Protection Directive may restrict the sending of e-mail to Australia from Member States and other countries which pass laws to comply with the Directive.

1 Chris Merritt, 'Australia now offside with Europe on privacy laws', *Financial Review*, 27 March 1997; Hans van Leeuwen, 'EU test planned on privacy issue', *Financial Review*, 13 March 1998.

2 Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, No L 281 *Official Journal of the European Communities*, 23 November 1995, 31 ('Data Protection Directive').

3 Ibid Recital 47.

4 The fifteen Member States of the European Union are: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden and the United Kingdom.

5 Data Protection Directive Article 32(1)

6 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, No L 24 *Official Journal of the European Communities*, 30 January 1998, 1 ('Telecommunications Privacy Directive'). The Directive is based on Common Position (EC) No 57/96 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks, No C 315 *Official Journal of the European Communities*, 24 October 1996, 30.

7 Ibid Articles 1, 2.

8 Ibid Article 15(1).

9 Data Protection Directive Article 3(1)

10 Telecommunications Privacy Directive Article 3(1).

11 Data Protection Directive Article 2(a).

12 Ibid Article 2(b).

13 Telecommunications Privacy Directive Article 2.

14 Ibid Article 2.

15 Data Protection Directive Article 6(1)(a).

16 Ibid Article 6(2).

17 Ibid Recital 47.

18 Jan Berkvens, 'Will the Data Protection Directive prevent a global information infrastructure?' (1995) 11(2) *Computer Law & Practice* 38, 42.

19 Telecommunications Privacy Directive Article 5(1).

20 Data Protection Directive Article 17(1).

21 Telecommunications Privacy Directive Article 4(1).

22 Ibid Article 4(2).

23 Data Protection Directive Article 25(2).

24 Ibid Article 25(1).

25 Chris Merritt, above n 1.

26 Kevin O'Connor, 'The Tightening of European Privacy Laws—What are the Implications for Australia?', *IIR Conference Paper*, 12 August 1996, 5.

27 Federal House of Representatives, Standing Committee on Legal and Constitutional Affairs, *In Confidence*, June 1995, 171-2; Department of Foreign Affairs, 'International Covenant on Civil and Political Rights' (1980) No 23 *Australian Treaty Series*.

28 Kevin O'Connor, above n 25. See also Graham Greenleaf, 'European Privacy Directive and data exports' (1995) 2(6) *Privacy Law & Policy Reporter* 105, 106.

29 Data Protection Directive Article 26(1).

30 Federal Government, *Law and Justice Policy*, February 1996, 28.

CONCLUSION

As the most participatory form of mass speech developed the Internet offers tremendous benefits to society by enabling millions of people around the world to exchange information and ideas. However, as the largest global network of computers on the planet the Internet also poses an unprecedented threat to the privacy of personal information. The information privacy of users of the Internet is rapidly diminishing as technological developments continually make it even easier for personal information to be improperly and surreptitiously collected. Users have less and less ability to determine for themselves to what extent information about them is communicated to others when using the Internet.

Internet e-mail is gradually replacing postal mail. However, many users send e-mail over the Internet containing their most intimate thoughts and feelings without properly considering the privacy risks associated with communicating by e-mail. They do not fully appreciate that most existing laws in Australia were not enacted with the Internet in mind. Consequently these existing laws provide only piecemeal privacy protection for Internet e-mail which does not prohibit system administrators, carriers, service providers and hackers snooping on messages in many instances.

Privacy has been widely recognised as a fundamental human right which individuals are reasonably entitled to expect. Respect for the autonomy of individuals requires that protection be provided for communications which are intended by individuals to be private. In Australia an expectation of e-mail privacy must be recognised as reasonable and given effect to particularly where Australians are becoming increasingly concerned about their privacy.

It is widely acknowledged that privacy interests must be balanced against competing public interests. An intrusion upon the privacy of an individual will not be unreasonable in circumstances where privacy interests are outweighed by competing public interests to a substantial degree. The Federal Government,[1] the Australian Broadcasting Authority[2] and the United States Court of Appeals in *American Civil Liberties Union v Reno*[3] have given precedence to privacy interests in protecting communications when these interests have conflicted with competing public interests.

Australia's international legal obligations under the International Covenant on Civil and Political Rights ('ICCPR')[4] require that it enacts laws which prohibit Internet e-mail being subjected to arbitrary interference by persons snooping on the Internet unless the interference is necessary in the public interest. The OECD Security Guidelines[5] impose a moral obligation on Australia to ensure that the use, provision and security of Internet e-mail services involves respect for the privacy rights and interests of users. Additionally, the Australian Privacy Charter ('APC')[6] similarly recognises that Australians are entitled to expect that they may conduct their affairs free from surveillance and that the privacy of their communications will be respected.

The collection of personal information by carriers and service providers snooping on the Internet and the use and disclosure of such information would not breach the OECD Data Protection Guidelines[7] or APC where the individual concerned consents or where authorised by law. Carriers and service providers should only be permitted to collect personal information by snooping on the Internet and to use, disclose and retain such information where necessary for a lawful purpose in the public interest in circumstances where the individual concerned does not expressly or impliedly consent and where not specifically authorised by law. In accordance with the APC carriers and service providers should only be allowed to collect the minimum amount of personal information necessary for a lawful purpose. In order to comply with the OECD Data Protection and Security Guidelines and APC carriers and service providers should be required to protect e-mail and Internet e-mail services with reasonable security safeguards such as password protection, secure networks and encryption where appropriate.

In this thesis I have argued that the piecemeal privacy protection provided for Internet e-mail in Australia is inadequate to prevent system administrators, carriers, service providers and hackers snooping on e-mail. The privacy protection afforded to Internet e-mail by the breach of confidence doctrine is inadequate and uncertain. The doctrine does not protect privacy per se. Information surreptitiously or improperly obtained may only be protected by an action for breach of confidence where an actual or

threatened use of the information is unconscionable.

The requirement under the Telecommunications Industry Ombudsman scheme for participating carriers and service providers to comply with the Information Privacy Principles ('IPPs') contained in the Privacy Act 1988 (Cth) provides only weak privacy protection for Internet e-mail. The scheme does not expressly require participating carriers and service providers to comply with the IPPs but merely permits a user to make a complaint if he or she believes that a carrier or service provider is not complying with the IPPs. The IPPs themselves set only an inadequate standard of confidentiality.

Advances in technology and the introduction of competition into the telecommunications industry mean that there are now significant gaps in the protection provided to communications under the Interception Act 1979 (Cth) ('Interception Act'). The Act may not restrict the communications and uses which carriers and service providers may make of e-mail stored in the mailboxes of users or on intermediate computers. Carriers and service providers may rely on the participant monitoring exception under the Act to intercept e-mail sent to or from an Internet e-mail service which they supply or received at such a service.

The protection provided for communications information under the Telecommunications Act 1997 (Cth) ('Telecommunications Act') is inadequate. The exceptions contained in the Act relating to the disclosure and use of communications information by carriers, service providers, telecommunications contractors and their employees set an inadequate standard of confidentiality being based on the IPPs. The exception relating to the performance of a person's duties is very wide being limited only by the activities which a carrier or service provider chooses to undertake.

Commonwealth, State and Territory legislation relating to the gaining of unauthorised access to a computer provides only restricted privacy protection for Internet e-mail. The legislation does not prohibit system administrators with unlimited access privileges to a computer from snooping on messages stored on the computer.

It may be argued that encryption should be relied upon by users of Internet e-mail services to protect the privacy of their messages. However, encryption does not absolutely ensure the privacy of the contents of an encrypted message and would not assist in the development of a culture of respect for privacy. Encryption should not be seen as a substitute for providing legal protection for the privacy of e-mail.

In this thesis I have also suggested measures for the reform of Australia's laws to ensure that Internet e-mail is provided with appropriate privacy protection. Amendments are required to be made to the Interception Act to address advances in technology and the introduction of competition into the telecommunications industry. The definition of 'interception' should be amended to include the viewing of a communication by any means in its passage over a telecommunications system. Carriers and service providers should not be permitted to rely upon the participant monitoring exception under the Act to unreasonably intrude upon the privacy of users of e-mail by snooping on messages.

The exceptions contained in the Telecommunications Act relating to the disclosure and use of communications information which are indirectly based on the IPPs should be amended and made more specific as should the IPPs themselves. The Act should also be amended to include provisions requiring the collection of only the minimum amount of communications information relating to another person's affairs, protection of such information with reasonable security safeguards and destruction of such information after it is no longer required. An industry code or standard should be developed under the Act which applies to Internet e-mail and provides guidance to carriers, service providers and telecommunications contractors as to when the collection of communications information relating to another person's affairs and the use, disclosure and retention of such information will be necessary for a lawful purpose in the public interest.

An offence should be created which prohibits a person decrypting encrypted e-mail unless specifically authorised by law or with the consent of the sender of the message. It is appropriate to provide a higher standard of privacy protection where the sender of e-mail has actively taken steps to protect the privacy of its contents. Such an offence would apply where a system administrator with unlimited access privileges to a computer decrypts encrypted e-mail which is stored on the computer. However, exceptions to the offence would need to be created where privacy interests are outweighed by public interests to a substantial degree.

I have argued that these suggested measures for the reform of Australia's existing laws are necessary for Australia to comply with its international legal obligations under the ICCPR and moral obligations under the OECD Data Protection and Security Guidelines. The sending of e-mail containing personal data to Australia from Member States of the European Union and other countries which enact laws to comply with the Data Protection Directive[8] may well be restricted unless these suggested measures for the reform of Australia's privacy laws are implemented.

The decision by the Federal Government to abandon its plans to extend privacy protection to the private sector under a co-regulatory approach is particularly disappointing in view of Australia's international legal and moral obligations respectively under the ICCPR and OECD Data Protection and Security Guidelines and the likely implications under the Data Protection Directive for the sending of e-mail to Australia. Internet e-mail deserves the highest protection from

the unprecedented threat posed to the privacy of personal information by system administrators, carriers, service providers and hackers snooping on the Internet.

1 Federal Government, *Australia Online*, February 1996, 17.

2 Australian Broadcasting Authority, *Investigation into the content of on-line services*, 30 June 1996, 30.

3 929 F Supp 824 (1996). The US Supreme Court has affirmed the decision of the US Court of Appeals: *Reno v American Civil Liberties Union* (Unreported, US Supreme Court, Stevens J, 26 June 1997).

4 Department of Foreign Affairs, 'International Covenant on Civil and Political Rights' (1980) No 23 *Australian Treaty Series*.

5 Organisation for Economic Co-operation and Development Guidelines for the Security of Information Systems (1992) ('OECD Security Guidelines').

6 Australian Privacy Charter Council, *Australian Privacy Charter*, December 1994.

7 Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980) ('OECD Data Protection Guidelines').

8 Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, No L 281 *Official Journal of the European Communities*, 23 November 1995, 31.

WA Society for Computers and Law Annual General Meeting—President's Report

Princes Plaza Hotel—31 July 1997

It has been another successful year for WASCAL, thanks to the efforts of the committee who have devoted a substantial amount of their free time on behalf of the Society organising the events held over the 12 months since the last AGM.

Seminars

Once again, the presentation of seminars has again been WASCAL's primary focus and it has hosted another 8 seminars in the last 12 months:

(a) last year's AGM seminar on Web Page tips and traps;

(b) Personal Computers and Lawyers—Two Worlds Colliding, a look at Internet Information and Research Tools and a Dragon Dictate demonstration;

(c) ACARB Joint Seminar—"Our Rights, Your Rights, Left Rights, Out Right?"!!!, the legality of looking at other people's e-mail and files;

(d) the Christmas "DOOM" party;

(e) "Providing Speedy Access to Justice - Automating the Legal Process", a legal expert system for compiling AAT applications;

(f) Microsoft Word vs WordPerfect - a shootout!

(g) involvement with the Supreme Court Library demonstration of the unreported decisions data base; and

(h) tonight's double-header: "Electronic Commerce" and "Admissibility of Electronic Documents".

Future Seminars

There is a joint seminar with the Law Society looking at real life uses of the Internet planned for August. There will be a joint Law Society/WASCAL demonstration of different accounting packages tentatively set down for August.

Following the success of last year's idea to generate a seminar topic list, we have instituted a similar discount deal this year. I am sure that the members will take advantage of the deal!

Finances and Membership

The finances of the Society remain healthy, as you will see from the Treasurer's report. Our membership has also continued to grow over the last twelve months.

Contact with Other Organisations

WASCAL keeps close contact with the Australian Computer Society, the Law Society Computerisation Committee (the active Computerisation Committee members tend to be active in WASCAL too) and ACARB. This will continue through the next financial year.

My Resignation

I have been the President of the Society for a number of years now. Regretfully, the pressures of work have increased markedly in that time and I find that I cannot give the Society the attention that is required of the President. I have therefore resigned my position, but will nominate for the position of Vice-President.