PRIVACY PROTECTION FOR INTERNET E-MAIL IN AUSTRALIA

Kent Davey
Australian Government Solicitor

[AA] *LLB (Hons) B. Sc. 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 the draft of the thesis.*

[A] *Simon Davies, Monitor (1996) 24.*

INTRODUCTION

'Privacy is a little like freedom: the less you have of it the easier it is to recognise.' [A]

The Internet enables millions of people around the world from diverse cultural, social, political and economic backgrounds to exchange information and ideas. One of the most popular ways of exchanging information and ideas over the Internet is by electronic mail or e-mail. Internet e-mail is gradually replacing ordinary postal mail and will eventually be the norm rather than the novelty it is today.[1] As a new medium it is predicted that e-mail will change the way we work and live.[2] It is estimated that about 95 billion e-mail messages were sent over the Internet last year.[3] The widest use of Internet e-mail is for personal messages.[4]

Almost anyone may secretly observe e-mail by snooping on the Internet. E-mail has been described as the 'world of postcards'.[5] Messages travelling over the Internet from computer to computer are open and available in the same way that postcards travel through the ordinary mail system. It is said that the only privacy the sender of e-mail has depends upon the 'honesty, ignorance and indifference' of those operating computers over which the message passes.[6] The sender of e-mail has no control over the route it takes over the Internet to reach the intended recipient. E-mail sent between two people in Australia may be routed through the United States. A copy of an e-mail message is stored by each intermediate computer over which the message passes.[7]

Although almost anyone may snoop on Internet e-mail, the focus of this article is limited to public Internet e-mail services and threats to privacy which are posed by computer system administrators, telecommunications carriers, telecommunications service providers and hackers snooping on e-mail sent using those services. A public Internet e-mail service is a service supplied to the public generally by a carrier or service provider. Snooping on private e-mail services supplied by employers for use by their employees is beyond the scope of this article as it involves issues concerning employee privacy rights which have been discussed elsewhere.[8]

Computer system administrators, telecommunications carriers, telecommunications service providers and hackers have the greatest ability to snoop on e-mail sent over the Internet using public Internet e-mail services. System administrators employed by carriers and service providers which supply public Internet e-mail services may use their unlimited computer access privileges to snoop on e-mail. They may snoop on e-mail on their own behalf or on behalf of the carrier or service provider which employs them. In contrast hackers have the ability to gain unauthorised access to computers over which e-mail passes for the purpose of snooping on messages.

In Australia the common law has failed to recognise a general legal right of privacy. Legal privacy protection afforded to Internet e-mail in Australia is piecemeal and derived from the action for breach of confidence, Privacy Act 1988 (Cth) ('Privacy Act') under the Telecommunications Industry Ombudsman ('TIO') scheme, Telecommunications (Interception) Act 1979 (Cth) ('Interception Act'), Telecommunications Act 1997 (Cth) ('Telecommunications Act') and Commonwealth, State and Territory legislation relating to the gaining of unauthorised access to a computer.

In this article I argue that the piecemeal privacy protection provided for Internet e-mail in Australia by these existing laws is inadequate to prevent computer system administrators, telecommunications carriers, telecommunications service providers and hackers snooping on e-mail sent over the Internet using public Internet e-mail services. I suggest measures for the reform of Australia's laws to ensure that Internet e-mail is provided with appropriate privacy protection. I argue that the reform of Australia's laws is necessary for Australia to comply with its international legal obligations under the International Covenant on Civil and Political Rights[9] and its moral obligations under the OECD Data Protection[10] and Security[11] Guidelines. I also argue that unless Australia' s laws are reformed the European Union's Data Protection Directive[12] may restrict the sending of e-mail to Australia from Member States of the European Union and other countries which enact laws necessary to comply with the Directive.

In light of this overview the Chapters of this article cover the following areas. Chapter 1 describes the development of the Internet into the largest global network of computers on the planet. Chapter 2 deals with the use of e-mail and the potential for snooping on e-mail passing over the Internet. Chapter 3 considers the recognition of privacy as a fundamental human right which has to be balanced

against competing public interests and the recognition given to privacy in Australia and internationally. Chapter 4 discusses the inadequacy of relying on encryption as a substitute for legal protection for the privacy of e-mail. Chapters 5, 6, 7, 8 and 9 respectively examine the privacy protection afforded to e-mail by the breach of confidence doctrine, Privacy Act under the TIO scheme, Interception Act, Telecommunications Act and Commonwealth, State and Territory legislation relating to the gaining of unauthorised access to a computer. Chapter 10 analyses the privacy protection provided for e-mail under the European Union's Data Protection and Telecommunications Privacy[13] Directives and considers the implications for the sending of e-mail to Australia. Recommendations for the reform of Australia's laws to ensure that Internet e-mail is appropriately protected are included at appropriate points within the Chapters. The main recommendations for reform are drawn together and commented upon in the Conclusion.

* *Simon Davies, Monitor (1996) 24.*

[1] *Philip Zimmermann, The Official PGP User's Guide (1995) 6.*

[2] *Jacob Palme, Electronic Mail (1995) 1.*

[3] *Stewart Carter, 'Netscape delivers message to e-mail rivals', The Australian, 4 March 1997.*

[4] *Electronic Mail Study Group, Report, January 1996. Available at http://www.ogit.gov.au/ica/*

[5] *Larry J Hughes, Internet Security Techniques (1995) 27.*

[6] *Bruce Schneier, E-Mail Security (1995) 3.*

[7] *Stephen Withers, Geoff Ebbs and Jeremy Horey, The Australian Internet Book (2nd ed 1995) 162.*

[8] *Jim Nolan, 'Privacy in the workplace - Part 3: some legal issues' (1995) 2(3) Privacy Law & Policy Reporter 48, 50, 58; Sheila McGregor, 'Privacy Aspects of Electronic Messaging' (1993) 7(10) Australian Computer Commentary 153, 156-159. See also Laurie Thomas Lee, 'Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop"' (1994) 28 The John Marshall Law Review 139; Ellen Forman, 'The message is: be very careful!', The Australian, 1 April 1997.*

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

[10] *Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).*

[11] *Organisation for Economic Co-operation and Development Guidelines for the Security of Information Systems (1992).*

[12] *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').*

[13] *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.*

CHAPTER 1 - THE INTERNET

A. *Largest Global Network of Computers on the Planet*

The Internet is the largest global network of computers on the planet. The word 'Internet' is derived from the expression 'Interconnected networks' which refers to a series of connected computer networks. The Internet is frequently described as the 'Information Superhighway'.[1] It is also referred to as 'Cyberspace' because as you travel around the global network of computers it seems as if you are 'travelling through the universe from galaxy to galaxy without regard to time or space.'[2]

Millions of computer networks which span continents, countries, cities, towns, communities and individuals are linked together by the Internet.[3] There is no way to determine exactly how many people are connected to the Internet. However, it is estimated that there are over 45 million people on the planet connected to the Internet.[4] Statistics are soon out of date as the Internet doubles in size approximately every 12 to 15 months.[5]

The Internet only exists and functions because millions of operators of computers and computer networks decided to use a common data transfer standard to exchange information.[6] No particular computer or computer network is essential for the existence or functioning of the Internet.[7] The operators of computers and computer networks themselves make decisions about whether to connect to the Internet and the information and services which they will supply to users.[8]

The Internet is considered to be somewhat anarchic as there is no central body responsible for its regulation and it is almost impossible to regulate technically.[9] No single academic, government, corporate or non-profit entity can itself censor or restrict access to all information and services available on the Internet. This has caused concern among the governments of various countries around the world.[10]

B. *Development of ARPANET in the United States*

The Internet originated in the United States in the late sixties when researchers working for the Advanced Research Projects Agency ('ARPA') of the United States Department of Defence ('US Defence Department') designed the ARPA Network ('ARPANet') to support military research on building networks that could withstand nuclear bomb attacks.[11] ARPANet was designed so that each computer on the network could communicate with any other network computer without having to obtain approval from a central computer. As a result computers on the network could continue to communicate notwithstanding the destruction of one or more network computers by a nuclear bomb attack.[12]

Computers connected to ARPANet communicated by sending and receiving messages in the form of packets of data.[13] Each packet consisted of a string of digital binary digits[14] which represented part of the

message being conveyed and the network address of the computer at the intended destination.[15] ARPANet operated as a packet switched network enabling several computers to communicate over a single telephone line at the same time by interspersing packets of data from the different computers.[16]

The Transmission Control Protocol/ Internet Protocol ('TCP/IP') became the standard for communications between ARPANet computers in 1983.[17] TCP breaks up messages into sequentially numbered packets of data and places the packets inside TCP envelopes. IP addresses the packets by placing each TCP envelope inside an IP envelope containing the network address of the computer at the intended destination. When the packets of data reach their intended destination TCP reassembles the packets into the original message.[18]

ARPANet computers used a network map containing the unique network addresses of all other computers to pass packets of data along the fastest route to their intended destination. No specific network route was specified for the packets. If a network computer did not respond then a computer would record this on the network map and pass the packets of data to another computer.[19] The packets would continue to pass over alternative routes until they reached their intended destination. It was usual for packets of data to pass between several network computers before reaching their destination.[20]

C. *AARNet as the Original Backbone of the Australian Internet*

The Australian Academic and Research Network ('AARNet') originally formed the backbone of the Australian Internet. It was established for academic and research purposes by the Australian Vice-Chancellors Committee ('AVCC') and the Commonwealth Scientific and Industrial Research Organisation ('CSIRO').[21] In 1988 AVCC agreed to provide funding to create AARNet to link together universities, CSIRO Divisions and government departments. AARNet was linked to the Internet in 1989 when an international satellite link was established between Hawaii and Melbourne.[22]

Early in 1994 AARNet adopted an open access policy allowing telecommunications service providers to engage in full commercial resale of Internet services. AVCC subsequently decided to return to operating an academic and research network as a result of the increased commercial pressures associated with managing AARNet. On 1 July 1995 AVCC sold to Telstra AARNet's long distance and international links together with its commercial client base.[23] More recently AVCC has decided to end its relationship with Telstra and move across to Optus the remainder of AARNet which now links together 37 universities and the whole of CSIRO.[24]

Telstra enhanced AARNet's long distance and international links to establish its own commercial Internet access service which provides the principal gateways for access to the Internet in Australia.[25] The gateways link together networks nationally and form the backbone of the Australian Internet. Each gateway consists of an intermediate computer known as a router.[26] The major online telecommunications service providers Compuserve Pacific, Telstra On-Australia[27] and Apple eWorld currently operate high profile proprietary computer networks in Australia which are linked to the Internet.[28]

D. *Use of the Internet in Australia*

At present Australia is the fifth largest user of the Internet. It is estimated that there are now more than 2.6 million Australian users of the Internet.[29] Australia has more computers connected to the Internet per person than any other country in the world except the United States.[30] It is also reported that Australia has one of the highest growth rates of Internet users in the world.[31]

Telstra which is the largest telecommunications carrier in Australia currently supplies an Internet access service to the public generally which allows users to access services available on the Internet.[32] Internet access services are also supplied by a large number of telecommunications service providers.[33] Telstra and major service providers generally offer their customers dedicated telecommunications network connections to the Internet. Other service providers tend to provide their customers with dial access through the telecommunications network.[34]

There are more than 5000 services currently available to users of the Internet.[35] The most popular Internet services are the World Wide Web which displays pages containing text images sound and animation, File Transfer Protocol which enables the transfer of files between computers, Newsgroups which cover various areas of interest to which individuals may post messages, Telnet which enables a computer to connect to another computer and operate it remotely, Gopher which retrieves archived information and Internet Relay Chat which allows users to type messages to other users in real time.[36] However, by far the most popular service available on the Internet is e-mail.[37]

[1] *Stephen Withers, Geoff Ebbs and Jeremy Horey, The Australian Internet Book (2nd ed 1995) 7-8.*

[2] *Berny Goodheart and Frank Crawford, Oz Internet (1996) 1.*

[3] *Ibid.*

[4] *'Beginners' Guide to Cyberspace' (1997) 3(2) Internet Australasia 81, 82.*

[5] *See Network Wizards, Internet Domain Survey. Available at http://www.nw.com*

[6] *American Civil Liberties Union v Reno 929 F Supp 824 (1996) (US Court of Appeals).*

[7] *Simon Davies, Monitor (1996) 35.*

[8] *Mark Neely, Australian Beginner's Guide to the Internet (2nd ed 1996) 11.*

[9] *Davies, above n 7.*

[10] *Neely, above n 8.*

[11] *Neely, above n 8, 10; Ed Krol and Paula Ferguson, The Whole Internet (1996) 14.*

[12] *Neely, above n 8, 10; Withers Ebbs and Horey, above n 1, 11-2.*

[13] *Davies, above n 7, 34.*

[14] *Zero's and one's.*

[15] *'Beginners' Guide to Cyberspace', above n 4, 81.*

[16] *Neely, above n 8, 13, 37.*

[17] *Richard Wiggins, The Internet for Everyone (1995) 7.*
[18] *Krol and Ferguson, above n 11, 31-7.*
[19] *Neely, above n 8, 13.*
[20] *Davies, above n 7, 34.*
[21] *Goodheart and Crawford, above n 2, 46.*
[22] *Krol and Ferguson, above n 11, 18-9.*
[23] *Krol and Ferguson, above n 11, 22.*
[24] *John Davidson, 'Optus lifts AARNet from Telstra', Financial Review, 22 January 1997.*
[25] *Ibid; Australian Telecommunications Authority, Value Added Services - Detailed Report, 17 December 1996, 56.*
[26] *Goodheart and Crawford, above n 2, 32.*
[27] *The service provider was re-branded as a result of the end of the relationship between Telstra and Microsoft: Australian Telecommunications Authority, above n 25.*
[28] *Goodheart and Crawford, above n 2, 35-9.*
[29] *Garry Baker, '1.2 million join Net community', The Age, 14 January 1997.*
[30] *Withers Ebbs and Horey, above n 1, 7-8.*
[31] *Australian Telecommunications Authority, above n 25, 26.*
[32] *Optus plans to supply an Internet access service within the next 6 months.*
[33] *The Australian Telecommunications Authority has identified in excess of 100 service providers in Australia which supply Internet access services: Australian Telecommunications Authority, above n 25, 26.*
[34] *Australian Telecommunications Authority, above n 25, 26.*
[35] *Goodheart and Crawford, above n 2, 5.*
[36] *'Beginners' Guide to Cyberspace', above n 4, 82-3, 86.*
[37] *Goodheart and Crawford, above n 2, 6.*

CHAPTER 2 - INTERNET E- MAIL

A. Use of E-mail for Communicating Over the Internet

Internet e-mail is already used by millions of people around the world and will soon be in use by hundreds of millions of people.[1] E-mail is one of the driving forces behind the rapid growth of the Internet providing businesses with global mail connections.[2] In Australia public Internet e-mail services are supplied by Telstra[3] and service providers[4] which supply Internet access services.[5]

E-mail is one of the most powerful applications available on the Internet as it acts as a key mechanism for communicating quickly and efficiently with clients, colleagues, business associates, friends and family.[6] Users of e-mail are often more relaxed and undisciplined in formulating the contents of their messages than they are with more formal documents such as letters and reports. E-mail messages are described as being 'chatty and personal'.[7] People are likely to reveal more of their intimate thoughts and feelings in e-mail than in writing or even orally.[8] It is said that people have a 'propensity to say stupid things in E-mail'.[9]

E-mail is often used for private communications between two individuals or an individual and a group of persons. The sender of e-mail may address the message to a single person or to a group or persons. In this sense e-mail performs a function analogous to the telephone and postal mail. A recipient of e-mail may read, save, print and/or delete the message. In addition a recipient of e-mail may send it over the Internet as part of another message by replying to the original message or by forwarding the original message to other persons even though these persons were never intended to receive it.

E-mail may also be sent to mailing lists which are lists of e-mail addresses of groups of people who share a common interest.[10] A user can subscribe to a list on a topic of interest to them. A subscriber to a mailing list receives copies of all messages posted to the list by other subscribers and may post messages to the list for forwarding to all subscribers.[11] Some mailing lists are overseen by a moderator who examines messages for their relevance and suitability before the message is forwarded to all subscribers.[12] A mailing list may be open or closed depending on whether acceptance of a user into the list requires the approval of the person responsible for maintaining the list.[13]

B. E-mail Passes Over the Internet in the Form of Packets of Data

E-mail messages may be sent over the Internet consisting of text, images, sound and/or animation. Examples of programs commonly used for sending e-mail include Microsoft Mail, Quickmail and Eudora. These programs enable attachments in the form of files to be sent with messages. Types of files which may be attached to messages include documents, computer programs, spreadsheets, pictures and video and audio files.

The two components of an e-mail message are the body and header of the message. The body contains the message itself. The header contains the e-mail address of the recipient, e-mail address of the sender, subject of the message, time the message was sent and length of the message. As e-mail passes over the Internet the network address of each intermediate computer over which the message passes is added to the header of the message. The route which the message took over the Internet may be determined from the header of the message.[14]

The e-mail address contained in the header of a message must be interpreted by intermediate computers or routers which deliver the message to its intended destination.[15] An example of an e-mail address is:

kent.davey@ag.gov.au

The @ symbol serves as the divider between that part of the address which identifies my mailbox and that part which identifies the location of the host computer which holds my mailbox.[16] Users are provided with a unique e-mail address by carriers and service providers which supply Internet e-mail services.

E-mail messages pass over the Internet in the form of packets of data. The packets may travel over different network routes to reach their intended destination. A copy of the packets of data is stored by each intermediate computer over which they pass.[17] When the message arrives

at its destination it is stored in the recipient's mailbox on a host computer operated by a carrier or service provider. The recipient may view the message by connecting to the host computer and downloading it.[18]

Public Internet e-mail services transmit e-mail over the Internet using the Simple Mail Transport Protocol ('SMTP') standard which is based on the Transmission Control Protocol/ Internet Protocol.[19] E-mail sent over the Internet using SMTP is encoded in plaintext using the American Standard Code for Information Interchange ('ASCII'). However, ASCII is one of the most common computer codes which is readable by virtually all computers.[20]

C. *Snooping on Internet E-mail by System Administrators, Carriers, Service Providers and Hackers*

Almost anyone may eavesdrop on e-mail passing over the Internet.[21] Unlike postal mail, e-mail sent over the Internet is generally not 'sealed' and may be accessed or viewed on any intermediate computer over which the message passes.[22] It has been suggested that a person should not include anything in an e-mail message that he or she is not prepared to have become public knowledge.[23]

Anyone who secretly observes e-mail passing over the Internet commits an attack on the Internet which is commonly known as 'snooping'.[24] The term 'snoop' is used in this article to denote the improper or surreptitious collection of information by accessing, viewing, listening to, recording and/or intercepting e-mail passing over the Internet without the knowledge of the sender of the message. The Internet is described as a 'one-stop shop for snooping'.[25] However, a major difficulty with snooping on a particular e-mail message is the task of finding it in the sea of other messages. This is described as being equivalent to looking for 'a small needle inside an enormous haystack'.[26]

The focus of this article is limited to snooping on e-mail by computer system administrators, telecommunications carriers, telecommunications service providers and hackers. The expression 'system administrator' is used to denote a person who has unlimited access privileges to every part of a computer. A system administrator may snoop on e-mail for himself or herself or on behalf of a carrier or service provider which employs him or her to administer a computer used for the supply of a public Internet e-mail service. Anyone who accesses a computer without authority or lawful excuse is referred to as a 'hacker'. The term 'carrier' is used to denote the holder of a telecommunications licence for the supply of telecommunications services to the public.[27] Anyone who supplies a listed carriage service to the public using a network unit owned by a carrier is referred to as a 'service provider'.[28]

The points at which e-mail may be snooped on by system administrators, carriers, service providers and hackers in its passage over the Internet include where:

(a) a copy of the message is stored in the 'Sent Mail' folder of the sender;

(b) a copy of the message is stored on one of the intermediate computers over which the message passes;[29]

(c) the message is stored in the mailbox of the intended recipient;

(d) a copy of the message is kept by a carrier or service provider for purposes such as message transmission, back-up, billing, network operation and network maintenance; and

(e) the message passes over a computer network or telephone line between two computers.

System administrators, carriers and service providers may snoop on e-mail stored in the mailboxes of users, copies of e-mail stored in 'Sent Mail' folders, copies stored on intermediate computers and copies kept by carriers and service providers. E-mail which bounces and is delivered to a system administrator by an intermediate computer which does not know where to send the message may also be snooped on by the administrator.[30]

Similarly, hackers may snoop on e-mail stored in the mailboxes of users, copies of e-mail stored in 'Sent Mail' folders, copies stored on intermediate computers and copies kept by carriers and service providers. Hackers may use sniffing software to snoop on e-mail. Sniffing software is designed for the purpose of finding network problems. However, it also facilitates snooping by placing the interface of a computer network in promiscuous mode. When in promiscuous mode the network interface intercepts and reports to the sniffing software the contents of all packets of data passing over the network.[31] Additionally, a hacker may use a conventional wiretap on a telephone line between two computers to snoop on e-mail by storing a copy of the message in his or her computer.[32]

[1] *Jacob Palme, Electronic Mail (1995) 1.*

[2] *Stephen Withers, Geoff Ebbs and Jeremy Horey, The Australian Internet Book (2nd ed 1995) 180.*

[3] *Optus plans to supply an Internet e-mail service within the next 6 months.*

[4] *Service providers which supply Internet e-mail services nationally include Access One, APANA, AUSNet Services, BlueSky OPC, Compuserv Pacific, Connect.com.au Pty Ltd, Corinthian Internet Services, Dialix, Hutchinsion Telecommunications (Australia) Ltd, IBM Global Network, MagNet, Magna Data, Microplex, Netspace Online Systems, On Australia, OzEmail, TMX, TPG Internet and Wisenet Internat. P/L: 'ISP Directory' (1997) 3(2) Internet Australasia 87, 87-8.*

[5] *Internet e-mail services are not supplied separately but are bundled together with Internet access services.*

[6] *G Allison Burgess, The Lawyer's Guide to the Internet (1995) 61. See also Anthony J H Morris 'Why Lawyers Need E-Mail' (1996) 34 (11) Law Society Journal 39.*

[7] *John Tyrril, 'Editorial Note' (1995) 42 Australian Construction Law Newsletter 36.*

[8] *Jeremy Horey, 'Free speech has no premium on Net', The Australian, 18 February 1997, 38.*

[9] *Tim Blair, 'Full and Frank Admissions From E-Mail's Dead Zone', Time, 6 November 1995, 75.*

[10] *Mark Neely, Australian Beginner's Guide to the Internet (2nd ed 1996) 93.*

[11] *Shea v Reno 930 F Supp 916 (1996) (US District Court) ('Shea').*
[12] *Neely, above n 10, 40.*
[13] *Shea 930 F Supp 916 (1996).*
[14] *Ed Krol and Paula Ferguson, The Whole Internet (1996) 68.*
[15] *Withers Ebbs and Horey, above n 2, 162.*
[16] *'Beginners' Guide to Cyberspace' (1997) 3(2) Internet Australasia 81, 83.*
[17] *Withers Ebbs and Horey, above n 2, 162.*
[18] *'Beginners' Guide to Cyberspace', above n 16.*
[19] *Electronic Mail Study Group, Report, January 1996. Available at http://www.ogit.gov.au/ica/; Australian Science and Technology Council, Networked Nation, September 1994, 43.*
[20] *William Powell and Others, Tools For Privacy (1995). Available at ftp://ftp.crl.com/users/ro/smart/TFP/*
[21] *Krol and Ferguson, above n 14, 396.*
[22] *American Civil Liberties Union v Reno 929 F Supp 824 (1996) (US Court of Appeals) ('Reno').*
[23] *Withers Ebbs and Horey, above n 2, 166; Krol and Ferguson, above n 14, 66.*
[24] *Larry J Hughes, Internet Security Techniques (1995) 27.*
[25] *Simon Davies, Monitor (1996) 64.*
[26] *Bruce Schneier, E-Mail Security (1995) 9.*
[27] *See Telecommunications Act 1997 (Cth) s 56.*
[28] *See Ibid s 87.*
[29] *Reno 929 F Supp 824 (1996), 834.*
[30] *Krol and Ferguson, above n 14, 66.*
[31] *Hughes, above n 24, 27-8.*
[32] *Powell and Others, above n 20.*

CHAPTER 3 - THE CONCEPT OF PRIVACY

Introduction

A right to privacy was first recognised by Warren and Brandeis in 1890 when they equated privacy with an individual's 'right to be let alone'.[1] However, the search for a definition of privacy is described as producing a discussion which is 'often sterile and, ultimately, futile.'[2] The subject matter encompassed by the concept of privacy varies with changing social and cultural views. The Australian Law Reform Commission ('ALRC') acknowledges that the concept is elusive and despite numerous attempts a satisfactory definition of privacy has never been achieved.[3]

Australians are becoming increasingly concerned about their privacy. They rank the confidentiality of personal information second only to education when considering important social issues. Computers are seen as a major threat to privacy. Many people think that computers have made it easier for confidential personal information to fall into the wrong hands.[4] A popular definition of 'information privacy' is that:

'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'[5]

However, this definition has been criticised for being too broad on the basis that privacy is instead the condition of not having personal facts about oneself known which do not already belong to the public record.[6]

For the purposes of this article e-mail privacy is the ability of the sender of a message to prevent persons acquiring personal information about the sender or another person by snooping on the contents of the message where 'personal information' is limited to:

'[T]hose facts, communications or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore want to withhold, or at least to restrict their collection, use or circulation.'[7]

The Sections of this Chapter cover the following areas relating to the application of the concept of privacy to Internet e-mail. Section A outlines the philosophical basis for protecting the privacy of communications as a fundamental human right which individuals are reasonably entitled to expect unless outweighed by competing public interests. Section B considers the extent of Australia's international obligations in relation to privacy. Section C examines the privacy rights and expectations which have been recognised in Australia. Section D considers the circumstances in which carriers and service providers may snoop on e-mail without unreasonably intruding upon the privacy of users. Section E contains two e-mail privacy case studies concerning snooping on e-mail by a system administrator and hacker respectively.

A. The Protection of Privacy as a Fundamental Human Right

It is recognised that privacy is a fundamental human right which every individual may reasonably expect. It supports human dignity and other key values such as freedom of speech and association.[8] In the 1969 Boyer Lectures Professor Cowen equated privacy with dignity stating:

'A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars.'[9]

Similarly, Bloustein expresses the view that an intrusion on an individual's privacy injures his or her individuality and human dignity:

'The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.'[10]

Westin believes that privacy performs four basic functions for individuals, namely, personal autonomy, emotional release, self-evaluation and limits and protects communications.[11] He sees privacy as 'basically an instrument for achieving individual goals of self-realization.'[12]

It has been more recently proposed by Regan that privacy should also be considered from a social perspective as it is of value to society in general as

well as the individual. Three reasons are given for the social importance of privacy. First, that it is a common value of all individuals. Secondly, that it has a public value to the democratic political system derived from its importance to the exercise of rights essential to democracy such as freedom of speech and association. Thirdly, that it is rapidly becoming a collective value as a result of technology and market forces which make it difficult for an individual to have privacy without everyone having a similar minimum level of privacy.[13]

Both the ALRC[14] and the Australian Privacy Charter ('APC')[15] recognise that Australians value privacy and are increasingly demanding that their privacy be recognised and protected. The ALRC view of the need for privacy protection acknowledges the social value of privacy and accords with the following submission it received:

'We reject as completely intolerable a society in which there is a total lack of respect for privacy. A society in which there is no restriction, legal or otherwise, on bugging of homes, tapping of phones, reading of letters of others, spying, and the like by police, investigators, and ordinary individuals ... impresses as one in which it would be unpleasant, extremely disagreeable, to live. Complete loss of privacy would involve much more and worse than this.'[16]

In Australia the existence of a free and democratic society requires respect for the autonomy of individuals and that there be limits on the power of the state and others to intrude on that autonomy.[17] Snooping on e-mail passing over the Internet is a form of intrusion into one's personal autonomy that interferes with the fundamental right of privacy which individuals may reasonably expect.

1. *High Public Policy of Protecting the Privacy of Communications*

It has been suggested that the general rule of our society is that a telephone conversation is private and confidential to the participants.[18] In telephone conversations many law-abiding citizens express themselves 'in a high expectation of privacy and confidentiality, about matters which are personal, potentially embarrassing, hurtful and destructive of relationships as well as banal and harmless.'[19] A similar observation may be made of the ways people express themselves when communicating by e-mail over the Internet. The ALRC believes that the need for personal autonomy requires that as a general principle communications which are intended by the participants to be private should not be monitored or intercepted without their consent.[20] Communications by e-mail over the Internet are intended to be private in the sense that the sender of a message only intends that it be read by the intended recipient or recipients.

The detailed scheme of control contained in the Interception Act is designed to give effect to the high public policy of protecting the privacy of communications passing over the telecommunications system and community trust in the integrity of the system.[21] State and Territory legislation similarly recognises the importance of protecting the privacy of communications by regulating the use of listening devices to overhear and record private conversations.[22] Internet e-mail is merely another form of communication which similarly deserves protection for the privacy of its contents.

2. *Reasonable Expectation of Privacy in Communications by E-mail*

Whether a person has a reasonable expectation of privacy in communications made by e-mail has been considered by a United States Air Force Court of Criminal Appeals in United States v Maxwell.[23] Maxwell was a subscriber to America Online which is a private on-line computer service. America Online had about 215,000 subscribers in the United States at the relevant time. The subscribers were able to communicate with each other by sending e-mail.

It was reported to an FBI agent that a number of subscribers to America Online were using the service to transmit and receive child pornography. The FBI agent obtained a search warrant to seize electronic transmissions made by a number of subscribers including Maxwell which were stored on America Online computers. As a result of the search it was discovered that Maxwell was involved in suspected criminal activity. Maxwell argued that the seizing of incriminating evidence from the America Online computers was unlawful on the basis that it breached his right of privacy under the Fourth Amendment. A person asserting a right to privacy under the Fourth Amendment must show that he had an actual expectation of privacy which society is prepared to objectively recognise as reasonable.

In Maxwell the Court of Criminal Appeals found that the military judge was in error to the extent that he had based his decision to admit the evidence seized from the America Online computers on the absence of any objective expectation of privacy. The Court found that the appellant maintained an objective expectation of privacy in e-mail stored on America Online computers which only he could access using a password and in e-mail he sent to other subscribers who had been individually assigned passwords.[24] The Court commented that:

'Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that appellant's computer transmissions would be received by anyone other than the intended recipients. .... In the modern age of communications, society must recognise such expectations of privacy as reasonable.'[25]

In Australia society must also recognise that individuals have a reasonable expectation in the privacy of their communications by Internet e-mail and protect the contents of messages from unreasonable intrusions.

3. *Balancing Privacy Interests and Competing Public Interests*

Warren and Brandeis themselves agreed that there are limitations on the right to privacy and that it does not prevent the publication of matters in the public interest.[26] The term 'public interest' is used in a broad sense in this article to denote both public and private social interests. Privacy interests are not absolute and must be balanced with complementary interests such as freedom of communication against competing public interests which include interests relating to law enforcement, national security, public revenue, public safety and rights and freedoms of others. The interests to be balanced at any particular time will depend upon the circumstances in the particular situation. Intrusions upon the privacy of an individual will not be unreasonable in circumstances where competing public interests outweigh privacy interests to a substantial degree.

Where privacy interests are to a substantial degree outweighed by competing public interests in intercepting communications it has been acknowledged internationally that privacy interests still require that there be stringent controls on the circumstances in which parliaments may permit interception and on the use which may be made of information obtain by such interception. In Klass v Federal Republic of Germany[27] the European Court of Human Rights expressed the view that the mere existence of legislation which permitted State authorities to listen to telephone conversations was a 'menace of surveillance' for all those to whom it could be applied.[28] Similarly, in Malone v Metropolitan Police Commissioner[29] Megarry V-C commented:

'However much the protection of the public against crime demands that in proper cases the police should have the assistance of telephone tapping, I would have thought that in any civilised system of law the claims of liberty and justice would require that telephone users should have effective and independent safeguards against possible abuses.'[30]

In enacting the Interception Act the Australian Parliament recognised the fundamental importance of protecting the privacy of communications although also recognising that privacy may be overridden where it conflicts with other significant community values provided that adequate safeguards exist.[31] Intrusions into telephone conversations are subject to strict controls under the Interception Act even where the intrusion is by a law enforcement or national security agency.[32] Similarly there should also be strict controls on intrusions into e-mail communications by persons snooping on the Internet to prevent possible abuses.

4. *Privacy and the Competing Public Interest of Law Enforcement*

The privacy of Internet e-mail may be unreasonably intruded upon by carriers and service providers snooping on its contents for the purpose of law enforcement by seeking to detect the commission of an offence under censorship legislation in Australia. Legislation to censor material transmitted over the Internet has already been enacted in Victoria, Western Australia and the Northern Territory.[33] However, the interests in law enforcement by seeking to detect the commission of an offence under this legislation may not outweigh the interests in the privacy of e-mail.

In Victoria, Western Australia and the Northern Territory it is an offence to use an on-line computer service to knowingly transmit objectionable material.[34] An on-line computer service is a service which permits the transmission of data or computer programs.[35] An Internet e-mail service is an on-line computer service as it permits the transmission of e-mail over the Internet. It would be an offence to send e-mail over the Internet which contains objectionable material.

The Federal Government and the Australian Broadcasting Authority ('ABA') have taken similar approaches to the censorship of private communications. A United States Court of Appeals has also considered the issue of censorship of communications over the Internet.

(a) *Policy of the Federal Government and Recommendation by the Australian Broadcasting Authority on Censorship*

The Federal Government released its policy for the regulation of on-line services prior to the last Federal Election. In relation to private communications the policy stated:

'Private one-to-one communications should remain private, apart from exceptional circumstances already covered by existing legal constraints, and will not be subject to more onerous regulation than are private communications in other media such as the letter post or telephony.'[36]

The ABA subsequently conducted an investigation into the regulation of the content of on-line services which also addressed the issue of private communications. The ABA relied upon intent as the basis for distinguishing between private and public communications. It considered a communication to be a private communication if it is the intention of the sender that only one individual or a small group of individuals should have access to the content of the communication. On the other hand it considered a communication to be a public communication if it is the intention of the sender that the content of the communication should be widely accessible.[37]

The sender of e-mail intends that the contents of the message only be made available to the person or persons to whom the message is addressed. In the ABA's view this characteristic of e-mail demonstrates that e-mail messages are essentially private communications. However, the ABA recognised that e-mail may take on the characteristics of a narrowcast or even a broadcast where it is addressed to a sufficiently large mailing list. In these circumstances e-mail may not be considered to be essentially private in nature.[38] After conducting its investigation the ABA recommended that:

'[W]hile the borders may be blurred to some degree the ABA believes that communications which are intended to be essentially private in nature, such as e-mail, should be exempted from content regulation.'[39]

The Federal Government and the ABA have both recognised the high public policy of protecting the privacy of communications which are intended to be private in nature. The censorship legislation in Victoria, Western Australia and the Northern Territory is inconsistent with the policy of the Federal Government and the recommendation of the ABA to the extent to which it applies to private communications by Internet e-mail. The interests in law enforcement by seeking to detect the commission of an offence under this legislation do not outweigh to a substantial degree the interests in the privacy of e-mail in circumstances where the message is intended to be a private communication.

(b) Censorship Legislation Held to be Unconstitutional by United States Court of Appeal

In American Civil Liberties Union v Reno[40] the plaintiffs[41] sought a preliminary injunction against the enforcement of challenged provisions[42] of the Communications Decency Act 1996 (US) ('CDA'). An offence is committed under the challenged provisions where a person uses a telecommunications device in interstate or foreign communications to knowingly transmit any obscene or indecent communication to a person under 18.[43]

The Court of Appeals in Reno held that the challenged provisions of the CDA were unconstitutional as they swept more broadly than necessary to prevent minors accessing indecent material on-line and would have a 'chilling effect' on the exercise of free speech by adult users.[44] In considering the regulation of content on the Internet Dalzell J expressed the view that 'the Internet deserves the broadest possible protection from government-imposed, content-based regulation.'[45] Dalzell J further stated:

'[T]he Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion.'[46]

In Australia the High Court has held that it is implied from the system of representative democracy for which the Australian Constitution makes provision that there is a right to freedom of communication in relation to public affairs and political discussion.[47] The Interception Act sustains and protects this implied constitutional freedom of communication by upholding privacy. If communications were not protected there would be a chilling effect as citizens would be even more suspicious of the privacy of their communications.[48] The chilling effect is applicable to communications by e-mail which also deserve the highest protection from intrusion whether by the Federal Government or anyone else in circumstances where public interests do not outweigh privacy interests to a substantial degree.

B. Australia's International Privacy Obligations

Australia has international privacy obligations under three instruments, namely, the International Covenant on Civil and Political Rights ('ICCPR')[49] and OECD Data Protection[50] and Security[51] Guidelines. Australia has either ratified or formally adopted each of these instruments.

1. International Covenant on Civil and Political Rights

On 4 August 1980 Australia ratified the ICCPR subject to several reservations and declarations.[52] Australia has been bound by international law to comply with the ICCPR within the terms of its ratification since 13 November 1980 when the ICCPR entered into force for Australia.[53] Where the common law is uncertain or legislation is ambiguous an Australian court may have regard to the provisions of the ICCPR to help resolve the uncertainty or ambiguity.[54] Although the ICCPR is included as a schedule to the Human Rights and Equal Opportunity Commission Act 1986 (Cth) it is not part of Australian municipal law.[55] However, the Human Rights and Equal Opportunity Commission has functions which include inquiring into any act or practice that may be inconsistent with any of the human rights and freedoms recognised by the ICCPR, promoting an understanding and acceptance of these human rights and freedoms and reporting to the Minister as to the action which needs to be taken by Australia in order to comply with the ICCPR.[56]

Article 17 of the ICCPR requires Australia to adopt such legislative or other measures necessary to ensure that all individuals within Australia have the right to protection of the law against arbitrary or unlawful interferences with his or her privacy, home and correspondence.[57] However, this requirement was ratified by Australia without prejudice to its right to enact laws authorising actions which impinge on an individual's privacy, home or correspondence in circumstances where the laws are necessary in a democratic society in the interests of national security, public safety, economic well-being of the country, protection of public health and morals or protection of the rights and freedoms of others.[58] Any law which affects an individual's privacy, home or correspondence must be sufficiently clear to give people an adequate indication of the circumstances in which an individual's privacy, home or correspondence may be interfered with.[59]

In Malone v United Kingdom[60] the European Court of Human Rights expressed the view that the interception by the police of a person's telephone communications for the purposes of a criminal investigation involved an unjustified interference by a public authority with the person's right to respect for his private life and correspondence contrary to Article 8 of the European Convention on Human Rights.[61] Article 8 of the Convention is similar to Article 17 of the ICCPR as ratified

by Australia. In Australia snooping on a communication by intercepting e-mail would similarly constitute an interference with the private life and correspondence of an individual.

In order to comply with its international legal obligations under the ICCPR Australia must enact laws which prevent e-mail being subjected to arbitrary interference by persons snooping on the Internet except where the interference is necessary in the interests of national security, public safety, economic well-being, public health and morals or rights and freedoms of others.

2. *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*

As a Member Country[62] of the OECD Australia proposed to formally adhere to the OECD Data Protection Guidelines in December 1984.[63] The Guidelines contain eight basic data protection principles applicable to both the public and private sectors which Member Countries are expected to implement with legal, administrative or other procedures to protect the privacy of individuals in relation to their personal data. Australia is not bound by international law to observe the Guidelines as they do not have treaty status. However, Australia is morally bound to comply with the Guidelines as a result of adopting them. The Principles contained in the Guidelines which are relevant to snooping are the Collection Limitation Principle, Use Limitation Principle and Security Safeguards Principle.

The Data Protection Guidelines define 'personal data' to mean 'any information relating to an identified or identifiable individual (data subject)'. E-mail will contain 'personal data' where it contains information about a person whose identity is apparent or can be ascertained from the contents of the message.

Personal data should be obtained by lawful and fair means and with the knowledge and consent of the data subject where appropriate in accordance with the Collection Limitation Principle. The collection of personal data by snooping may be contrary to this Principle on the basis that it constitutes the collection of data by unfair means.

Pursuant to the Use Limitation Principle personal data should not be used or disclosed other than for a purpose specified not later than at the time of collection except with the consent of the data subject or by lawful authority. A person who collects personal data by snooping on e-mail would act contrary to this Principle if he or she used or disclosed the data without the data subject's consent or lawful authority.

The Security Safeguards Principle requires that personal data should be protected by reasonable security safeguards against unauthorised access, use or disclosure. Carriers and service providers which supply Internet e-mail services should be required to use security safeguards such as password protection, secure networks and encryption where appropriate to protect e-mail. The appropriateness or providing security safeguards is considered in relation to the OECD Security Guidelines below.

3. *OECD Guidelines for the Security of Information Systems*

Australia and the other OECD Member Countries adopted the OECD Security Guidelines on 26 November 1992.[64] The Guidelines apply to all information systems in the public and private sectors and are intended to act as a foundation for the construction of a framework by Member Countries for the protection of these systems which should include legal, administrative, self-regulatory and other measures. Again Australia is not bound by international law to observe the Guidelines as they do not have treaty status but is morally bound to comply with the Guidelines. The Ethics Principle and Proportionality Principle contained in the Guidelines are relevant to Internet e-mail services.

The Guidelines define 'information systems' to mean 'computers, communications facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them'. Computers used to supply Internet e-mail services would be 'information systems' for the purposes of the Guidelines.

The Ethics Principle requires that the use, provision and security of information systems should be such that the rights and legitimate interests of others are respected. Carriers and service providers should be required to ensure that the use, provision and security of Internet e-mail services is such that the privacy rights and interests of users are respected.

In accordance with the Proportionality Principle security measures should be appropriate and proportionate to the value of and degree of reliance on information systems and to the potential harm resulting from a security failure. Security measures should be assessed by weighing the cost of each possible security measure against the severity and probability of harm and its costs.[65] Carriers and service providers which supply Internet e-mail services should be required to take security measures which are appropriate and proportionate to the value of and degree of reliance users place on their services and the potential harm caused by snooping on e-mail. This will depend upon the circumstances in the particular situation.

C. *Recognition of Privacy Rights and Expectations in Australia*

Although the common law in Australia does not recognise a general legal right of privacy, the Privacy Act 1988 (Cth) ('Privacy Act') expressly protects personal information. The Australian Privacy Charter ('APC') also expressly sets out the privacy rights that people are entitled to expect will be recognised and protected.

1. *General Legal Right of Privacy not Recognised by the Common Law in Australia*

In Australia the common law does not recognise a tort of violation of privacy which would protect e-mail containing personal information from a person snooping on the Internet.[66]

The decision by the High Court in Victoria Park Racing Co v Taylor[67] is generally cited as authority for this proposition. The High Court held that no action could be taken by the plaintiff to prevent the defendant broadcasting horse races from a platform overlooking the plaintiff's racecourse which had been constructed on the defendant's adjoining land. Latham CJ stated:

'The claim ... has also been supported by an argument that the law recognises a right of privacy which has been infringed by the defendant. However desirable some limitation upon invasions of privacy might be, no authority was cited which shows any general right of privacy exists.'[68]

As there is no actionable general legal right of privacy the acquisition of personal information by a person snooping on the Internet would not constitute tortious conduct. The common law provides only limited and incidental privacy protection against snooping on e-mail in circumstances where there is a breach of an existing law. Examples of existing laws which provide limited and incidental protection include the laws relating to breach of confidence, trespass, nuisance, passing off, injurious falsehood and defamation.[69]

2. *Privacy Rights under the Privacy Act and Privacy Expectations under the Australian Privacy Charter*

In Australia the Privacy Act expressly protects the privacy of personal information. The protection provided for Internet e-mail by the Privacy Act under the Telecommunications Industry Ombudsman scheme is considered in Chapter 6. The Copyright Act 1968 (Cth) may also provide incidental privacy protection for e-mail by prohibiting the copying of messages in certain circumstances. However, consideration of copyright infringement issues is beyond the scope of this article.[70]

In addition to these legislative initiatives several of the Privacy Principles contained in the APC apply to personal information. The APC was launched by the APC Council on 5 December 1995.[71] The aim of the Council is to take privacy protection beyond the regulatory environment and into the private sector as an issue of best practice.[72] The Privacy Principles contained in the APC are intended to act as a benchmark against which to measure the practices of both the public and private sectors and the adequacy of codes and legislation.[73]

In acknowledging the concerns of Australians about privacy the APC notes that Australians value privacy and expect that their rights to privacy will be recognised and protected. The APC states that people have a right to privacy of their communications, information privacy and freedom from surveillance. The Privacy Principles contained in the APC set out the privacy rights that people are entitled to expect will be recognised and protected and the obligations of others to respect those rights. However, the Privacy Principles have no legal status and create no legal obligations.[74] The Privacy Principles which are relevant to snooping on e-mail are the Surveillance Principle, Privacy of Communications Principle, Collection Limitation Principle, Use and Disclosure Limitation Principle, Security Principle and Retention Limitation Principle.

The Freedom from Surveillance Principle recognises that people have a right to conduct their affairs free from surveillance by the observation or recording of their communications or personal information. People are entitled to expect that they may conduct their affairs by e-mail without anyone snooping on the contents of their messages.

In accordance with the Privacy of Communications Principle people who wish to communicate privately are entitled to respect for their privacy even when communicating in public places. The Internet may be regarded as a public place in the sense that any member of the public may obtain access to the Internet through a carrier or service provider for the purpose of accessing services available on the Internet. However, this would not preclude people wishing to communicate privately by e-mail over the Internet being entitled to expect that the privacy of their messages would be respected.

The collection of personal information should not be surreptitious and only the minimum amount of personal information should be collected by lawful and fair means and for a lawful and precise purpose specified at the time of collection in order to comply with the Collection Limitation Principle. People are entitled to expect that personal information would not be collected by a person surreptitiously snooping on e-mail passing over the Internet. Snooping on e-mail is inconsistent with this Principle as no purpose is specified at the time of the collection of any personal information and it may constitute the collection of such information by unfair means. However, in accordance with the Consent Principle the consent of the person concerned may justify snooping on e-mail without breaching the Collection Principle.

The Use and Disclosure Limitation Principle recognises that personal information should only be used or disclosed for the purpose specified at the time of collection or for any purpose authorised by law or consented to by the person concerned. A person who obtains personal information by snooping on e-mail would act inconsistently with this Principle if he or she used or disclosed the information without lawful authority or consent.

Pursuant to the Security Principle personal information should be protected by security safeguards proportionate to its sensitivity and adequate to ensure compliance with the APC. Security safeguards which people are entitled to expect that carriers and service providers would use to protect e-mail include password protection, secure networks and encryption where appropriate. The appropriateness of providing security safeguards is considered above in relation to the OECD Security Guidelines.

The Retention Limitation Principle recognises that personal information should be destroyed or made anonymous after it is no longer

required for its lawful uses. People are entitled to expect that copies of e-mail containing personal information will not be kept by carriers and service providers any longer than necessary for a lawful purpose.

D. Snooping on E-mail by Carriers and Service Providers Without Unreasonably Intruding Upon the Privacy of Users

Carriers and service providers legitimately need to collect personal information by snooping on e-mail sent over the Internet for purposes such as message transmission, back-up, billing, network operation and network maintenance. Information collected by carriers and service providers for these purposes may legitimately need to be used, disclosed and retained by them.

A person who sends e-mail over the Internet probably impliedly consents to carriers and service providers collecting personal information by snooping on the message and using and disclosing such information for the purpose of message transmission. It should be understood by senders of e-mail that message transmission may involve the collection, use and disclosure of a copy of the message by carriers and service providers operating intermediate computers over which the message passes.

Where a person uses an Internet e-mail service supplied by a carrier or service provider he or she probably impliedly consents to the carrier or service provider collecting personal information by snooping on the message and using, disclosing and retaining such information for the purposes of back-up and billing. It is common practice to collect and retain copies of messages in case of accidental loss or unauthorised alteration or destruction. If such loss, alteration or destruction occurs then a carrier or service provider may need to use or disclose a copy of the message. A person should appreciate that a carrier or service provider which charges its customers according to the amount of data which they transmit over the Internet needs to collect, use, disclose and retain a copy of the header of messages which contains information about their length.

Personal information may be collected, used, disclosed and retained by carriers and service providers where the person concerned consents without there being a breach of the OECD Data Protection Guidelines or APC. However, carriers and service providers may need to be specifically authorised by law to collect personal information by snooping on e-mail and to use, disclose and retain such information for the purposes of network operation and network maintenance without there being a breach of the OECD Data Protection Guidelines or APC in circumstances where the individual concerned does not expressly or impliedly consent. Network operation and network maintenance are arguably tasks which are carried out by carriers and service providers in the interest of protecting the rights and freedoms of other persons to use Internet e-mail services. Australia may enact laws to protect the rights and freedoms of others without breaching the ICCPR as ratified by Australia.

Carriers and service providers may also legitimately need to collect personal information by snooping on Internet e-mail and to use, disclose and retain such information where the individual concerned has not expressly or impliedly consented and where there is no specific authorisation by law. However, it would be an unreasonable intrusion upon the privacy of users to allow carriers and service providers to collect personal information by snooping and to use, disclose and retain such information for any lawful purpose as this would be equivalent to permitting the collection, use, disclosure and retention of such information unless prohibited by law.

Unless specifically authorised by law or with the express or implied consent of the individual concerned carriers and service providers should only be permitted to collect personal information by snooping and to use, disclose and retain such information where necessary for a lawful purpose in the public interest. The interests to be balanced will depend upon the circumstances in the particular situation. If the public interests outweigh privacy interests to a substantial degree then carriers and service providers may collect, use, disclose and retain such information without unreasonably intruding upon the privacy of the individual concerned. However, carriers and service providers should only be permitted to collect the minimum amount of personal information necessary for a lawful purpose in accordance with the APC.

A code of practice should be required to be developed by carriers and service providers which provides guidance as to when the collection of personal information by snooping on e-mail and the use, disclosure and retention of such information will be necessary for a lawful purpose in the public interest. The development of industry codes and standards under the Telecommunications Act 1997 (Cth) is discussed in Chapter 8.

E. E-mail Privacy Case Studies

There have been two highly publicised incidents in Australia which have involved snooping on e-mail. The first concerned a 22 year old student, Quincey, who was charged under the Classification of Computer Games and Images (Interim) Act 1995 (Qld) ('Queensland Classification Act') after a system administrator came across pornographic material whilst clearing Quincey's mailbox. The second involved a hacker, Peter Mackay, leaking copies of personal and politically sensitive e-mail messages from the Federal Attorney-General's Department to the Shadow Attorney-General.

Case Study I: System Administrator Snooping on E-mail

Quincey subscribed to an Internet access service supplied by a service provider known as Global Information Links ('GIL'). A system administrator employed by GIL noticed pornographic file names whilst clearing a temporary directory of downloaded files on GIL's host

computer. He reported this to the police who raided Quincey's home and confiscated computer hardware and boxes of disks.[75] Quincey was charged under the Queensland Classification Act with the offences of possession and copying of child pornography depicted in a child abuse computer game.[76] However, the charge of possession of child pornography was dropped shortly before trial.[77]

After the raid GIL publicly stated that it would 'continue to provide police with the names of any members found peddling pornography on the Internet'. System administrators of GIL were reported to be looking for anything irregular whilst clearing the mailboxes of GIL's subscribers.[78] In response to this report GIL's subscribers expressed their privacy concerns by writing to GIL requesting specific advice on GIL's privacy policies. GIL did not provide the advice requested or any official response at all.[79]

At trial the system administrator gave evidence that the defendant downloaded the files from an Internet site at Michigan State University.[80] The defendant claimed to have deleted the files as soon as he found out what they contained.[81] Robertson J found that the files downloaded by the defendant were within the wide definition of 'bulletin board' and thereby excluded from the definition of 'computer game'.[82] The jury was instructed to return a verdict of not guilty and the defendant was discharged.[83]

This case involving Quincey highlights the tension between the protection of privacy and the creation of an offence which applies to the content of material transmitted over the Internet. GIL's subscribers were justified in expressing their privacy concerns with the actions taken by GIL snooping on their private e-mail. GIL appears to have given no consideration to the privacy intrusive nature of its actions. The privacy of users of e-mail may be unreasonably intruded upon by carriers and service providers which take it upon themselves to snoop on the contents of messages for the purpose of ascertaining whether any users have committed an offence under censorship legislation in Australia.

Case Study II: Hacker Snooping on E-mail

In 1995 the Federal Attorney-General's Department was subject to an attack by a hacker which involved the leaking of 13,000 copies of personal and politically sensitive e-mail messages to Amanda Vanstone who was at the time the Federal Shadow Attorney-General.[84] It is reported to be the biggest leak of information in the entire history of the Federal Government.[85] The Attorney-General's Department provides its officers with both a private and public Internet e-mail service which enables them to send internal messages within the Department and external messages over the Internet.

Peter Mackay was an information technology officer employed with the Attorney-General's Department at the time he copied onto disks e-mail messages containing personal and politically sensitive information from the mailboxes of 129 officers of the Department.[86] He was able to crack the passwords of officers which were blank or used their user identification or a variant of their identification. Mackay also wrote a program called 'SDKHelp' which he used to crack the passwords of officers.[87]

Mackay delivered the disks containing the copies of the e-mail messages to Vanstone in packages. Vanstone received 36 disks in total which she promptly returned to the Attorney-General's Department.[88] A week later the police arrested Mackay who was charged with disclosing information and sentenced to nine months in jail of which he served three before being released.[89]

If Mackay had not delivered copies of the e-mail messages to Vanstone his privacy intrusive actions may never have been detected and he may not have been arrested. It is often extremely difficult to ascertain whether a person has snooped on the contents of an e-mail message. Many organisations are reluctant to report anyone they discover snooping on their computer system for fear of adverse publicity and a potential loss in confidence of customers who use the system.[90]

It is claimed that hackers make up to 100 attacks per day against Federal Government computer systems alone.[91] A series of recent attacks by hackers has compromised the computer systems of Internet service providers around the world. The hackers exploited a gap in computer software which enabled them to launch attacks on computer systems remotely bypassing Internet security features such as firewalls.[92]

Conclusion

A right of privacy was first recognised by Warren and Brandeis in 1890. Although, privacy has since been widely recognised as a fundamental human value which individuals are reasonably entitled to expect, the common law in Australia has failed to recognise any such general legal right. A right of privacy is not only of value to individuals but to society generally.

An important element of privacy is respect for the personal autonomy of individuals which requires that communications which are intended to be private should be protected. People expect that communications by e-mail will remain private and confidential to the sender and recipient. In Australia society must recognise as reasonable the expectation of privacy for e-mail communications particularly where Australians are increasingly becoming concerned about their privacy.

Privacy interests must be balanced with complementary interests against competing public interests. Where privacy interests are outweighed by public interests to a substantial degree intrusion upon the privacy of the individual concerned will not be unreasonable. In balancing these interests the Federal Government, ABA and the United States Court of Appeal in Reno have given precedence to the interests in protecting the privacy of communications. However, even when privacy interests are outweighed to a substantial degree by

competing public interests which take precedence there is still a need to safeguard privacy interests against possible abuses.

In order to comply with its international legal obligations under the ICCPR Australia must enact laws which prohibit Internet e-mail being subject to arbitrary interference by persons snooping on the Internet unless the interference is necessary in the public interest. Australia has a moral obligation under the OECD Security Guidelines to ensure that the use, provision and security of Internet e-mail services respect the privacy rights and interests of users of such services. The APC has similarly recognised 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 snooping on e-mail and the use, disclosure and retention of such information by carriers and service providers would not breach the OECD Data Protection Guidelines or APC where the individual concerned consents or where authorised by law. A person who sends e-mail over the Internet probably impliedly consents to carriers and service providers collecting, using, disclosing and retaining personal information for the purposes of message transmission, back-up and billing. However, carriers and service providers would need to be specifically authorised by law to collect, use, disclose and retain personal information for the purposes of network operation and network maintenance without there being a breach of the OECD Data Protection Guidelines or APC.

Unless specifically authorised by law or with the express or implied consent of the individual concerned carriers and service providers should only be permitted to collect personal information by snooping on e-mail and to use, disclose and retain such information where necessary for lawful purposes in the public interest. Carriers and service providers which supply Internet e-mail services should develop a code of practice to provide guidance as to when the collection, use, disclosure and retention of such information will be necessary for a lawful purpose in the public interest. In accordance with the APC only the minimum amount of personal information necessary for a lawful purpose should be collected by carriers and service providers. Additionally, there should be a requirement on carriers and service providers to protect e-mail and Internet e-mail services with reasonable security safeguards such as password protection, secure networks and encryption where appropriate to comply with the OECD Data Protection and Security Guidelines and APC.

[Chapters 4 to 10 and the Conclusion will be published in the next two issues of the Journal]

[1] *Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.*

[2] *Raymond Wacks, 'The Poverty of "Privacy"' (1980) 96 Law Quarterly Journal 73, 75.*

[3] *Australian Law Reform Commission, Report No 22, Privacy (1983) Vol 1 paras 19-20 ('ALRC Report').*

[4] *Privacy Commissioner, Community Attitudes to Privacy, August 1995, 7-10.*

[5] *Alan F Westin, Privacy and Freedom (1967) 7.*

[6] *William A Parent, 'A New Definition of Privacy for the Law', (1983) 2 Law and Philosophy 305, 308, 329.*

[7] *Raymond Wacks, 'Introduction', Privacy - International Library of Essays in Law and Legal Theory (1993) Vol 1, xvi.*

[8] *John Fairfax Publications v Doe (1995) 37 NSWLR 81, 97 (Kirby P) ('John Fairfax Publications'); Australian Privacy Charter Council, Australian Privacy Charter, December 1994.*

[9] *Professor Zelman Cowen, The Private Man (1969) 9.*

[10] *Edward J Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 New York University Law Review 962, 1003.*

[11] *Westin, above n 5, 37.*

[12] *Westin, above n 5, 39.*

[13] *Priscilla M Regan, Legislating Privacy (1995) 212-43.*

[14] *ALRC Report Vol 1 para 35.*

[15] *Australian Privacy Charter Council, above n 8.*

[16] *McCloskey, 'The Concept of Privacy and the Right to Privacy', Submission to the Australian Law Reform Commission (1978) 1. See ALRC Report Vol 1 para 35.*

[17] *Australian Privacy Charter Council, above n 8.*

[18] *John Fairfax Publications (1995) 37 NSWLR 81, 97 (Kirby P).*

[19] *Ibid.*

[20] *ALRC Report Vol 2 para 1126.*

[21] *John Fairfax Publications (1995) 37 NSWLR 81, 97 (Kirby P); Director of Public Prosecutions v Serratore (1995) 38 NSWLR 137, 147 (Kirby P).*

[22] *Listening Devices Act 1969 (Vic); Listening Devices Act 1984 (NSW); Listening Devices Act 1972 (SA); Listening Devices Act 1978 (WA); Listening Devices Act 1991 (Tas); Listening Devices Act 1992 (ACT); Listening Devices Act 1990 (NT); Invasion of Privacy Act 1971 (Qld).*

[23] *42 MJ 568 (1995) ('Maxwell').*

[24] *Ibid 575.*

[25] *Ibid 576. cf Smyth v The Pillsbury Company 914 F Supp 97 (1996) (US District Court).*

[26] *Warren and Brandeis, above n 1, 214-6.*

[27] *(1978) 2 EHRR 214 ('Klass').*

[28] *Ibid 230.*

[29] *[1979] 1 Ch 344.*

[30] *Ibid 381.*

[31] *Taciak v Australian Federal Police (1995) 131 ALR 319, 331 (Sackville J).*

[32] *John Fairfax Publications (1995) 37 NSWLR 81, 97 (Kirby P).*

[33] *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic) ('Victorian Classification Act'); Censorship Act 1996 (WA) ('WA Censorship Act'); Classification of Publications and Films Act (NT) ('NT Classification Act')*

[34] *Victorian Classification Act ss 57(1), 57(3); WA Censorship Act s 101(1)(a); NT Classification Act s 50Z(1)(a).*

[35] *Victorian Classification Act s 56; WA Censorship Act s 99; NT Classification Act s 50X.*

[36] *Federal Government, Australia Online, February 1996, 17.*

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

[38] *Ibid.*

[39] *Ibid.*

[40] *929 F Supp 824 (1996) (US Court of*

Appeals) ('Reno').

[41] The American Civil Liberties Union includes 'various organisations and individuals who, inter alia, are associated with the computer and/or communications industries, or who publish or post materials on the Internet, or belong to various citizens groups.': Ibid.

[42] CDA ss 223(a), 223(b).

[43] CDA s 223(a)(1)(B).

[44] Reno 929 F Supp 824 (1996) (Sloviter CJ and Buckwalter J). The decision of the Court of Appeals has been appealed to the US Supreme Court. See also Shea v Reno 930 F Supp 916 (1996) (US District Court).

[45] Reno 929 F Supp 824 (1996).

[46] Ibid.

[47] Australian Capital Television Pty Ltd v Commonwealth (1992) 177 CLR 106 ('Australian Capital Television'); Nationwide News v Wills (1992) 177 CLR 1 ('Nationwide News'). See also Theophanous v Herald & Weekly Times Ltd (1994) 68 ALJR 713; Stephens v West Australian Newspapers Ltd (1994) 68 ALJR 765. In the cases of Levy v Victoria and Lange v Australian Broadcasting Corporation application has been made to the High Court to reopen and reconsider the decisions in Australian Capital Television and Nationwide News.

[48] John Fairfax Publications (1995) 37 NSWLR 81, 109 (Kirby P).

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

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

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

[52] Department of Foreign Affairs, above n 49, 18-20.

[53] Department of Foreign Affairs, above n 49, footnote 6.

[54] Mabo v The State of Queensland (1992) 175 CLR 1, 42 (Brennan J); Dietrich v The Queen (1992) 177 CLR 292, 360 (Toohey J) ('Dietrich')

[55] Kioa v West (1985) 159 CLR 550, 570 (Gibbs CJ); Dietrich (1992) 177 CLR 292, 305-6 (Mason CJ and McHugh J), 359-60 (Toohey J).

[56] Human Rights and Equal Opportunity Act 1986 (Cth) s 11.

[57] Department of Foreign Affairs, above n 49, 6. See also Universal Declaration of Human Rights Article 12; European Convention on Human Rights Article 8.

[58] Department of Foreign Affairs, above n 49, 19.

[59] See Malone v United Kingdom (1984) 7 EHRR 14, 40-41.

[60] (1984) 7 EHRR 14.

[61] Ibid 38-9. See also Klass (1978) 2 EHRR 214, 230.

[62] Australia became a Member Country of the OECD by acceding to the Convention on the Organisation for Economic Co-operation and Development on 7 June 1971: Department of Foreign Affairs, 'Convention on the Organisation for Economic Co-operation and Development' (1971) No 11 Australian Treaty Series 4, footnote †. The other Member Countries of the OECD are Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, New Zealand, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States.

[63] Federal Attorney-General's Department, Press Release No 180/84, 10 December 1984.

[64] Organisation for Economic Co-operation and Development, Press Release, 27 November 1992.

[65] Explanatory Memorandum Accompanying the Organisation for Economic Co-operation and Development Guidelines for the Security of Information Systems (1992).

[66] ALRC Report Vol 1 para 805.

[67] (1937) 58 CLR 479 ('Victoria Park Racing'). See also Kizon v Palmer (Unreported, Federal Court, Jenkinson Lindgren and Kiefel JJ, 31 January 1997); Tom Cruise and Nicole Kidman v Southdown Press Pty Ltd (1993) 26 IPR 125; Australian Consolidated Press v Ettinghausen (Unreported, New South Wales Court of Appeal, Gleeson CJ Kirby P and Clarke JA, 13 October 1993) 14; Kaye v Robertson [1991] FSR 62; Malone v Metropolitan Police Commissioner [1979] 1 Ch 344; Bernstein v Skyviews Ltd [1978] 1 QB 479.

[68] Victoria Park Racing (1937) 58 CLR 479, 495-6.

[69] Maureen Tangney, 'Is there a tort of privacy in Australia?' (1992) 11(1) Communications Law Bulletin 38. See also Gordon Hughes, Data Protection in Australia (1991) 224-55.

[70] See Gordon Hughes, Data Protection in Australia (1991) 250-53.

[71] Graham Greenleaf, 'Information Technology and the Law' (1995) 69 Australian Law Journal 90.

[72] Tim Dixon, 'Privacy Charter sets new benchmark in privacy protection' (1995) 2(3) Privacy Law & Policy Reporter 41.

[73] Greenleaf, above n 71, 90.

[74] Australian Telecommunications Authority, Privacy Advisory Committee, Telemarketing and the Protection of the Privacy of Individuals, October 1995, 22.

[75] R v Quincey (Unreported, Ipswich District Court, Robertson J, 29 October 1996) ('Quincey').

[76] Queensland Classification Act ss 26(3), 27(4), Schedule 2 - see definitions of 'computer game' and 'computer generated image'.

[77] Irene Graham, 'The First "Net Porn" Trial in Queensland - Verdict: Not Guilty', 15 December 1996. Available at http://www.com.au/~rene/liberty/

[78] Ibid.

[79] Ibid.

[80] Quincey.

[81] Ibid.

[82] Queensland Classification Act Schedule 2.

[83] Quincey.

[84] John Hilvert, 'Hacker fights to get back federal PS job', The Australian, 17 October 1996.

[85] Craig Henderson and Tracey Aubin, 'To Catch a Spy', Who, 3 July 1995, 28.

[86] Ibid.

[87] Hilvert, above n 84.

[88] Henderson and Aubin, above n 85, 28-9.

[89] Hilvert, above n 84.

[90] Vic Kamay, 'Shifting the Paradigm of Computer Crime and Enterprise Security', Proceedings of Combating Computer Fraud (Conference), 7-8 June 1995, 2.

[91] Tasker Ryrie, 'Beware: hacker attack!', Charter, February 1997, 28.

[92] Charles Wright, 'Hackers compromise Internet providers', Financial Review, 19 March 1997; Steve Creedy, 'Hackers run riot through servers', The Australian, 25 March 1997.