The Internet and privacy — some issues facing the private sector

Paul McGinness

Privacy may be described as:

> "the interest of the individual in deciding for himself how much of his personal life he will share with others, that is, to decide for himself whether personal information will be communicated to others, and if so to whom, when, how and to what extent".[1]

This definition indicates that the notion of "Privacy" extends beyond the concept of preventing a person from going through one's underwear drawer. It may encompass the ability to deliver information to a colleague without a third person being able to see it, the ability to screen information from "sensitive" eyes, the ability to treat information as being confidential, the desire not to be involuntarily subjected to other people's whims or the disclosure of information to third persons without authorisation.

These concepts are by no means a leviathan which have arisen from the on-line communication quagmire. Legal principles and legislation have been introduced over many years to deal with these concepts although there is no doubt that the rate of development of modern technology has added a new dimension to dealing with these issues. This paper considers some of these aspects of privacy and the Internet which may be applicable to the private sector.

Duty of confidence & encryption

It is well accepted that a person who receives information which is confidential in nature is not entitled to disclose that information without the consent of the confider or until the information has entered into the public domain other than as a result of the disclosure by the confidant.[2] One of the elements required to attract the duty of confidence is that the information must have been imparted in circumstances importing an obligation of confidence.[3]

It may be said that the placement of information upon on-line bulletin boards is akin to public display and that even the use of E-mail is analogous to sending messages by postcard. The argument runs that such messages cannot be said to have been imparted in circumstances importing an obligation of confidence if every man and his literate dog can read the message. Consequently, it would appear that the placement or transmission of information (that is confidential in nature) by a confidant on the Internet, without taking any steps to maintain secrecy, would constitute a breach of that person's duty of confidence.

Alternatively, the placement of confidential information on the Internet by the confider without security measures may preclude the confider from claiming the information continues to be confidential. This would certainly be the case for information placed by the confider on a bulletin board but what if the information was passed through an E-mail service and was "intercepted"?

The following comments of Megarry V-C in *Malone v Metropolitan Police Commissioner* were made in relation to eavesdropping of telephone conversations:

> "it seems to me that a person who utters confidential information must accept the risk of any unknown overhearing that is inherent in the circumstances of the communication."[4]

It does not take much imagination to see that these words may be equally applicable to E-mail over the Internet. However, some authors have rejected the notion that confidence in information is lost merely because there is a risk that 'eavesdropping' may occur[5]. The principle that the duty of confidence falls upon any person that receives the confidential information in circumstances where that person had reason to believe that the information was confidential should apply equally to circumstances where the confider did not expect the receiver to obtain the information.

Will the use of encryption programs for information transmitted over the Internet enhance the claim for confidentiality?

The issue of encryption of television broadcast was considered in *BBC Enterprises Ltd v HiTech Xtravision Ltd*[6]. In that case the BBC operated a satellite delivered television service for Western Europe (but not including the UK). Broadcasts were encrypted and could be viewed only by the use of a decoder. The decoders were available only through the BBC or its authorised distributors. Hi-Tech sold the decoders in Europe without the permission of the BBC. The BBC sought injunctions against Hi-Tech on the grounds that Hi-Tech was in breach of s298 of the UK *Copyright, Designs and Patents Act 1988*[7]. This issue was eventually the subject of appeals to the Court of Appeal[8] and the House of Lords[9].

Of immediate interest was the discussion, albeit briefly, by Scott J at first instance, of whether encryption attracts confidentiality. He said:

"If an author chooses to place a coded message in a public medium he cannot, in my judgment, complain if

members of the public decode his message. If the content, once decoded, does not qualify for protection on confidentiality grounds, the law of confidentiality is not, in my judgment, of any relevance."[10]

In this case, Scott J held the content of the programmes broadcast was not confidential in nature. If the information was of a confidential nature then surely encryption must be of relevance as it is evidence that the communication was imparted in circumstances importing an obligation of confidence.

Encryption programs are now readily available on the Internet[11]. It is submitted that the person who encrypts information may therefore be importing to the recipients that the information is considered to be of a confidential nature and that if it is received it should be treated as being confidential.

The improper conduct of 'cracking' an encryption code and the ease with which this may be done may be relevant to determine whether the confidentiality of the information may be maintained.

The comments of Megarry V-C may indicate that a person who transmits information over the Internet, even though that information has been encrypted, cannot complain if an unauthorised person decodes the information since that may be an inherent risk of the Internet. Does this argument have greater force where a 'weak' encryption program has been used?

But what of the 'unconscionable' behaviour of the 'hacker' who, without the authorisation of the confider, cracked the code? In *Franklin v Giddins*[12] the plaintiff had developed a novel strain of nectarine by grafting budwood to root stocks. The defendant (a trade competitor) trespassed on the plaintiff's land and stole the plaintiff's novel nectarine trees. Justice Dunn held it to be unconscionable for a person to obtain a benefit from stealing a trade secret. Should not the hacker be placed in the same shoes? There is a strong argument, morally and logically, that a wrongful acquisition of information should at least raise a presumption that the information is confidential.[13]

The evidence in *Franklin v Giddins* indicated that the plaintiff had done everything he reasonably could to protect from theft the variety of nectarine. This involved having general surveillance over fruit pickers and visitors. The fact that the plaintiff did not use guard dogs or an electric fence did not persuade Dunn J. to an alternative views as "people could normally be expected to respect the plaintiff's rights of property".[14]

Could it be said that a user of the Internet had not done everything he or she reasonably could to prevent the information from unauthorised disclosure if he or she used a 'weak' encryption program? There are now reports that 40 bit encryption programs can be easily decoded by programs that may cost no more than $400 and take no more than 5 hours.[15] United States Government authorities have acknowledged the weak nature of such 40 bit programs by proposing to approve the export of 64 bit encryption programs.[16] Does it matter that the confider does not have any 'rights of property' when transmitting on the Internet?

Yet the duty of confidentiality emanates from 'unconscionable conduct'. Nothing more should be required of a person communicating information than to take measures that would indicate to a recipient that the information was not for general perusal. Once that has been achieved the recipient must act conscientiously and the duty not to disclose without authorisation should apply. It is submitted that any form of reasonable encryption should be sufficient to impose upon the unauthorised recipient the duty not to disclose the information obtained by decoding the information.

Privacy legislation

Commonwealth Government agencies have for some time been subject to the *Privacy Act 1988* which adopts principles designed to secure personal information from unauthorised or improper use. The *Privacy Act* sets out eleven information privacy principles ('IPPs'). The *Privacy Act* is more concerned with the collection, handling and dissemination of records of personal information rather than the wider aspects of privacy such as telemarketing, surveillance or censorship.[17]

Furthermore, other than with respect to certain dealings with tax file numbers and credit information, the *Privacy Act* does not apply to the private sector. It now seems accepted that the Commonwealth Government has the constitutional power to amend the *Privacy Act* to extend it to the private sector by using its external affairs power.[18] Whether it chooses to do so remains to be seen[19] although it would be of no surprise if it did so given the Australian Privacy Council's Privacy Charter which is designed to promote a 'best practice' of principles for the private sector, and the apparent growing concern in Australia to protect an individual's privacy on the information super-highway.

The New Zealand *Privacy Act* 1993 does extend the Information Privacy Principles to the private sector.[20] It goes further by enabling the Privacy Commissioner to issue codes of practice to apply to non-public agencies.[21] A recent announcement by the NSW Attorney-General, Mr Shaw, indicates that a proposed new human rights and justice commission will have the power to develop codes of conduct in relation to privacy for the NSW private sector that may have the force of law as regulations under proposed new privacy legislation.[22]

What is the nature of the information which private sector organisations will be required to 'protect' if the

Privacy Act were to be extended?

'Personal Information' is defined to mean:

> "information or an opinion (including information forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".[23]

It is clear from the Explanatory Memoranda for the Privacy Bill 1986 that 'personal information' is intended to extend beyond merely names, addresses, dates of birth etc but may also include the nature of one's business, the financial position of one's business or even habits of an individual (such as brand preference, expenditure routines and the like). One commentator concludes that the concept of personal information "is likely to embrace any information about a natural person".[24]

In *Re Pfizer and Department of Health, Housing and Community Services*"[25] the AAT noted that "if the identity [of a person] is apparent or can be reasonably be ascertained from a *telephone number or other material*, then such material would fall within the section"[26] (emphasis added). Would this extend to a person's Internet address or domain name? There is no certainty that a person transmitting information from a domain is in fact the person believed to be rooted at the site. Is this any different from being able to confirm that the subscriber to a telephone number is not an imposter?

Perhaps the most pertinent IPP in the context of the Internet is that the record keeper is required to ensure that the record is protected by such security safeguards as is reasonable to take in the circumstances against loss, unauthorised use or disclosure, or misuse.[27]

What are "reasonable" safeguards? The principles of the law of negligence may be a guide. A reasonable person would assess the likelihood of risk of loss or disclosure and possible preventative measures including the expense of such measures.[28] As evidence of increased 'hacking' skills or greater sensitivity of the information being transmitted (such as credit card or bank account details) becomes more prevalent so the level of security would be expected to increase.

The Privacy Commissioner believes that Commonwealth agencies would be assisted in fulfilling their obligations under IPP 4 by complying with the Commonwealth Protective Security Manual ("PSM").[29] The PSM refers, among other things, to classification and sanitation of information, accreditation of systems, use of audit trails, security audits and non-use of privately owned computers.[30] The ramifications for an agency failing to fulfil its obligations under IPP 4, at this stage, may involve a declaration by the Privacy Commissioner that a person is entitled to an amount for compensation.[31] However, the House of Representatives Standing Committee on Legal Constitutional Affairs' Report into the Protection of Confidential Personal and Commercial Information recommended that the Privacy Act 1988 be amended to provide that an agency have strict liability for unauthorised disclosure of personal information and that an 'aggrieved' person be entitled to compensation.[32]

Private organisations (particularly under-resourced small businesses) may be faced with unforseen and perhaps significant impositions arising from the possibility of privacy provisions applying to the private sector in the future (either through Commonwealth or State legislation), strict liability compensation provisions, a broad view of "personal information" and the ingenuity of sophisticated 'cyberpunks'.

Liability of service providers

If 'privacy' concerns the ability of a person to decide what, when and how information is to be communicated to others, where does that leave the service provider? Should the service provider be held accountable for the disclosure of information through its service?

This vexed question has been considered in part by the Senate Select Committee on Community Standards Relevant to the Supply of Services Using Electronic Technologies in its report on the Regulation of Computer On-line Services (**"the Senate Committee"**)[33] and to a lesser extent by the Commonwealth Department of Communications and the Arts' Consultation Paper on the regulation of On-line Information Services.[34]

Both recommended that a self regulatory scheme be introduced for on-line services utilising codes of practice. Criminal offence provisions were suggested for the transmission of objectionable material but adherence to a Code of practice would be grounds for a defence to such a charge.

The Senate Committee was of the view that:

- "some effort" should be made by network operators to address the issue of the nature of content transmitted through their networks (although the Senate Committee did not elaborate on the nature of the provisions which it thought should be in the network provider's contracts)[35] and network operators should contribute 'some part of the revenue' that they earn towards the cost of operating any regulatory system.[36]
- with particular reference to the distribution of objectionable material to minors, Access Providers be required "to adopt whatever practical measures are available for ensuring the identification of clients, as an aid to future regulatory action".[37]
- an Information Service Provider be entitled to a defence to a charge of distributing objectionable material if it did not knowingly transmit the objectionable material or if it took steps in good faith to restrict access to that material.[38]

The Privacy Commissioner has stated:

> "Technical experts or those who make available new products and services should be obliged to explain fully the personal information management implications of new technologies. This should include detailed assessments of how particular applications generate, use and transmit personal information about individuals."[39]

The ironic twist is that the greater control or influence which the network and service providers have over the content of material transmitted on the Internet the more likely it may be that the Courts would hold them liable on other legal grounds. This would certainly seem to be the lesson from the United States case of *Stratton Oakmont v Prodigy Services Company*[40] at least in respect of defamation claims.

In the *Prodigy* case, Prodigy provided a bulletin board service known as "Money Talk". Statements appeared on this BBS which the plaintiff claimed was defamatory. Although Prodigy had no direct input concerning the content of the statement the Court held that Prodigy was a publisher of the statement and was therefore liable. In the Court's view Prodigy was liable as it sought to distinguish its service from its competitors by claiming that it screened material that would be placed on the BBS. It issued guidelines concerning permitted content and it engaged 'Board Leaders' to monitor incoming transmissions and to censor material in accordance with the guidelines. This case is in contrast to another U.S. case, *Cubby v CompuServe*[41], where CompuServe was held to be not liable as it had not undertaken any 'editorial' role in relation to material that was placed on its BBS.[42]

Similarly, would the law of negligence be invoked if a service provider takes upon itself a 'guardian angel' role but fails to meet an objective standard of what controls it was able to put in place but which it failed to apply? Is the service provider's relationship with subscribers or even users of sufficient proximity for the Court to find a duty of care was owed? Would adherence to an industry code of practice satisfy such a duty of care?

As Australian Courts have declined to find a common law right of privacy these issues may only be peripheral to protecting an individual's personal and confidential information. Nevertheless, these issues indicate that measures that may be taken to protect an individual's privacy may be achieved at the expense of imposing an additional legacy upon operators of the 'media' through which such an invasion may occur.

1 Australian Law Reform Commission, Privacy and Personal Information, Discussion Paper No 14, 1980
2 see Intellectual Property Law in Australia McKeough and Stewart, Butterworths, 1992, paras 307-308.
3 see *Coco v AN Clark Engineers* [106D] RPC 41
4 [1979] Ch 344, 376
5 See Meagher, Gummow and Lehane Equity Doctrines and Remedies 2nd Ed, Butterworths, para 4190 who state that "it requires no great effort, no straining of principle to restrain the activities of an eavesdropper"
6 (1989) 18 IPR 63.
7 Which prevents an unauthorised person from selling "a device designed or adapted to enable or to assist persons to receive programmes or other transmissions when they are not entitled to do so."
8 (1990) 20 IPR 367.
9 (1991) 21 IPR 461.
10 (1989) 18 IPR 63, 77.
11 Such as the Pretty Good Privacy Program developed by Phil Zimmerman.
12 [1978] Qd R 72.
13 See Lahore, Garnsey, Dwyer, Duffy and Covell, Patents, Designs and Trade Marks Law, Vol 1, Butterworths, para 3.7.120.
14 [1978] Qd R 72, 80.
15 Local Cyphos too Weak to Block Hackers, John Hilvert, The Australian, 20 February 1990, p20.
16 Electronic Privacy Information Centre, EPIC Alert, Vol 2.09 and 2.14, 9 November 1995.
17 Is there a tort of Privacy in Australia?, Maureen Tangney, Communications Law Bulletin, Vol 11, No 1, p38; Telemarketing and the Protection of the Privacy of Individuals, AUSTEL Privacy Advisory Committee, section 6..2.
18 Since Australia ratified the International Covenant Civil and Political Rights on 12 August 1980, Article 7 states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". See Telemarketing and the Protection of the Privacy of Individuals, AUSTEL Privacy Advisory Committee which noted that the Attorney-General's Department, the Australian Law Reform Commission and the Administrative Review Council all formed this view of the Commonwealth's constitutional powers.
19 The review of the Freedom of Information Act 1982 by the Administrative Review Council and the Australian Law Reform Commission also involves review of the issue of extending the Privacy Act to the private sector, see Duncan Kerr, the High Road to Security Policing the Info Superhighway, Australian Intellectual Property Law Bulletin, April 1995.
20 An 'agency' is defined as "any person or body of person, whether corporate or unincorporated and whether in the public sector or private sector".
21 s46.
22 Human rights watchdog gets teeth, Michael Sharp, Sydney Morning Herald, April 5, 1996.
23 section 6(1).
24 see P Bayne K Rubenstein, The Concept of "Information relating to Personal Affairs" and "Personal Information", Australian Journal of Administrative Law, Vol 1 No 4 1994 p226, 234.
25 (1993) 30 ALD 647.
26 ibid at 664.
27 IPP No 4(1) s.14 Privacy Act 1988.
28 Overseas Tankship (UK) Ltd v The Miller Steamship Co Pty Limited (1967) 1 AC 617 (Wagon Mound No 2).
29 Report House of Representatives Standing Committee on Legal and Constitutional Affairs, in Confidence, June 1995, para 3 11 1.
30 see Part VI, PSM, October 1990.
31 s52(1)(b)(iii) Privacy Act 1988.
32 In Confidence, ibid, para 8.8.6; this recommendation was also supported by the Privacy Commissioner and the Attorney-General's Department.
33 November 1995.
34 July 1995.
35 para 3.33.
36 para 3.34.
37 para 3.40.
38 para 3.50, *Recommendation* 6.
39 Kevin O'Connor, Privacy Commissioner, Privacy Law and Policy Reporter (1995) 2 PLPR 23.
40 Supreme Court, State of New York, 3 October 1995, Justice Ain, also available on the Internet at http://www.cpsr.org/cpsf/free_speech/so_v_prodigy_1995.txt.
41 for an Internet reference see ftp://ftp.eff.org/pub/CAF/law/cubby_v_compuserve.txt.
42 for a more detailed discussion of defamation and on-line information services see Legal Pitfalls in Cyberspace: Defamation on Computer Networks, Timothy Arnold-Moore, Journal of Law and Information Science, 5(2), 1994, pp165-209.

Paul McGinness (BA.LLB (Hons) (ANU), B.Ec (ANU)) is a Senior Associate in the Canberra office of Deacons Graham & James (formerly Sly & Weigall), Lawyers