Privacy Protection for Internet E-mail in Australia

Kent Davey
Australian Government Solicitor
(Part 2 of 3 parts)

L LB(Hons) B Sc LL M This article is based on a thesis submitted in partial fulfilment of the requirements of the degree of Master of Laws of the University of Melbourne. *The author would like to thank Associate Professor Mark Sneddon of the University for his comments on earlier drafts of the thesis.*

CHAPTER 4 — E-MAIL ENCRYPTION

Introduction

If e-mail messages are postcards then encryption envelopes may prevent them being read by anyone other than the intended recipient.[1] The OECD Cryptography Guidelines recognise that:

'[T]he fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.'[2]

There is no legislative constraint on the use of encryption in Australia. Anyone may encrypt e-mail in order to protect the privacy of its contents. However, encryption of e-mail will not absolutely ensure that its privacy will be protected and should not be seen as a substitute for providing legal protection for the privacy of e-mail.

The encryption of a message involves converting its contents into unintelligible text by substituting each symbol of the message for another symbol. The OECD Cryptography Guidelines define 'encryption' to mean 'the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.' If encryption works properly only the intended recipient will be able to decrypt the message by converting its contents back into the original format.[3]

The Sections of this Chapter address the following issues concerning the use of encryption to protect the privacy of Internet e-mail. Section A looks at the elements of secret key and public key encryption systems. Section B discusses the strength of encryption systems in view of the risks of keys being broken. Section C examines the implications of encryption for law enforcement agencies. Section D addresses the suggestion of the Broadband Services Expert Group ('BSEG') and the policy of the Federal Government in relation to the use of encryption to protect privacy.

A. Elements of Encryption Systems

The two elements of encryption are an algorithm and a key. An algorithm converts the plaintext of a message into cyphertext and the cyphertext back into the original plaintext. A key is a random string of binary digits that is used together with an algorithm when encrypting and decrypting messages.[4] The two main types of encryption systems in use today are secret key encryption ('SKE') and public key encryption ('PKE').[5]

1. *Secret Key Encryption Using a Single Key*

SKE is described as symmetric cryptography as a single key is used for both encrypting and decrypting messages.[6] This key is known as a secret key.[7] Examples of algorithms which work with a secret key include the Data Encryption Standard ('DES')[8] which uses a 56-bit key and the International Data Encryption Algorithm ('IDEA')[9] which uses a 128-bit key.

A significant difficulty with encrypting messages using SKE is that the secret key must be held by both the sender and recipient and has at some time to be sent by the party which created it to the other party.[10] The privacy of messages encrypted with either DES or IDEA to a certain degree lies in the ability of the sender and recipient of the message to keep the key secret.

2. *Public Key Encryption Using Public and Private Keys*

PKE is described as asymmetric cryptography as two different keys are used for encrypting and decrypting messages. The characteristics of the keys are such that one cannot be easily derived from the other. One key known as the public key is disclosed to the public. The other key known as the private key is held only by the owner of the key. Messages encrypted using the public key can only be decrypted by the holder of the private key and vice versa.[11] An example of an algorithm that works with both a private key and a public key is RSA.[12] The private and public keys of RSA are functions of a pair of large prime numbers usually between 384-bits and 1024-bits in length.[13]

Messages encrypted using PKE are considered to be more secure than e-mail encrypted using SKE as the private key need never be in the possession of anyone other than the owner of the key.[14] The privacy of a message encrypted with RSA to a certain degree lies in the ability of the owner of the private key to keep the key secret. The public keys of people wishing to receive messages must be readily available to be used for encrypting messages if PKE is to be effective.[15]

3. Pretty Good Privacy as the Defacto Standard for E-mail Security

The most popular program used to encrypt Internet e-mail is Pretty Good Privacy ('PGP') which relies on PKE.[16] It has become the defacto standard for e-mail security.[17] PGP uses IDEA for encrypting messages with a single 128-bit secret key. PGP then uses RSA with the recipient's public key to encrypt the 128-bit key itself.[18] Both the IDEA encrypted message and RSA encrypted 128-bit key are sent to the recipient. The recipient uses a copy of PGP with his or her private key to decrypt the RSA encrypted 128-bit key. PGP then uses the decrypted 128-bit key with IDEA to decrypt the message itself.[19]

B. The Strength of Encryption Systems

An encryption system may be weak or strong depending on whether or not there is a significant risk that the key may be broken by an organisation with access to sufficient computing power. The strength of SKE and PKE systems depends upon the key-length of keys used for encrypting and decrypting messages.[20] It is recommended that a minimum key-length of 90 bits be used with SKE systems and that keys with a key-length at least 10 times greater be used with PKE systems. DES uses a 56-bit key and is described as providing inadequate protection against a corporate or government attacker which is prepared to commit substantial resources.[21]

Keys used with some PKE systems which were thought to be unbreakable have been broken by using a technique which involves measuring how long a computer takes to decrypt messages. The time measurements provide clues about what is happening as the message is decoded. The technique is equivalent to guessing the combination of a lock by seeing how long it takes a person to turn the dials. The attack may be carried out in steps which involve guessing a private key bit by bit enabling errors to be easily detected. A hacker may simply correct the error and try again. By carrying out an attack in steps a hacker may break even the most complex private keys used with some PKE systems.[22]

Advances in computer technology are continually increasing the size of keys required to provide encrypted messages with adequate protection particularly against attacks by organisations which are willing to invest substantial amounts of time and money.[23] Even when using large keys there is always the possibility of some revolutionary mathematics discovery which may enable the cracking of encrypted messages thought to be unbreakable. It is said that every code devised by man may be broken.

C. The Implications of Encryption for Law Enforcement Agencies

In Australia and overseas law enforcement agencies consider interception to be an essential tool for law enforcement.[24] Australian law enforcement and national security agencies have not considered encryption to be a significant threat to interception in the past. The Australian Federal Police ('AFP') are optimistic that a solution to encryption will be available in a number of instances.[25]

The Telecommunications Act 1997 (Cth) ('Telecommunications Act') requires a carrier to ensure that it is possible to execute a warrant under the Telecommunications (Interception) Act 1979 (Cth) in relation to a telecommunications service supplied by means of a telecommunications network or facility operated by the carrier unless the Minister makes a written determination exempting the carrier from this requirement.[26] However, this requirement would not appear to extend to deciphering encrypted communications for law enforcement purposes.[27]

Under the Telecommunications Act the Minister may give a carrier written notice requiring that a telecommunications network or facility operated by it or a telecommunications service supplied by means of such a network or facility have a specified kind of interception capability which is to be provided on terms and conditions agreed between the carrier and the AFP, National Crime Authority, Australian Security Intelligence Organization or a declared eligible State authority.[28] The agreed terms and conditions may require the carrier to intercept and decrypt encrypted e-mail passing over the Internet.

The policy of the Federal Government for the regulation of on-line services addressed the issue of requiring the use of weak encryption systems for law enforcement purposes stating:

'[T]he onus is on security agencies to demonstrate that the benefits of mandating "crackable" codes... outweigh the social and economic consequences of the loss of personal privacy and commercial security that this would entail.'[29]

This has not yet been demonstrated by law enforcement or national security agencies. As a result there is currently no legislative restriction on the use of encryption in Australia.[30]

D. Suggestion of the Broadband Services Expert Group and Policy of the Federal Government in Relation to the Use of Encryption to Protect Privacy

Encryption has been suggested by the BSEG as a possible solution to the preservation of privacy in the communications environment.[31] In making this suggestion the BSEG noted that '[d]eveloping a culture of respect for privacy will be as important as technology in preserving privacy in the networked environment.'[32] The use of encryption by itself is unlikely to develop a culture of respect for the privacy of Internet e-mail.

In relation to the use of encryption to protect personal information for electronic commerce purposes the policy of the Federal Government states:

'Transactions will not be initiated unless people are confident that personal and financial information is protected from unauthorised interception. Heavy-handed attempts

to ban strong encryption techniques will compromise commercial security, discouraging online service industries (particularly in the financial sector) from adopting Australia as a domicile. This would result in a substantial economic loss to the country.'[33]

The use of encryption to provide privacy protection for Internet e-mail containing personal information would appear to be endorsed by the Federal Government at least in relation to electronic commerce.

In August 1996 the Federal Government established an Information Policy Advisory Council ('IPAC') to investigate and provide advice on social, technological and regulatory issues arising as a result of the rapid development of on-line services such as the Internet.[34] IPAC has the task of providing options for the implementation of open encryption standards which meet commercial needs.[35] However, commercial needs do not necessarily equate with privacy needs.

Conclusion

The privacy of encrypted Internet e-mail depends upon the strength of the encryption system used to encrypt the message and the ability of the sender and recipient to keep the key secret when using SKE and the ability of the owner of the private key to keep it secret when using PKE. Although the keys used to encrypt e-mail with some PKE systems were considered to be unbreakable, some of these keys have been broken. Additionally, encryption will not protect e-mail which is stored in the mailbox of a user in an unencrypted form.

It is unsatisfactory for the privacy of encrypted Internet e-mail to depend largely upon the key used for decryption remaining secret and the message not falling into the hands of a person who is able to break the decryption key and crack the message. The use of encryption alone would not assist in the development of a culture of respect for the privacy of e-mail which has been recognised as being as important as technology in protecting privacy in the communications environment. Encryption should not be seen as a substitute for providing legal protection for the privacy of e-mail.

1 Bruce Schneier, *E-Mail Security* (1995) 5-6.
2 Organisation for Economic Co-operation and Development Guidelines for Cryptography Policy (1997) ('OECD Cryptography Guidelines'). The Guidelines were adopted by the OECD on 27 March 1997. Available at http://www.oecd.org/dsti/iccp/
3 Larry J Hughes, *Internet Security Techniques* (1995) 42.
4 Schneier, above n 1, 17-8.
5 Hughes, above n 3, 47.
6 Roger Clarke, 'Cryptography issues in plain text' (1996) 3(2) *Privacy Law & Policy Reporter* 24, 24-5.
7 Hughes, above n 3, 47.
8 Bruce Schneier, *Applied Cryptography* (1994) 224.
9 Ibid 261.
10 Clarke, above n 6, 25.
11 Hughes, above n 3, 48.
12 The algorithm RSA was named after its three inventors who were Ron Rivest, Adi Shamir and Leonard Adleman: Schneier, above n 8, 282.
13 Schneier, above n 8, 284.
14 Clarke, above n 6, 25.
15 Graham Greenleaf, 'OECD searches for crypto-consensus' (1996) 3(2) *Privacy Law & Policy Reporter* 21, 23.
16 Another popular program is Riordan's Internet Privacy-Enhanced Mail which implements the Privacy Enhanced Mail standard for exchanging e-mail: Schneier, above n 8, 435.
17 Hughes, above n 3, 156.
18 RSA is not used for encrypting the message as it would take approximately 100 times longer than IDEA: Hughes, above n 3, 60-1.
19 Schneier, above n 1, 135-42.
20 Clarke, above n 6, 24.
21 Matt Blaze and Others, *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*, January 1996. Available at http://www.bsa.org/policy/encryption/
22 The Times, 'Hacker breaks secret of public key encryption', *The Australian*, 2 April 1996.
23 Blaze and Others, above n 21.
24 P J Barrett, *Review of the Long Term Cost Effectiveness of Telecommunications Interception*, 1 March 1994, 29.
25 Ibid 44.
26 Telecommunications Act ss 319, 320. Item 10 of the Telecommunications Legislation Amendment Bill 1997 will repeal Part 15 of the Telecommunications Act and substitute a new Part 15 which applies new arrangements to procedures for establishing an interception capability for telecommunications services in Australia and the funding of this interception capability. Under the new Part 15 the Federal Attorney-General will be able to determine a new level of interception capability based upon a relevant international standard or guideline.
27 Barrett, above n 24, 43.
28 Telecommunications Act ss 322, 323(1), 326, 328; Telecommunications (Interception) Act 1979 (Cth) s 5 - see definition of 'agency'. The eligible State authorities which have been declared are the Victorian Police, New South Wales Police, New South Wales Crime Commission, New South Wales Independent Commission Against Corruption and South Australian Police. Other authorities may also obtain access to intercepted communications when they are involved in a joint operation with one of these authorities: Australian Telecommunications Authority, *Telecommunications and Law Enforcement*, June 1995, 6-7.
29 Federal Government, *Australia Online*, February 1996, 16 ('*Australia Online*').
30 Barrett, above n 24, 44. However, Regulation 13B of the Customs (Prohibited Exports) Regulations 1901 (Cth) requires permission in writing or a licence from the Minister to export specified cryptographic equipment and software.
31 Broadband Services Expert Group, *Networking Australia's Future*, December 1994, 67.
32 Ibid.
33 *Australia Online* 15. See also Gerard Walsh, *Review of Policy relating to Encryption Technologies*, 10 October 1996. Available at http://www.efa.org.au/Issues/Crypto/Walsh/
34 Department of Communications and the Arts, *Press Release*, 23 August 1996.
35 *Australia Online* 15. IPAC was formerly known as the Information Policy Task Force.

CHAPTER 5 — E-MAIL AND THE BREACH OF CONFIDENCE DOCTRINE

Introduction

Almost any information which is confidential may be protected by the breach of confidence doctrine.[1] The fact that information contained in e-mail may only exist in electronic form would not appear to preclude protection being given to it. The doctrine affords protection to both the tangible and the intangible.[2]

The breach of confidence doctrine provides only incidental protection for privacy interests as it does not protect privacy per se. A person may seek to rely upon the action for breach of confidence to prevent a person snooping on the Internet using or disclosing the contents of e-mail messages. However, e-mail containing confidential personal information will only be protected by the action in certain circumstances.[3]

The Sections of this Chapter look at the following issues relating to the extent to which the breach of confidence doctrine may be relied upon to protect the privacy of Internet e-mail. Section A discusses the elements of the action for breach of confidence. Section B looks at the circumstances in which confidential information may be disclosed in the public interest without breaching an obligation of confidence. Section C examines the relationship between

the breach of confidence doctrine and decryption of encrypted information.

A. Elements of the Action

Three elements are generally required for information to be protected by the breach of confidence doctrine. First, the information must have the necessary quality of confidence about it. Secondly, it must generally have been imparted in circumstances which expressly or by implication create an obligation of confidence. Thirdly, there must be an actual or threatened unauthorised use or disclosure of the information.[4]

1. *Information Must Have the Necessary Quality of Confidence to be Confidential*

Information will not be protected by the breach of confidence doctrine unless the information is confidential in the sense that it has 'the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge'.[5] It has been suggested that information must possess a quality of 'inaccessibility' before it will be protected.[6] Whether information contained in e-mail may have the necessary quality of confidence will depend upon how courts interpret the accessibility of e-mail passing over the Internet.

E-mail has been described as the 'world of postcards' in that messages pass over the Internet open and available to be read by anyone in the same way that postcards travel through the postal mail.[7] As a result e-mail may be considered to be too accessible for any personal information which it contains to have the necessary quality of confidence. However, e-mail encrypted using a strong encryption system is likely to be sufficiently inaccessible for information which it contains to have the necessary quality of confidence.

2. *An Obligation of Confidence Arises From the Circumstances in Which Information is Imparted*

Information which is confidential will be protected by the action for breach of confidence if it is disclosed in circumstances which expressly or by implication create an obligation of confidence. At the time of disclosure the recipient of the information should understand that the information is being received by him or her for a specific and limited purpose.[8] However, the protection of privacy requires that personal information be protected whether or not it has been disclosed in circumstances in which an obligation of confidence arises.

An obligation of confidence may arise as a result of an express or implied confidentiality term in a contract between the sender of e-mail and the carrier or service provider supplying the Internet e-mail service. Alternatively, an obligation of confidence may expressly arise by reason of the sender of e-mail including a confidentiality statement in the message. An example of a such a statement is as follows:

'This e-mail message contains confidential information and is intended only for the addressee. If you are not the intended recipient then any use or disclosure of the contents of this message is strictly prohibited.'

An obligation of confidence will arise by implication if the circumstances are such that any reasonable person standing in the shoes of the recipient would have realised upon reasonable grounds that e-mail containing confidential information was received by him or her in confidence.[9]

It has been suggested that if information is confidential in nature then encryption of the information using any form of reasonable encryption would be evidence that the information was imparted in circumstances importing an obligation of confidence.[10] The stronger the encryption system used to encrypt e-mail containing confidential information the more likely it is that an obligation of confidence will arise in circumstances where a person obtains the information by snooping on the Internet.

(a) *An Obligation of Confidence May Arise Where Information is Improperly or Surreptitiously Obtained*

Where confidential information is improperly or surreptitiously obtained an obligation of confidence may arise even though the information has not been communicated in confidence. A person snooping on e-mail passing over the Internet obtains information by improper or surreptitious means. Equity will restrain the publication of confidential information improperly or surreptitiously obtained if it should not be divulged.[11] However, courts in the United Kingdom and Australia have formulated different rationales for the intervention of equity in these circumstances.

(i) *Approach of Courts in the United Kingdom to the Protection of Information Improperly or Surreptitiously Obtained*

The improper or surreptitious acquisition of information has been considered in the United Kingdom in the cases of *Malone v Metropolitan Police Commissioner*[12] and *Francome v Mirror Group Newspapers*.[13] In *Malone* the police lawfully had a tap placed on the plaintiff's telephone line. The plaintiff sought to restrain the use of the information obtained by the police by arguing that its use would be a breach of confidence. In rejecting the plaintiff's argument Megarry V-C expressed the view:

'It seems to me that a person who utters confidential information must accept the risk of any unknown hearing that is inherent in the circumstances of communication..... When this is applied to telephone conversations, it appears to me that the speaker is taking such risks of being overheard as are inherent in the system..... In addition, so much publicity in recent years has been given to instances (real or fictional) of the deliberate tapping of telephones that it is difficult to envisage telephone users who are genuinely unaware of this possibility.'[14]

In accordance with the approach taken by Megarry V-C users of Internet e-mail would be required to accept the risk of a person snooping on the contents of their messages particularly given the fact that it is widely acknowledged that the Internet is not a secure communications medium.[15]

However, this approach whereby information will no longer be confidential in circumstances where there is a risk of snooping should be rejected on the basis that equity responds to unconscionable conduct which need not relate to any consensual dealing.[16]

In *Francome* the plaintiff sought to restrain the publication of information obtained by the unlawful tapping of his telephone conversations on the basis that it would be a breach of confidence. The Court of Appeal granted an injunction against publication of the information. The case of *Malone* was distinguished by Fox LJ on the basis that Megarry V-C had expressly stated that his decision was limited to circumstances involving the lawful tapping of a telephone.[17] In distinguishing *Malone* Fox LJ stated:

'Illegal tapping by private persons is quite another matter, since it must be questionable whether the user of a telephone can be regarded as accepting the risk of that in the same way as, for example, he accepts the risk that his conversation may be overheard in consequence of the accidents and imperfections of the telephone system itself.'[18]

The decision of the Court of Appeal in *Francome* indicates that the breach of confidence doctrine may be relied upon in the United Kingdom to protect confidential information improperly or surreptitiously obtained by a person unlawfully in circumstances where the information has not been communicated in confidence.[19]

(ii) Approach of Australian Courts to the Protection of Information Improperly or Surreptitiously Obtained

In Australia the confidentiality of information improperly or surreptitiously obtained has been considered by the Queensland Supreme Court in *Franklin v Giddins*.[20] The defendant stole budwood from the plaintiff's orchard and used the budwood to propagate a special variety of nectarine known as the 'Franklin Early White' in competition with the plaintiff. He argued that the budwood was not 'information confidentially imparted'.

In *Franklin* Dunn J held that the stolen budwood was a trade secret and that the defendant had breached an equitable obligation of confidence owed to the plaintiff by using the stolen budwood. In Dunn J's view the actions of the defendant were unconscionable because he used his wrongful conduct to better his position:

'I find myself quite unable to accept that a thief who steals a trade secret, knowing it to be a trade secret, with the intention of using it in commercial competition with its owner, to the detriment of the latter, and so uses it is less unconscionable than a traitorous servant.'[21]

Dunn J relied upon unconscionability as the basis for holding that the defendant had breached an obligation of confidence owed to the plaintiff. Courts have not sought to define unconscionability as whether conduct is unconscionable will depend upon the circumstances in the particular situation. Conduct will be deemed to be unconscionable where it can be seen in accordance with the ordinary concepts of mankind to be so unfair and against conscience that a court should intervene.[22]

According to Dunn J an obligation of confidence may arise in relation to confidential information which has been improperly or surreptitiously obtained in circumstances where it has not been communicated in confidence.[23] However, the approach taken by Dunn J seems unnecessarily broad as he could have identified more clearly the circumstances in which the use or disclosure of confidential information improperly or surreptitiously obtained will breach an obligation of confidence.[24]

The fact that an obligation of confidence may arise where confidential information is improperly or surreptitiously obtained without being communicated in confidence is supported by a later statement in *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* by Deane J:

'[T]he equitable jurisdiction to grant relief against an actual or threatened abuse of confidential information.... lies in an obligation of confidence arising from the circumstances in or through which the information was communicated or obtained.'[25]

In Australia an obligation of confidence may arise in circumstances where the use or disclosure of confidential information improperly or surreptitiously obtained by a person snooping on Internet e-mail would be unconscionable. However, if Australian courts follow the approach taken by courts in the United Kingdom the action for breach of confidence may only be relied upon to protect such information where it is acquired in unlawful circumstances.

3. *An Actual or Threatened Unauthorised Use or Disclosure of Confidential Information*

An obligation of confidence will not be breached unless it is established that there was an actual or threatened unauthorised use or disclosure of confidential information for a purpose other than that for which it was disclosed. The fact that a person may not intend to breach an obligation of confidence is irrelevant as liability is strict.[26] Liability may be imposed even in circumstances where a person uses or discloses confidential information in error[27] or subconsciously.[28]

It is uncertain whether a person would have to establish that use or disclosure of confidential information would cause detriment or prejudice to succeed in an action for breach of confidence. The authorities are unclear in relation to whether detriment or prejudice is required.[29] It may be arguable that detriment in the form of mental distress would be caused to a person where he or she becomes aware that another person has snooped on e-mail containing his or her personal information.

In *Fractionated Cane Technology Ltd v Joseph Ruiz-Avila* McPherson J suggested that the presence of detriment is not necessary for a person to be able to rely upon the breach of confidence action:

'In most if not all the reported cases,

the information has been used or threatened to be used for a purpose that was in fact detrimental. That should not, however, be permitted to obscure the fact that it is, broadly speaking, the misuse or misappropriation of the information that evokes the intervention of equity.'[30]

The requirement that information be misused or misappropriated for it to be protected may mean that persons snooping on e-mail containing confidential information only for the purpose of viewing the message without any intention of otherwise using or appropriating it will not breach any obligation of confidence. There appears to be no authority which has held that the mere viewing of confidential information constitutes a misuse or misappropriation of it.[31]

B. Disclosure of Confidential Information in the Public Interest

Liability for breach of confidence will not be imposed where a person has 'just cause of excuse' for disclosing confidential information.[32] However, the disclosure of the information must be 'in the public interest'.[33] The application of the public interest test involves a weighing of public interests which change over time according to the circumstances of each particular situation.

The disclosure of information in the public interest has been considered by the High Court in *Commonwealth v John Fairfax & Sons Ltd.*[34] Mason J stated:

'It makes legitimate the publication of confidential information ... so as to protect the community from destruction, damage or harm. It has been acknowledged that the defence applies to disclosures of things done in breach of national security, in breach of the law (including fraud) and to disclosure of matters which involve dangers to the public.'[35]

The disclosure of confidential information will not be prevented in circumstances where the public interest in disclosure of the information outweighs the public interest in confidentiality.[36] However, in balancing these public interests sufficient weight may not be given to privacy interests which are traditionally seen as private interests.

A distinction must be drawn between information the disclosure of which is 'in the public interest' and information which is only 'of public interest'.[37] The disclosure of confidential information would be justified in circumstances where the disclosure is in the public interest but not where the disclosure is merely of public interest. Additionally, the disclosure must be to the 'proper authorities' for it to be in the public interest.[38]

C. Breach of Confidence and the Decryption of Encrypted E-mail

In the United Kingdom the relationship between the breach of confidence doctrine and decryption of encrypted information has been considered in *BBC Enterprises Ltd v Hi-Tech Xtravision Ltd.*[39] The plaintiff operated a satellite television service for Western Europe excluding the United Kingdom. The satellite signals were encrypted and could only be viewed using a decoder available from the plaintiff or an authorised distributor. The plaintiff sought an injunction to prohibit the defendant from selling the decoders without the plaintiff's permission relying upon confidentiality among other grounds.

At first instance in *BBC Enterprises* Scott J held that the television programs broadcast were not confidential in nature. In considering the application of the law of confidentiality to the encrypted broadcasts Scott J stated:

'The broadcasts are encrypted, but it is possible for Hi-Tech, and no doubt others, to decode the encryption. To do so is, in my judgment, no more a breach of confidence than it would be to decode a coded message placed in the columns of *The Times*. 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.'[40]

The judgment of Scott J indicates that anyone may decrypt information which is placed in a public medium without breaching an obligation of confidence. Although the Internet may be regarded as a public medium in the sense that any member of the public may obtain access to it, e-mail sent over the Internet is not distributed as widely as satellite television signals. The comments of Scott J would not be applicable to the decryption of e-mail sent over the Internet which is not as widely distributed.

Conclusion

The privacy protection afforded to Internet e-mail containing personal information by the breach of confidence doctrine is inadequate and uncertain. The Australian Law Reform Commission similarly concluded that the doctrine provides inadequate protection for invasions of privacy interests.[41] The action for breach of confidence may only be relied upon to protect confidential information which has been communicated or obtained in circumstances in which an obligation of confidence arises. Personal information acquired by a person snooping on Internet e-mail would not be protected if it is not confidential or obtained in such circumstances.

E-mail sent over the Internet may be considered to be too accessible to have the necessary quality of confidence for it to be protected by the breach of confidence doctrine. Where a person surreptitiously or improperly obtains personal information by snooping on the Internet an obligation of confidence may not arise in Australia unless an actual or threatened use or disclosure of the information is unconscionable. The mere viewing of e-mail containing personal information may not be sufficiently detrimental for a person to succeed in an action for breach of confidence. Additionally, the exception which permits the disclosure of confidential

information in the public interest may not give sufficient weight to privacy interests when balancing the public interests in disclosure and confidentiality.

1 Jill McKeough and Andrew Stewart, *Intellectual Property In Australia* (1991) 48; Staniforth Ricketson, *The Law of Intellectual Property* (1984) 815.
2 *Seager v Copydex* [1967] 2 All ER 415 (*'Seager'*); *Talbot v General Television Corp Ltd* [1980] VR 224 (*'Talbot'*). See also Gordon Hughes, *Data Protection in Australia* (1991) 203.
3 *Foster v Mountford* (1976) 29 FLR 233; *Stephens v Avery* [1988] 2 WLR 1280; *Argyll v Argyll* [1967] Ch 302.
4 *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, 47 (Megarry J) (*'Coco'*).
5 *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) 65 RPC 203, 215 (Lord Greene MR).
6 Francis Gurry, *Breach of Confidence* (1984) 70.
7 Bruce Schneier, *E-Mail Security* (1995) 3.
8 McKeough and Stewart, above n 1, 63.
9 *Coco* [1969] RPC 41, 48 (Megarry J).
10 Paul McGinness, 'The Internet and privacy - some issues facing the private sector' (1996) 29 *Journal for the Australian and New Zealand Societies for Computers and the Law* 25, 26.
11 *Lord Ashton v Pape* [1913] 2 Ch 469, 475 (Swinfen Eady LJ); *Commonwealth of Australia v John Fairfax and Sons Ltd* (1980) 147 CLR 39, 50 (Mason J) (*'John Fairfax & Sons'*); *Deputy Commissioner of Taxation v Rettke* (1995) 31 ATR 59, 63 (Cooper J).
12 [1979] 1 Ch 344 (*'Malone'*).
13 [1984] 2 All ER 408 (*'Francome'*).
14 *Malone* [1979] 1 Ch 344, 376.
15 Stephen Withers, Geoff Ebbs and Jeremy Horey, *The Australian Internet Book* (2nd ed 1995) 166; Ed Krol and Paula Ferguson, *The Whole Internet* (1996) 66.
16 Meagher, Gummow and Lehane, *Equity Doctrines and Remedies* (3rd ed 1992) 871-2.
17 *Francome* [1984] 2 All ER 408, 414-5.
18 Ibid 415.
19 Megan Richardson, 'Breach of Confidence, Surreptitiously or Accidentally Obtained Information and Privacy: Theory Versus Law' (1994) 19 *Melbourne University Law Review* 673, 694.
20 [1978] Qd R 72 (*'Franklin'*).
21 Ibid 80.
22 *Zoneff v Elcom Credit Union Ltd* (1990) 94 ALR 445, 463 (Hill J).
23 Ricketson, above n 1, 828.
24 Gurry, above n 6, 165.
25 (1984) 156 CLR 414, 437–8 (*'Moorgate Tobacco'*).
26 Hughes, above n 2, 209.
27 *Interfirm Comparison (Aust) Pty Ltd v Law Society of New South Wales* [1975] 2 NSWLR 104.
28 *Talbot* [1980] VR 224; *Seager* [1967] 2 All ER 415.
29 *John Fairfax & Sons* (1980) 147 CLR 39, 51 (Mason J); cf *Moorgate Tobacco* (1984) 156 CLR 414, 438 (Deane J).
30 (1987) 8 IPR 502, 514.
31 Hughes, above n 2, 210.
32 *Fraser v Evans* [1969] 1 QB 349, 362 (Lord Denning MR).
33 *Initial Services Ltd v Putterill* [1968] 1 QB 396, 405 (Lord Denning MR) (*'Initial Services'*).
34 (1980) 147 CLR 39.
35 Ibid 57.
36 Ibid 52.
37 *British Steel Corporation v Granada Television Ltd* [1981] AC 1096, 1168 (Lord Wilberforce).
38 *Initial Services* [1968] 1 QB 396, 405–6 (Lord Denning MR); *Attorney-General for the United Kingdom v Heinemann Publishers Australia Pty Ltd* (1987) 8 NSWLR 341, 380-1 (Powell J).
39 (1989) 18 IPR 63 (*'BBC Enterprises'*).
40 Ibid 77.
41 Australian Law Reform Commission, Report No 22, *Privacy* (1983) Vol 1 para 70.

CHAPTER 6 — PRIVACY PROTECTION FOR E-MAIL UNDER THE TELECOMMUNICATIONS INDUSTRY OMBUDSMAN SCHEME

Introduction

Carriers and some service providers are indirectly required to comply with the Information Privacy Principles ('IPPs') contained in the Privacy Act 1988 (Cth) ('Privacy Act') through their participation in the Telecommunications Industry Ombudsman ('TIO') scheme. The IPPs contained in the Privacy Act only apply directly to Commonwealth agencies in the public sector. The IPPs protect the privacy of individuals by providing protection for their personal information.

The Privacy Act has been criticised on the basis of its limited jurisdictional scope.[1] In response to these criticisms the Federal Government proposed a co-regulatory approach for extending privacy protection to the private sector. Earlier this year the Government decided to abandoned its proposed co-regulatory approach in favour of industry self-regulation under voluntary codes of practice to reduce 'business red tape'.[2] In announcing its decision to abandon the co-regulatory approach the Government recommended that the States not implement privacy and data protection legislation due to concerns about the 'regulatory burden'. However, Victoria and New South Wales are still considering the introduction of such legislation.[3]

The sections of this Chapter cover the following areas relating to the protection provided for Internet e-mail by the indirect requirement under the TIO scheme for participating carriers and service providers to comply with the IPPs contained in the Privacy Act. Section A discusses what constitutes personal information. Section B considers the indirect application of the IPPs to carriers and service providers under the TIO scheme. Section C outlines the co-regulatory approach proposed by the Federal Government and considers the implications of the Government's decision earlier this year to abandon this approach.

A. Personal Information is Information About an Individual

The collection, storage and security, individual access and correction, use, and disclosure of personal information is regulated by the IPPs contained in the Privacy Act. 'Personal information' is defined in the Act to mean:

'[I]nformation or an opinion (including information or an opinion 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'.[4]

The Act defines an 'individual' to mean 'a natural person'.[5] E-mail will contain 'personal information' for the purposes of the Act where it contains information about a person whose identity is apparent or can reasonably be ascertained from the information.

It has been suggested that information about a person relates to his or her 'personal affairs' if it 'affects the person as an individual whether it is known to other persons or not.'[6] The view has been expressed that the name and telephone number of a person could not constitute 'information relating to the personal affairs' of that person.[7] Although the concept of 'personal information' is wider than 'personal affairs', it is doubtful that an individual's e-mail address by itself would constitute 'personal information'.

Although an individual's e-mail address may not by itself constitute 'personal information', it may still identify the sender and recipient of a message in circumstances where their identities are not apparent from the contents of the message. The e-mail

addresses of the sender and recipient are included in the header of a message unless the message is sent to an anonymous remailer which provides anonymity by stripping some of this information from the header.[8] It is a question of fact whether the identities of the sender and recipient of e-mail can reasonably be ascertained from their e-mail addresses.[9]

In *Re Pfizer Pty Ltd v Department of Health, Housing and Community Services*[10] the Administrative Appeals Tribunal ('AAT') considered whether the identity of an individual is apparent or could reasonably be ascertained from a telephone number for the purpose of applying the exemption under the Freedom of Information Act 1982 (Cth) ('FOI Act') relating to the unreasonable disclosure of personal information about any person.[11] The FOI Act and the Privacy Act contain identical definitions of 'personal information'.[12]

The applicant in *Re Pfizer* applied to the AAT for the review of a decision by the Department of Health, Housing and Community Services ('DHHCS') to deny the applicant access to documents concerning a certain drug. The documents contained the telephone numbers of individuals involved in the drug regulation process. The AAT held that the telephone numbers contained in the documents had to be deleted before the documents could be released under the FOI Act as the numbers could identify individuals involved in the drug regulation process. A person's identity is just as likely to be disclosed by his or her e-mail address as by his or her telephone number. Where the use of an e-mail account is password protected then an e-mail address is more likely to reveal the person's identity.

E-mail will contain personal information where it contains information about the sender or recipient which affects him or her as an individual. The identities of the sender and recipient of e-mail are likely to be apparent from the contents of the message or reasonably ascertainable from their e-mail addresses which are included in the header of the message. E-mail may also contain personal information about a person other than the sender or recipient of the message where the identity of that other person is apparent or reasonably ascertainable from the contents of the message.

B. Application of the Information Privacy Principles to Carriers and Service Providers

The eleven IPPs contained in the Privacy Act only apply directly to Commonwealth agencies.[13] This is a significant limitation on the privacy protection afforded to e-mail under the Act.[14] However, the Privacy Commissioner has the function of encouraging corporations to develop programs for the handling of records of personal information that are consistent with the OECD Data Protection Guidelines.[15]

Carriers and service providers are not directly required to comply with the IPPs as they are not 'Commonwealth agencies' for the purposes of the Privacy Act.[16] However, carriers and service providers participating in the TIO scheme are indirectly required to comply with the IPPs. The Telecommunications Act 1997 (Cth) ('Telecommunications Act') requires all carriers and service providers which supply Internet access services to enter into the TIO scheme.[17]

Under the TIO scheme a user may make a complaint to the TIO if he or she believes that a carrier or service provider which is participating in the scheme is interfering with his or her privacy by not complying with the IPPs or any applicable industry specific standard.[18] Carriers and service providers may interfere with the privacy of a user where they snoop on his or her Internet e-mail in contravention of the IPPs.

The TIO may resolve a complaint under the TIO scheme by making a determination that a carrier or service provider pay up to $10,000 compensation to a complainant or by directing the carrier or service provider to remedy the situation.[19] All decisions made by the TIO are binding on carriers and service providers participating in the scheme.[20]

The IPPs relevant to snooping on Internet e-mail concern the collection, storage and security, use and disclosure of personal information.

1. Collection Principle

In order to comply with IPP 1 carriers and service providers should not collect personal information for inclusion in a record or generally available publication unless:

(a) the collection of the information is necessary for a lawful purpose directly related to their functions or activities; and

(b) the information is collected by lawful and fair means.

'Collection' is not defined in the Privacy Act. The Macquarie Dictionary (2nd edition) defines 'collect' to mean 'to gather together; assemble'.

Carriers and service providers will not have to comply with IPP 1 unless they collect personal information for inclusion in a record or generally available publication.[21] A 'record' is defined in the Privacy Act to include a document and database (however kept) but does not include 'articles in the course of transmission by post'.[22] The Acts Interpretation Act 1901 (Cth) widely defines a 'document' to include 'any article or material from which sounds, images or writings are capable of being reproduced'.[23] E-mail stored on a computer would be a 'record' for the purposes of the Privacy Act. However, it is unclear whether e-mail passing over the Internet would be a record for the purposes of the Act as it may be considered to be an article 'in the course of transmission by post'. The application of the IPPs should be clarified so that it is clear that they apply to e-mail passing over the Internet.

The lawful purposes for which a carrier or service provider may collect personal information under IPP 1 will depend upon the scope of its functions and activities. The scope of the functions and activities of a Commonwealth agency is limited by the legislation under which the agency is established. However, the

scope of the functions and activities of carriers and service providers may be very wide being limited only by the functions and activities which they choose to undertake.

Personal information should only be collected under IPP 1 where necessary for a lawful purpose in the public interest. This would involve weighing privacy interests against public interests. The collection of personal information for any lawful purpose may unreasonably intrude upon the privacy of the individual concerned unless privacy interests are outweighed to a substantial degree by public interests in collecting the information.[24] The balancing of privacy interests against public interests has been considered in Chapter 3. The collection of personal information by snooping may not be considered to be a fair means of collecting such information.[25]

IPPs 2 and 3 also concern the collection of personal information. However, IPPs 2 and 3 only apply where personal information is solicited by the collector and are not applicable to the collection of personal information by snooping as personal information is not solicited in these circumstances.

2. *Storage and Security Principle*

Pursuant to IPP 4 carriers and service providers which have possession or control of a record which contains personal information must ensure that it is protected by reasonable security safeguards against loss, unauthorised access, use, modification or disclosure and other misuse. Carriers and service providers would have possession or control of a record of e-mail which is stored on a computer operated by the carrier or service provider. The reasonable security safeguards which carriers and service providers may use to protect e-mail include password protection, secure networks and encryption where appropriate. The appropriateness of providing security safeguards has been considered in Chapter 3.

3. *Use and Disclosure Principles*

In accordance with IPPs 10 and 11 respectively carriers and service providers which have possession or control of a record which contains personal information must not use the information for a purpose other than that for which it was obtained or disclose the information unless:

(a) the individual concerned consents;

(b) necessary to prevent a serious and imminent threat to the life or health of any person;

(c) for a purpose required or authorised by law; or

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

Under IPP 10 carriers and service providers may also use personal information for a purpose directly related to the purpose for which the information was obtained.

Personal information may also be disclosed by carriers and service providers under IPP 11 where the individual concerned is reasonably likely to have been aware that information of that kind is usually disclosed to another person. This exception should be deleted as it permits unreasonable intrusions upon the privacy of individuals. If the disclosure is not covered by another exception then the consent of the individual concerned should be required to be obtained in the circumstances.

In order to comply with IPP 9 carriers and service providers which have possession or control of a record containing personal information must only use it for relevant purposes. Although the relationship between IPPs 9 and 10 is unclear, the better view would seem to be that IPP 9 is subject to IPP 10 as IPP 10 is more specific.

A limitation on the privacy protection afforded to personal information by IPP 10 is that it only restricts the use of such information where the information is obtained for a particular purpose. Where personal information is not obtained for a particular purpose IPP 10 would not be applicable. The uses which carriers and service providers may make of personal information which they may not have obtained for a particular purpose should similarly be restricted to ensure that its privacy is properly protected.

A person to whom personal information is disclosed by a Commonwealth agency under an exception contained in IPP 11 may not use or disclose the information for a purpose other than the purpose for which it was disclosed. A similar restriction should apply to persons to whom a carrier or service provider discloses personal information under an exception.

The former Privacy Commissioner criticised IPPs 10 and 11 on the basis that they 'set a weak minimum standard for confidentiality which is largely inadequate.'[26] He considered that the language of IPPs 10 and 11 was 'too vague and loose' which resulted in conflicting interpretations of the provisions.[27] The use and disclosure of personal information for a purpose required or authorised by law under IPPs 10 and 11 may be broadly interpreted to allow any lawful action by a carrier or service provider.[28] Any disclosure or use of personal information by a service provider or an employee of a carrier or service provider under an exception contained in the Telecommunications Act would be authorised by law.[29] The uses and disclosures which service providers and employees may make of communications information relating to a person's affairs under the Telecommunications Act is considered in Chapter 8.

It has been recommended that the exceptions contained in IPPs 10 and 11 should be made more specific.[30] IPPs 10 and 11 may be made more specific by requiring that personal information may only be used or disclosed for a lawful purpose in the public interest. This requirement would involve weighing privacy interests against public interests which has been considered in Chapter 3. The laws enforcement of which would justify the use or disclosure of personal information under IPPs 10 and 11 should be clearly

identified. It has been suggested that the expression 'protection of the public revenue' should also be clarified.[31]

4. *Additional Principles to be Included in the IPPs*

A principle needs to be included in the IPPs which requires that only the minimum amount of personal information should be collected for a lawful purpose. The collection of only the minimum amount of personal information necessary accords with the Collection Limitation Principle contained in the Australian Privacy Charter ('APC').[32] The collection of more personal information than necessary unreasonably intrudes upon the personal affairs of the individual concerned as personal information would then be stored unnecessarily. Although IPP 3 requires that the collection of personal information should not intrude to an unreasonable extent upon the affairs of the individual concerned, it would not be applicable to the collection of personal information by snooping as the information is not solicited in these circumstances.

The IPPs should also include a principle which requires that personal information be destroyed after it is no longer required for a lawful purpose in the public interest. This principle would also require the weighing of privacy interests against public interests which has been considered in Chapter 3. Such a principle would be consistent with the Retention Limitation Principle contained in the APC. The retention of personal information for longer than required for a lawful purpose in the public interest unreasonably intrudes upon the privacy of the individual concerned as the information may be unnecessarily used or disclosed. The co-regulatory approach proposed by the Federal Attorney-General's Department for the extension of privacy protection to the private sector similarly recognised the importance of including such a principle in the IPPs.[33]

C. The Extension of Privacy Protection to the Private Sector

Several bodies have recommended that the Privacy Act be extended to the private sector.[34] In response to these recommendations the Federal Attorney-General's Department released a Discussion Paper proposing a co-regulatory approach for extending privacy protection to the private sector.[35] The Attorney-General intended to develop legislation for introduction in 1997 which would have provided privacy protection for all Australians in accordance with international best practice.[36] However, earlier this year the Federal Government decided to abandon the co-regulatory approach in favour of industry self-regulation under voluntary codes of practice to reduce 'red tape' for businesses.[37] The Government's decision is likely to have implication for the flow of personal data into Australia from Member States of the European Union. These implications are considered in Chapter 10.

The privacy of personal information may only be properly protected by the extension of privacy protection to the private sector. The Federal Government's decision earlier this year to abandon its proposed co-regulatory approach for the extension of privacy protection in favour of industry self-regulation under voluntary codes of practice means that effective sanctions may not be able to be imposed upon persons who do not comply with such codes. Any protection provided for Internet e-mail by a voluntary code under a self-regulatory scheme would be very limited where the code does not have legislative backing. An industry code or standard for the protection of e-mail which applies to the telecommunications industry may be developed under the Telecommunications Act. The development of industry codes and standards under the Telecommunications Act is discussed in Chapter 8.

Conclusion

The Federal Government's decision to abandon its plans to extend privacy protection to the private sector under a co-regulatory scheme in favour of industry self-regulation under voluntary codes of practice is disappointing in view of the fact that a similar scheme has been successfully implemented in New Zealand.[38] Effective sanctions may not be able to be imposed on carriers and service providers under a voluntary code of practice developed under a self-regulatory scheme with the result that any protection provided for Internet e-mail by such a code would be very limited. The Government has also deterred the States and Territories from introducing privacy and data protection legislation by recommending that they do not implement such legislation.

The indirect requirement for carriers and service providers participating in the TIO scheme to comply with the IPPs contained in the Privacy Act provides only weak protection for Internet e-mail. The TIO scheme does not expressly require participating carriers and service providers to comply with the IPPs but merely permits a user to make a complaint to the TIO if he or she believes that a carrier or service provider is not complying with the IPPs. If users are unaware that a carrier or service provider is not complying with the IPPs no sanction may be imposed on the carrier or service provider under the TIO scheme.

The IPPs themselves provide inadequate protection for personal information. Personal information should only be able to be collected under IPP 1 for a lawful purpose in the public interest. A person to whom personal information is disclosed by a carrier or service provider should only be able to use or disclose the information for the purpose for which it was disclosed. The exceptions contained in IPPs 10 and 11 should be made more specific by being amended as indicated above. Additionally, the IPPs should also include principles which permit only the minimum amount of personal information to be collected for a lawful purpose and

which require that such information be destroyed after it is no longer required for a lawful purpose in the public interest.

1 Federal House of Representatives, Standing Committee on Legal and Constitutional Affairs, *In Confidence*, June 1995, 161 (*'In Confidence'*).
2 Hans van Leeuwen, 'Howard scraps privacy plan for private sector', *Financial Review*, 24 March 1997; Kirsty Simpson, 'Privacy law alarms', *Herald Sun*, 26 March 1997.
3 Privacy Commissioner, *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector*, August 1997 (*'Privacy Consultation Paper'*). Available at http://www.hreoc.gov.au/hreoc/privacy See also Queensland Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland - Issues Paper*, 2 May 1997. Available at http://www.parliament.qld.gov.au/
4 Privacy Act s 6(1).
5 Ibid s 6(1).
6 *Colakovski v Australian Telecommunications Authority* (1991) 100 ALR 111, 118 (Lockhart J).
7 Ibid 119.
8 Andre' Bacard, *The Computer Privacy Handbook* (1995) 66.
9 Graham Greenleaf, 'Privacy principles — irrelevant to cyberspace? (1996) 3(6) *Privacy Law & Policy Reporter* 114, 114-5. See also Charisse Castagnoli, 'Someone's been reading my E-mail! Privacy protection for electronic mail users in the US and the EC' (1993) 9(6) *Computer Law & Practice* 215, 218.
10 (1993) 30 ALD 647 (*'Re Pfizer'*).
11 FOI Act s 41(1).
12 Ibid s 4(1), Privacy Act s 6(1).
13 Privacy Act ss 6(1), 14, 16.
14 In contrast the New Zealand Privacy Act 1993 (NZ) applies to personal information collected by organisations in both the public and private sectors.
15 Privacy Act s 27(1)(n); Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).
16 Telstra ceased to be a Commonwealth agency on 1 February 1992: Telstra Corporation Act 1991 (Cth) s 26; Privacy Act s 6(1) - see definition of 'agency'.
17 Telecommunications Act ss 245, 246.
18 Telecommunications Industry Ombudsman Constitution cl 4.1.
19 The TIO may also make a recommendation that a carrier or service provider pay up to $50,000 compensation which the carrier or service provider is obliged to consider: Ibid cl 6.2.
20 Ibid cl 6.1.
21 A 'generally available publication' is defined in s 6(1) of the Privacy Act.
22 Privacy Act s 6(1).
23 Acts Interpretation Act s 25.
24 Section 72(b) of the Privacy Act allows a Commonwealth agency to make an application to the Privacy Commissioner for a written determination that an act or practice which breaches an IPP shall be disregarded where the public interest in the agency doing the act or engaging in the practice outweighs to a substantial degree the public interest in adhering to the IPP. See also Information Strategy Unit of the Tasmanian Department of Premier and Cabinet, *Information Privacy Principles — A Discussion Paper*, August 1996, 18–23.
25 Greenleaf, above n 9, 115.
26 *In Confidence* 64.
27 Ibid.
28 Ibid 65.
29 Telecommunications Act ss 279-294.
30 *In Confidence* 66.
31 Ibid 68.
32 Australian Privacy Charter Council, *Australian Privacy Charter*, December 1994.
33 Federal Attorney-General's Department, *Discussion Paper - Privacy Protection in the Private Sector*, September 1996, 12 (*'Privacy Discussion Paper'*).
34 Broadband Services Expert Group, *Networking Australia's Future*, December 1994, 67; National Information Services Council Legal Issues Group, *Legal Issues Paper*, August 1995; Senate Economics References Committee, *Connecting You Now... — Telecommunications Developments Towards The Year 2000*, November 1995, 70; *In Confidence* 173; Australian Law Reform Commission and Administrative Review Council, *Freedom of Information Discussion Paper*, May 1995, 125.
35 *Privacy Discussion Paper*.
36 Daryl Williams, 'Privacy and the private sector', (1996) 3(5) *Privacy Law & Policy Reporter* 81, 84.
37 Simpson, above n 2. The Privacy Commissioner has released a proposal for a self-regulatory national scheme for fair information practices in the private sector: *Privacy Consultation Paper*.
38 Privacy Act 1993 (NZ).

CHAPTER 7 — E-MAIL INTERCEPTION

Introduction

The Telecommunications (Interception) Act 1979 (Cth) ('Interception Act') is intended to protect the privacy of users of the telecommunications system by prohibiting the interception of communications passing over the system except where justified for law enforcement or national security purposes.[1] E-mail passing over the Internet is considered to be too easy to intercept.[2]

A significant difficulty with the application of the Interception Act to Internet e-mail is that the Act is not technology neutral. The Act was drafted primarily to apply to the interception of voice communications as opposed to text based communications such as e-mail. It has been suggested that the application of the Act should be reviewed as a result of the increasing use of telecommunications systems for other services such as e-mail which do not necessarily involve voice communications.[3]

The Sections of this Chapter cover the following issues concerning the privacy protection afforded to Internet e-mail by the Interception Act. Section A considers the circumstances in which an offence is committed under the Act where a person intercepts e-mail. Section B discusses the application of the participant monitoring exception to carriers and service providers. Section C examines the exceptions under the Act for employees of carriers and service providers and persons lawfully engaged by them. Section D looks at the exceptions for law enforcement and national security agencies under the Act.

A. Offence of Intercepting a Communication Passing Over a Telecommunications System

Under the Interception Act it is an offence for any person to intercept a communication passing over a telecommunications system.[4] A communication passing over a telecommunications system is intercepted by listening to or recording by any means the communication in its passage over the system without the knowledge of the person making the communication.[5] It is also an offence under the Act for a person to communicate to another person, make use of or make a record of information obtained by lawfully or unlawfully intercepting a communication.[6] These offences should not be given a narrow construction in view of the recognition given in the Act to the high public policy of protecting privacy.[7]

The Interception Act contains exceptions to these offences for employees of carriers and service providers, persons lawfully engaged by them and law enforcement and national security agencies. Similarly, a restrictive approach should be taken to the statutory construction of the exceptions in view of the recognition given in the Act to protecting privacy.[8] The exceptions are discussed later in this Chapter.

The only rights and remedies which an individual has in relation to the

interception of a communication passing over a telecommunications system against persons other than carriers and service providers are the rights provided for in the Interception Act itself.[9] Under the Act a person has a civil right of action against anyone who intercepts a communication to which he or she is a party in contravention of the Act.[10] A person also has a civil right of action against anyone who in contravention of the Act communicates or uses information obtained by intercepting such a communication.[11] These civil remedies were created to promote the privacy of users of telecommunications systems.[12]

The relevant issues to be considered in determining whether an offence is committed where a person snoops on e-mail passing over the Internet are:

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

(2) Whether the Internet constitutes a 'telecommunications system'?

(3) When is e-mail 'listened to' and 'recorded'?

(4) When is e-mail intercepted without the knowledge of the person making the communication?

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

A 'communication' is defined in the Interception Act to include a message and any part of a message 'whether: (a) in the form of: (i) speech music or other sounds; (ii) data; (iii) text; (iv) visual images, whether or not animated; or (v) signals; or (b) in any other form or combination of forms'.[13] E-mail would clearly be a 'communication' as it may consist of text, images, sound and/or animation.

2. *Whether the Internet Constitutes a 'Telecommunications System'?*

The Interception Act defines a 'telecommunications system' to mean 'a telecommunications network that is within Australia ... and includes equipment, a line or other facility that is connected to such a network and is within Australia'.[14] A 'telecommunications network' is defined in the Act to mean 'a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both'.[15] The effect of these two definitions would be that the Australian Internet and all computer networks within Australia including Local Area Networks and Wide Area Networks would be considered to be 'telecommunications systems' whether or not they are connected to a telecommunications network operated by a carrier.[16] Computers linked to the Australian Internet would also be part of a 'telecommunications system' being equipment connected to a telecommunications network.

3. *When is E-mail 'Listened to' and 'Recorded'?*

The word 'listening' is not defined in the Interception Act. However, the Macquarie Dictionary (2nd edition) defines the word 'listen' to mean 'attend closely for the purpose of hearing; give ear'. E-mail consisting of sounds would be 'listened to' where a person hears the contents of the message.

The word 'recorded' is also not defined in the Interception Act. However, the word 'record' is defined in the Act to mean 'a record or copy, whether in writing or otherwise, of the whole or a part of the communication, being a record or copy made by means of the interception'.[17] A communication would be 'recorded' where a person makes a permanent record or copy of it. However, a communication may not be 'recorded' where it is merely displayed on a computer screen as the display would be transient and the communication would not be stored in any permanent form. This is a significant restriction on the privacy protection afforded to communications by the Act.

The definition of 'interception' contained in the Interception Act should be amended to include viewing a communication by any means in its passage over a telecommunications system without the knowledge of the person making the communication. An offence would then be committed where a person snoops on e-mail passing over the Internet by viewing its contents.

Where a person listens to or records Internet e-mail stored in mailboxes of recipients or on intermediate computers there may not be an 'interception' for the purposes of the Interception Act. The issue of whether unread e-mail stored on a computer may be 'intercepted' has been considered in the United States. An offence is committed under the Electronic Communications Privacy Act 1986 (US) ('ECPA') where a person intentionally intercepts an electronic communication.[18] The ECPA defines 'intercept' to mean 'the aural or other acquisition of the contents of any electronic communication through the use of any electronic, mechanical or other device.'[19]

The defendant in *Steve Jackson Games v United States Secret Service*[20] believed that a Bulletin Board Service ('BBS') operated by the plaintiff was used by a group of computer hackers known as the Legion of Doom. The defendant obtained a search warrant to seize and review all information and documents in the plaintiff's BBS computers which contained unread e-mail messages. The plaintiff argued that the defendant unlawfully 'intercepted' electronic communications in breach of the ECPA by seizing and reviewing the e-mail messages stored in the BBS computers.

Sparks J held that the defendant had not 'intercepted' the unread e-mail as the seizure of the e-mail had to be contemporaneous with its transmission for there to be an 'interception' contemplated by the ECPA.[21] It has been suggested that the decision by Sparks J is illogical as the privacy protection afforded to e-mail by the ECPA constantly changes during transmission depending on whether the message happens to be passing over a wire or stored on an intermediate computer at the time it is captured.[22]

Internet e-mail stored in mailboxes of recipients or on intermediate computers may not be 'intercepted' for the purposes of the Interception Act where a person listens to or records the message unless the listening or recording is contemporaneous with

the transmission of the message. The Act does not impose any restrictions on the communications and uses which may be made of information relating to the contents of a communication which has not been obtained by the 'interception' of the communication. The disclosures and uses which carriers, service providers and their employees may make of information relating to the contents of a communication is considered in Chapter 8.

4. *When is E-mail Intercepted Without the Knowledge of the Person Making the Communication?*

At least the consent of the party speaking at the relevant time in a telephone conversation is required for the interception of the conversation to be with the knowledge of the person making the communication for the purposes of the Interception Act.[23] It is likely that only the consent of the sender of e-mail would be required for the interception of the message to be with the knowledge of the person making the communication as only the sender makes the message pass over the Internet. Even where the sender is replying to an earlier message from the recipient and the reply contains a copy of the earlier message only the consent of the sender would seem to be required as the e-mail messages of the sender and recipient would appear to be separate 'communications' for the purposes of the Act.

In *Bohach and Catalano v The City of Reno*[24] a US District Court considered whether the storage of copies of messages on an intermediate computer was an 'interception' of the messages for the purposes of the ECPA. The plaintiffs were officers of the Reno Police Department who sent messages to each other over the Department's 'Alphapage' message system which enabled the transmission of brief alphanumeric electronic messages to the visual displays of pagers. All messages were recorded and stored by the system and all users had been notified that their messages would be 'logged on the network'. The plaintiffs were subject to an internal affairs investigation based on the contents of their messages. They claimed that the storage of their messages on the Department's computer was an 'interception' of the messages in breach of the ECPA.

Reed J held that no 'interception' occurred by reason of the storage of the messages on the Reno Police Department's computer. He queried how there could have been an 'interception' in the ordinary sense of the word where 'no computer or phone lines have been tapped, no conversations picked up by hidden microphones, no duplicate pager "cloned" to tap into messages intended for another recipient.'[25] If there had been an 'interception' of the messages Reed J was of the view that consent would likely be implied 'for one who sends a message using a computer must surely understand that the message will pass through the computer.'[26]

The storage of Internet e-mail in mailboxes of recipients and on intermediate computers is necessary for the transmission of messages over the Internet. Such storage of e-mail may not be an 'interception' of the message for the purposes of the Interception Act as the storage would be unlikely to be without the knowledge of the person making the communication. The sender of e-mail probably impliedly consents to such storage by sending the message over the Internet. Where information relating to the contents of a communication has not been obtained by the 'interception' of the communication the Act imposes no restrictions on the communications and uses which may be made of such information. Chapter 8 considers the disclosures and uses which carriers, service providers and their employees may make of information relating to the contents of a communication.

B. Participant Monitoring Exception

In accordance with the participant monitoring exception a communication is not intercepted where a person who is lawfully on premises to which a telecommunications service is supplied by a carrier or service provider listens to or records a communication passing over a telecommunications system of which that service forms a part. The listening to or recording must be by means of apparatus or equipment which forms part of the telecommunications service. The communication must be a communication that is being made to or from that service or that is being received at that service in the ordinary course of the operation of the telecommunications system.[27]

The mischief contemplated by the participant monitoring exception was listening to or recording a communication by means of apparatus or equipment that was not supplied by Telstra.[28] It is intended that the exception be given full literal effect despite any overlap with the other exceptions contained in the Interception Act.[29] However, the application of the exception is surrounded by uncertainty as it was drafted when Telstra had a monopoly on providing all telecommunications services and equipment. Advances in technology have added further to this uncertainty.[30]

The relevant issues to be considered in determining whether the participant monitoring exception applies where a person snooping on the Internet intercepts e-mail are:

(1) When is a person 'lawfully on premises'?

(2) What is a 'telecommunications service'?

(3) What is 'apparatus' and 'equipment'?

(4) When does apparatus or equipment form 'part of a telecommunications service'?

(5) When is a communication made to or from or received at a telecommunications service?

1. *When is a Person 'Lawfully on Premises'?*

The expression 'lawfully on premises' is not defined in the Interception Act. However, the word 'on' is defined in the Macquarie Dictionary (2nd ed) to mean 'immediate proximity'. A carrier or service provider which supplies an

Internet e-mail service would be 'lawfully on premises' to which the service is supplied where the host computer which holds the mailboxes of users is located on the premises of the carrier or service provider itself.

2. *What is a 'Telecommunications Service'?*

The Interception Act defines a 'telecommunications service' to mean:

'[A] service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier [or service provider] but not being a service for carrying communications solely by means of a radiocommunication'.[31]

An Internet e-mail service would be a 'telecommunications service' as it enables e-mail to be carried over the Australian Internet and other networks in Australia operated by carriers and service providers.[32] The host computer which holds the mailboxes of users would form part of the Internet e-mail service as it is the means which enables e-mail to be carried over the Australian Internet and other networks.

3. *What is 'Apparatus' and 'Equipment'?*

The word 'apparatus' is not defined in the Interception Act. However, the word 'apparatus' is defined in the Macquarie Dictionary (2nd ed) to mean 'an assemblage of instruments, machinery, appliances, materials, etc, for a particular use'. The word 'equipment' is defined in the Interception Act to mean 'any apparatus or equipment used, or intended for use, in or in connection with a telecommunications network, but does not include a line'.[33] The Macquarie Dictionary (2nd ed) defines the word 'equip' to mean 'anything used in or provided for equipping' and the word 'equipping' to mean 'to furnish or provide with whatever is needed for services or for any undertaking'. These definitions suggest that the words 'apparatus' and 'equipment' are broad concepts. It is likely that network interfaces and all other parts of a computer network including computers themselves which may be used to listen to or record e-mail would be 'apparatus' or 'equipment' for the purposes of the Interception Act.

4. *When Does Apparatus or Equipment Form 'Part of a Telecommunications Service'?*

Apparatus or equipment used to listen to or record a communication must form 'part of a telecommunications service' for the participant monitoring exception to be applicable. The apparatus or equipment may also need to be supplied by a carrier or service provider for the exception to apply. In *R v Curran and Torney*[34] the Victorian Supreme Court considered whether an offence was committed under the Interception Act by recording telephone calls using a portable tape recorder.

The defendants in *Curran and Torney* were two criminals who were hiding in a house. They connected a telephone in such a way that calls could be made upon the telephone service of a neighbouring house. The neighbour experienced telephone difficulties and reported to Telstra[35] that he believed that someone else was using his telephone service. As he thought Telstra was doing nothing about it he used a portable tape recorder to record the telephone calls made by the criminals and gave the recording to the police.

McGarvie J held that the neighbour committed an offence under the Interception Act by recording the calls. The participant monitoring exception was not applicable as the neighbour had not recorded the calls made by the criminals using equipment which was 'part of a telecommunications service' supplied by Telstra.[36]

5. *When is a Communication Made to or From or Received at a Telecommunications Service?*

A communication must be a communication that is made to or from a telecommunications service or received at such a service in the ordinary course of the operation of a telecommunications system of which the service forms part. Carriers and service providers which supply Internet e-mail services may seek to rely upon the participant monitoring exception to listen to or record e-mail sent to or from the service where the host computer is located on the premises of the carrier or service provider itself. The participant monitoring exception may also be sought to be relied upon by carriers and service providers to listen to or record e-mail which is received at an Internet e-mail service in the ordinary course of the operation of the Internet. E-mail may be received at an Internet e-mail service where the service acts as an intermediate computer for the passing of messages over the Internet.

The application of the participant monitoring exception to the interception of Internet e-mail is uncertain as it was never intended to apply to messages passing over the Internet. The exception permits unreasonable intrusions upon the privacy of users of e-mail. It allows carriers and service providers to snoop on e-mail by intercepting messages sent to or from an Internet e-mail service which they supply or received at such a service in the ordinary course of the operation of the Internet.

C. Exceptions for Employees of Carriers and Service Providers and Persons Lawfully Engaged by Them

Exceptions under the Interception Act permit employees of carriers and service providers and persons lawfully engaged by them to intercept communications passing over a telecommunications system and communicate and make use of information obtained by intercepting communications without committing an offence under the Act.

1. *Interception of Communications Passing Over a Telecommunications System*

It is said that carriers and service providers have an important obligation to keep their networks fully maintained and operational which requires a certain level of monitoring and recording of communications.[37] An exception allows employees of carriers and service providers and persons lawfully engaged by them to

intercept communications in the course of their duties for the purpose of network operation or network maintenance. However, it must be reasonably necessary for the employee or person lawfully engaged to intercept the communication in order to perform his or her duties effectively.[38]

In determining whether it was reasonably necessary for employees of carriers and service providers and persons lawfully engaged by them to intercept a communication in order to perform his or her duties effectively a court may have regard to any matters specified in the regulations made under the Interception Act.[39] As no matters have yet been specified in the regulations it is arguable that the exception would not comply with the ICCPR on the basis that the law is not sufficiently clear to give users an adequate indication as to the circumstances in which an employee or person lawfully engaged may intercept a communication.[40] Matters should be specified in the regulations to indicate when it is reasonably necessary for employees and persons lawfully engaged to intercept communications.

2. *Communication and Use of Information Obtained by Intercepting a Communication*

An exception allows employees of carriers and service providers to communicate or make use of information lawfully or unlawfully obtained by intercepting a communication where the information relates to network operation, network maintenance or the supply of telecommunications services by the carrier or service provider.[41] Another exception permits employees to communicate to other carriers and service providers information lawfully or unlawfully obtained by intercepting a communication where the information relates to network operation, network maintenance or the supply of telecommunications services by the other carrier or service provider. The communication of the information to the other carrier or service provider must be for the purpose of the carrier or service provider carrying on its business relating to the supply of telecommunications services.[42] Carriers and service providers to which such information has been communicated may only communicate or use the information for the purpose for which it was communicated.[43]

The circumstances in which employees of carriers and service providers may communicate or make use of information relating to the supply of telecommunications services should be clarified. The exceptions contained in the Telecommunications Act 1997 (Cth) ('Telecommunications Act') concerning the disclosure and use of information relating to network operation, network maintenance and the supply of telecommunications services by employees of carriers, carriage service providers and telecommunications contractors are more restrictive than the exceptions contained in the Interception Act.[44] Chapter 8 examines the exceptions contained in the Telecommunications Act relating to the disclosure and use of communications information by employees.

An exception under the Interception Act also allows employees of carriers and service providers to communicate to the Australian Federal Police ('AFP'), National Crime Authority ('NCA') and eligible State authorities[45] information lawfully obtained by intercepting a communication for purposes connected with the investigation of a serious offence.[46] This exception may be justified on the basis that the public interests in the investigation of serious offences outweigh privacy interests.

D. Exceptions for Law Enforcement and National Security Agencies

Law enforcement and national security agencies are said to be excited about the potential for snooping on the Internet.[47] The rights of interception vested in law enforcement and national security agencies are said to be vital for protecting the lawful interests of the community against organised crime.[48] The exercise of these rights is justified on the basis that upholding the law outweighs the privacy rights of individuals.[49] The attendant invasion of privacy has been described as 'regrettable'.[50]

An offence is not committed under the Interception Act where a communication passing over a telecommunications system is intercepted under a warrant.[51] The AFP, NCA and declared eligible State authorities[52] may apply to an eligible Federal Court Judge for a warrant in respect of a telecommunications service for the purpose of obtaining information which would assist in the investigation of a serious offence.[53] A warrant may be issued by a Judge in relation to an Internet e-mail service.

When issuing a warrant for a serious offence which does not involve murder, kidnapping or narcotics an eligible Federal Court Judge must have regard to how much the privacy of persons would be interfered with by the interception of communications under the warrant.[54] A Judge must exercise the power to issue a warrant without bias and fairly by weighing the competing considerations of privacy on the one hand and law enforcement on the other.[55] Consideration is to be given to any interference with the privacy of communications.[56]

Conclusion

There are significant gaps in the protection afforded to Internet e-mail by the Interception Act. Advances in technology and the introduction of competition into the telecommunications industry have widened these gaps by providing carriers and service providers with even more opportunities to intercept communications. Where a communication is not 'intercepted' the Act does not impose any restrictions on the communications and uses which may be made of information relating to the contents of the communication. A communication may not be 'intercepted' where it is merely viewed on a computer screen as the

display would be transient without the communication being permanently stored. E-mail which is stored in the mailboxes of intended recipients or on intermediate computers may also not be 'intercepted' under the Act. The participant monitoring exception may be relied upon by carriers and service providers to intercept e-mail sent to or from an Internet e-mail service which they supply or received at such a service where the service is located on the premises of the carrier or service provider itself.

Amendments are required to be made to the Interception Act to address the advances in technology and the introduction of competition into the telecommunications industry. The definition of 'interception' needs to be amended to include viewing a communication by any means in its passage over a telecommunications system. The participant monitoring exception should not be able to be relied upon by carriers or service providers to unreasonably intrude upon the privacy of users of e-mail by snooping on messages. The regulations made under the Act should specify matters to indicate when it is reasonably necessary for employees of carriers and service providers and persons lawfully engaged by them to intercept communications in order to perform their duties effectively. The circumstances in which employees may communicate or use information relating to the supply of telecommunications services should be clarified.

1 *John Fairfax Publications v Doe* (1995) 37 NSWLR 81, 97 (Kirby P) ('*John Fairfax Publications*'); *Taciak v Australian Federal Police* (1995) 131 ALR 319, 330 (Sackville J) ('*Taciak*'); *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222, 229 (Lee J); *R v Smith* (1991) 52 A Crim R 447, 449 (Kennedy, Pidgeon and Pollard JJ).
2 Philip Zimmermann, *The Official PGP User's Guide* (1995) 6.
3 Holly Raiche, 'Privacy and telecommunications after 1997' (1996) 3 *Privacy Law & Policy Reporter* 53.
4 Interception Act ss 7(1)(a), 105.
5 Ibid s 6(1).
6 Ibid ss 5A, 63(1).
7 *John Fairfax Publications* (1995) 37 NSWLR 81, 97 (Kirby P).
8 *Taciak* (1995) 131 ALR 319, 331 (Sackville J).
9 *Kizon v Palmer* (1997) 142 ALR 488, 521 (Lindgren J).
10 Interception Act s 107A(3).
11 Ibid s 107A(4).
12 Telecommunications (Interception) Amendment Bill 1994 Explanatory Memorandum 2.
13 Interception Act s 5(1).
14 Ibid.
15 Ibid.
16 Graham Greenleaf, '"Interception" on the Internet - the risks for ISPs' (1996) 3(5) *Privacy Law & Policy Reporter* 93.
17 Interception Act s 5(1).
18 ECPA s 2511(1)(a).
19 Ibid s 2510(4).
20 816 F Supp 432 (1993) (US District Court) ('*Steve Jackson Games*'). The decision was affirmed in *Steve Jackson Games v United States Secret Service* 36 F 3d 457 (1994) (US Court of Appeals).
21 Ibid 442. See also *Bohach and Catalano v The City of Reno* 932 F Supp 1232 (1996) (US District Court); *State of Oklahoma v One (1) Pioneer CD-ROM changer and Davis* 891 P 2d 600 (1994) (US Court of Appeals).
22 William Powell and Others, *Tools For Privacy* (1995). Available at ftp://ftp.crl.com/users/ro/smart/TFP/
23 *R v Padman* [1979] Tas SR 37, 40 (Crawford J).
24 932 F Supp 1232 (1996).
25 Ibid 1236.
26 Ibid.
27 Interception Act s 6(2).
28 *R v Migliorini* (1981) 53 FLR 221, 225-6 (Cosgrove J).
29 *R v McHardie* [1983] 2 NSWLR 733, 749-50 (Begg, Lee and Cantor JJ). cf *Taciak* (1995) 131 ALR 319, 331 (Sackville J).
30 Frances Wood, 'Your telephone calls: recording and monitoring' (1996) 3(1) *Privacy Law & Policy Reporter* 14, 15-6.
31 Interception Act s 5(1).
32 See also Australian Telecommunications Authority, *Value Added Services Study - Interim Report*, 9 May 1996. 36-7.
33 Interception Act s 5(1).
34 [1983] 2 VR 133 ('*Curran and Torney*').
35 Telstra was formerly known as Telecom.
36 *Curran and Torney* [1983] 2 VR 133, 152-3.
37 Angus Henderson, 'Interception: It's a Difficult Job, But Someone Has to Do It' (1995) May *Australian Communications* 61.
38 Interception Act ss 7(2)(a), 7(2)(aa). The requirement that the listening or recording be 'reasonably necessary' was inserted in response to certain allegations by a group of persons known as the 'Casualties of Telecom' about monitoring and recording of customer telephone services: Commonwealth, *Hansard*, Senate, 7 December 1994, 4131.
39 Interception Act s 7(2A).
40 See *Malone v United Kingdom* (1984) 7 EHRR 14, 40–1.
41 Interception Act s 63B(1).
42 Ibid s 63B(2).
43 Ibid s 73.
44 Telecommunications Act s 291.
45 Eligible state authorities are all State Police Forces, New South Wales Crime Commission, Royal Commission into the New South Wales Police Service, New South Wales Independent Commission Against Corruption and Queensland Criminal Justice Commission: Interception Act s 5.
46 Ibid ss 5, 65A. The serious offences specified involve murder, kidnapping, narcotics, loss of a person's life, serious personal injury, serious damage to personal property, serious fraud, serious loss of revenue, bribery or corruption, substantial planning and organisation, money laundering and computers: Interception Act ss 5, 5D.
47 Simon Davies, *Monitor* (1996) 64.
48 Commonwealth, *Hansard*, Senate Legal and Constitutional Legislation Committee, 21 March 1995, 448.
49 Henderson, above n 37, 61.
50 *Grollo v Commissioner of Australian Federal Police* (1995) 131 ALR 225, 250 (McHugh J) ('*Grollo*').
51 Interception Act s 7(2)(b).
52 The eligible State authorities which have been declared are the Victorian Police, New South Wales Police, New South Wales Crime Commission, New South Wales Independent Commission Against Corruption and South Australian Police. Other authorities may also obtain access to intercepted communications when they are involved in a joint operation with one of these authorities: Australian Telecommunications Authority, Law Enforcement Advisory Committee, *Telecommunications and Law Enforcement*, June 1995, 6–7.
53 Interception Act ss 39, 45, 46. The Telecommunications (Interception) and Listening Device Amendment Bill 1997 will amend the Interception Act to permit the Minister to nominate specified members of the Administrative Appeals Tribunal to issue interception warrants for law enforcement purposes.
54 Ibid s 46(2)(a).
55 *Grollo* (1995) 131 ALR 225, 231 (Brennan CJ, Deane, Dawson and Toohey JJ); *Coco v The Queen* (1994) 179 CLR 427, 444 (Mason CJ, Brennan, Gaudron and McHugh JJ) ('*Coco*').
56 *Coco* (1994) 179 CLR 427, 438 (Mason CJ, Brennan, Gaudron and McHugh JJ).