treated as effective from 23 February 1999. However, it is doubtful at this late stage whether the changes will be of any real assistance in Year 2000 remidiation.

The proposed amendments will only affect the scope of acts that constitute a breach of the *Copyright Act* and not the rights of a party under a licence. Where the owners of computer software wish to prevent decompilation, they can do so by putting a prohibition in the licence agreement. As most standard software licences prohibit decompilation, it is difficult to see how the Bill will encourage interoperability, innovation and Y2K compliance in the commercial software industry.

ASIO LEGISLATION AMENDMENT BILL

The ASIO Legislation Amendment Bill, which was introduced into Parliament in March 1999, contains provisions extending ASIO's powers in relation to computer systems and the on-line environment.

The changes will allow ASIO to hack into computer systems and install surveillance tools, intercept Internet traffic and alter access control and encryption systems to monitor communications.

The Bill has been criticised by privacy groups such as the Electronic Frontiers Foundation who have expressed concern that the unqualified application of such powers may result in invasions of privacy and the fabrication of electronic evidence.

It will be up to Parliament to ensure that the protection of Australia's national security interests does not infringe the privacy of members of the public. For the time being, there is no proposal to place a control on this far-reaching power.

[1] 96-511, 26 June 1997
[2] (1997) 191 CLR 140

Electronic Transmissions to Clients —A Lawyer's Duties

Tim Jones & Michael Rubb, Minter Ellison

With the steady advance of the Information Age, clients are beginning to demand instant communication with their lawyer by electronic means, the most common being e-mail. While e-mail is a convenient and quick method of communication for both the lawyer and the client (although clients sometimes believe that their lawyer should solve their legal problem just as instantly) often neither party is aware of the security risks associated with e-mail.

In providing advice to clients by e-mail, lawyers may well be exposed to legal proceedings by clients in cases where sensitive material falls into the wrong hands.

In drawing attention to the lawyer's potential exposure to liability to the client in providing advice by e-mail, this article will look at the following issues:

- What is 'e-mail'?
- How does it work?
- Security issues
- Security measures
- Implications of failure to implement security measures
- Disclaimers and e-mail policies

WHAT IS 'E-MAIL'?

Most lawyers are now aware of how e-mail works and the advantages it offers in service delivery. It allows quick written communication to clients, and allows the lawyer to attach application documents (such as Word, Word Perfect and Excel) containing, for example, contracts and pleadings to clients. It also allows multiple addressing of messages very quickly, without the need to send multiple copies of documents in the same fashion as required by letters and faxes.

E-mail is simply 'electronic mail'. It is the correspondence between people of written messages from one personal computer ('PC') to another. A common way of connecting computers is through the Internet (there are other ways such as online services like CompuServe, which routes e-mail through internal lines), which transmits data 'packets' to computers that are on the same circuit. Normally a computer will not access a data packet that is not addressed to the user. However, software is available that allows a user to accept data packets that are not addressed to that user (explained further below).

The Internet is not a secure medium due mainly to the fact that Internet communication channels are shared channels. The Internet is a network comprising thousands of computers throughout the world, connected by telephone lines, dedicated data lines, satellite transmissions and cable TV networks. The information intended for any computer on a network may pass through virtually any number of other computers while in transit.

HOW DOES E-MAIL WORK?

E-mail typically works as follows:

1. The sender writes the message

on his or her PC. By way of a dial-up modem connection, the data is sent to the mail server of his or her Internet Service Provider ('ISP').

2. The ISP of the sender sends the e-mail out into the Internet. Larger messages are split into smaller data packages that each individually search the fastest way to the ISP of the addressee. In transit, the packages pass through numerous computers of third parties which forward the packet to the addressee.

3. The ISP of the addressee receives the e-mail and stores it on the ISP's mail server. The addressee usually receives a notification about the message in his or her 'in - box'.

4. The addressee connects to the mail server of the ISP and down loads the waiting message to his or her PC in order to read it.

The e-mail communication between two customers of an online service (such as CompuServe) basically follows the same pattern, however, the message is not sent through the Internet, but via an internal network.

SECURITY ISSUES

In basic terms, e-mails can be intercepted and read or tampered with by third parties on the Internet. The implications of this from a lawyer's perspective are serious.

Security issues associated with purchasing goods and services on the Internet (e.g. credit card fraud) have been the recent subject of media attention. The security issues associated with e-mail have not been afforded the same attention but are just as important, and perhaps more so in their potential to impact upon lawyers in their dealings with clients.

SENSITIVE MATERIAL

The following types of information are examples of sensitive material which may be transferred between lawyer and client:

- Prospectus details
- Client financial details
- Litigation strategy
- Commercial or litigation negotiation strategy
- Adverse evidence in a criminal matter
- Sensitive commercial information eg tender, merger/ acquisition details

While security breaches involving the above types of information may never occur, the potential should be enough to concern most lawyers.

The main security risks in respect of sensitive client information involve integrity and authentication.

INTEGRITY AND AUTHENTICATION

Integrity has to do with whether the e-mail (and attachments) which reaches the client has been already read, or has been tampered with.

Authentication has to do with whether the e-mail which the client has received was actually sent by the person stated as the author.

'Eavesdroppers' or 'spies' are people who breach e-mail integrity and authentication. They include 'hackers', 'crackers', 'spoofers' and 'sniffers'.

HACKERS AND CRACKERS

Hackers and crackers can affect a person's computer systems by infiltrating and controlling, or damaging the system from which e-mail originates.

Hackers engage in the unauthorised entry to, or modification of, computer systems. The hacker's main purpose is to alter the system so that they can access it at a later date for whatever means they wish.

Crackers are the Internet equivalent of vandals. They break into the system and damage files.

SPOOFING AND SNIFFING

Most lawyers would be aware of the exploits of hackers and crackers, but few would be aware of the existence of spoofers and sniffers.

Every computer connected to the Internet has a number serving as an 'address' (a 'numerical domain'). These domains are used to direct e-mail messages to the correct recipient. Every computer in the Internet that is forwarding e-mail messages can be configured to not only pass on incoming data packets, but also store a copy of them.

Spoofing is the where an e-mail is intercepted on the Internet and tampered with without the sender's knowledge. The recipient may then act upon the spoofed e-mail to his or her detriment. The sender has no way of knowing the content of the e-mail actually received by the recipient, unless the recipient contacts the sender and queries it.

The practice of sniffing is similar, however, the sniffer only reads the e-mail without tampering with it. The e-mail will reach the intended recipient, who will be none the wiser that his or her privacy has been invaded.

Sniffing and spoofing both have implications in respect of litigation or commercial strategy or any form of confidential information which is intended to remain confidential.

SECURITY MEASURES

While is it not always possible to prevent hacking and cracking, there are inexpensive and effective measures to prevent spoofing and sniffing, namely digital signature and encryption software.

DIGITAL SIGNATURES

Digital signatures are the electronic equivalent of handwritten signatures. Digital signatures don't look like conventional signatures. They are mathematical algorithms appended to an e-mail and viewed on the screen as an apparently random sequence of letters and numbers. Each sequence is unique to a particular e-mail.

Unlike encryption, a digital signature doesn't change the contents of the document - it merely provides a method whereby the recipient can verify the authenticity of the

document. Any change, however minor, such as a single space inserted in the document, will change the digital signature. The contents can still be read by a sniffer, but if the contents are tampered with, the resulting document will have a different digital signature. For this reason, digital signatures are useful to prevent spoofing but not sniffing. Encryption is more effective in preventing spoofing (see ***Encryption***, below).

When a client receives an e-mail containing a digital signature, it is quick and easy to verify the digital signature.

The process of using a digital signature involves a ***public key*** and a ***private key***. The digital signature will be created by the private key and verified by the public key.

Prior to sending a message to his or her client, a lawyer will have provided him or her with the public key, which is basically a small software program. It contains a code identified with the owner of the private key. To verify a signature, a client's public key software calculates the digital signature code of the sender and if the message digest and signature block are identical, the signature is valid.

A person can only use a digital signature effectively if they have both the computer file that generates the signature and the secret password that allows use of that file.

CERTIFICATION AUTHORITIES

It is possible to check whether a public key belongs to a particular person. Certification Authorities ('CA's') are third parties whose purpose is to hold public key information so that signatures can be verified by receivers (in the future, law firms may well become CA's, regulated by a state agency for quality control and key integrity). Verification by a CA is designed to protect against a situation where prior to sending a message, an imposter pretends to be someone and provides the public key for use with their private key ('digital signature spoofing'). If for example, a client is fooled by the impersonator, any subsequent e-mails bearing a digital signature would be verified by the public key because it would correspond with the imposter's private key.

The purpose of the CA is perhaps analogous to that of a notary public, who essentially certifies that the person signing a document is who the person claims to be. Signatures which are outside the third party system are not necessarily invalid. However, the message integrity is not as great as one within the third party system.

The CA will be able to verify whether the person who sent the public key is actually who they claim to be. The reliability of the CA will depend upon its own standards of proof of identity. Obviously a CA which requires a high standard of proof of identity will be more reliable than one who does not.

Standards and legislation regarding the use of digital signatures

In April 1998, the Federal Attorney-General's Electronic Commerce Experts Group ('ECEG') reported (in its *Issues Paper No 1*) on a wide range of e-commerce issues, including the legislation required to implement a public key infrastructure.

As a result of ECEG's recommendations, the Commonwealth Government is currently in the process of drafting a proposed framework for the use of digital signatures.

The *Electronic Transactions Bill 1999* was introduced into Parliament on 30 June 1999 and is currently the subject of debate. The Bill is designed to encourage electronic commerce by allowing existing legal requirements in relation to paper based commerce to be satisfied by electronic means. For the purposes of a Commonwealth Law, a transaction will not be invalid merely for the reason that it took place by way of electronic communication.

In the absence of agreement between the parties on the issue, the Bill also sets out the requirements for authentication of electronic communications. 'Electronic Signatures' must identify the person and his or her approval of the electronic communication. Such signatures must also be as reliable as is appropriate for the purposes for which the information is communicated.

The National Public Key Infrastructure Working Group Report on Certification Authorities and a Public Key Infrastructure was released earlier this year.[1] The Working Group recommends the establishment of a peak body to oversee the Australian National Electronic Authentication Framework ('ANEAF'). The Working Group suggests that the focus of the peak body should initially be on public key infrastructure, and in particular, to establish a national public key infrastructure ('NPKI') under the ANEAF.

On 23 June 1999, Senator Richard Alston (Federal Ministry for Communications, Information Technology and the Arts) announced that the Government will establish a peak body to oversee the development of a national framework for electronic authentication of online activity. The new National Electronic Authentication Council ('NEAC') aims to do the following:

- Provide a national focal point on authentication matters including co-ordination of authentication related activities at a national and international level.
- Provide advice to Government on authentication and related matters.
- Oversee the development by industry bodies and Standards Australia of a framework of technical standards and codes of business practice on authentication matters.
- Provide best practice information and advice to industry in respect of authentication matters.[2]

It would seem that once basic authentication information is

available to industry and consumers that law firms would certainly be expected to be aware of the issues associated with authentication, including security issues.

A uniform public key infrastructure is likely to be the subject of the Federal Government's next Bill drafted in response to the ECEG report. It is anticipated that it will address uniformity of authentication technology, the apportionment of liability for security breaches, and standards for CAs.

ENCRYPTION

Encryption is similar to a digital signature, however, it allows an entire message to be encrypted, rather than just the signature. The entire message will be scrambled by the private key and can only be unscrambled by use of the paired public key, which the client will have been given prior to receiving the message.

Encryption is an effective way to prevent sniffing, and is perhaps more useful than a digital signature when transmitting sensitive material via e-mail.

E-MAIL SECURITY PROGRAMS

E-mail security software is readily and cheaply available and practical to use. Some examples are described on the Law Society of WA web site.[3]

Instances of security breach

Although it is not exactly easy to eavesdrop on or tamper with someone's e-mail, far less target a particular individual's or firm's e-mail by searching out a single data packet passing through the Internet, there have been enough instances to justify caution.

The following examples of security breaches are taken from the Massachusetts Institute of Technology *Technology Review*:

- In Autumn of 1993, a student at Dartmouth University sent forged electronic mail saying that a midterm exam in professor David Becker's course on Latin American politics was cancelled because Becker had a family emergency. The mail message was sent at 11:00 p.m. the night before the test. Only half of the class showed up for the exam the next morning.
- In October 1994, someone broke into the computer account of Grady Blount, a professor of environmental science at Texas A&M University, and sent out racist electronic mail to more than 20,000 people on the Internet. It was by no means a harmless practical joke. 'We received death threats as the result of that hate mail that was sent out under my name', recalls Blount, who says that even his research grants were put in jeopardy as a result of the incident.

Implications of a lawyer's failure to implement security measures

A lawyer who fails to implement the necessary security measures exposes the e-mail to a security breach. As a result, the client may lose legal professional privilege over the e-mail (and attachments) or suffer financial damage resulting from improper use of the e-mail.

The client may then have grounds to seek damages from the lawyer in contract or in tort, or both. Perhaps the most relevant causes of action would be:

1. breach of duty to refrain from disclosing privileged communications; and
2. breach of the lawyer's duty of confidence to the client.

The client may also have grounds for professional sanctions against the lawyer for failure to implement the necessary security measures.[4] This article however, does not attempt to address this issue.

LEGAL PROFESSIONAL PRIVILEGE

It is a lawyer's duty to ensure that his or her client's valid claim for legal professional privilege is not lost.[5] A lawyer who breaches this duty by disclosing his or her client's privileged communications may confer a right of action on the client in respect of the breach, and may be exposed to a claim for damages.[6]

Legal professional privilege covers:

- confidential communications between the lawyer and client; and
- documents which are made for the sole purpose of advice or to be used in anticipated or existing legal proceedings.[7]

E-MAIL CAN BE 'PRIVILEGED'

E-mail communications can potentially satisfy both of the above two requirements. *Prima facie*, privileged communications include any communications between the lawyer and client via e-mail.[8] It may also include any printed copy of an e-mail or attachment which in itself is privileged[9] and may include any printed copy of an e-mail or attachment which is non-privileged[10].

WHAT TYPES OF E-MAIL WILL BE CONSIDERED PRIVILEGED?

One of the fundamental conditions of legal professional privilege is that the communication or document must be confidential.[11] Legal professional privilege will not apply where the communication took place in circumstances where confidentiality did not attach.[12] Common examples include communications between the lawyer or client in the presence of third parties[13](but see *R v Uljee*, below) or events or knowledge which are already within the public domain[14].

In these types of situations, the parties ought not reasonably consider the communication to be of a confidential nature.

It is not unreasonable for two corresponding parties to consider e-mails confidential. Although a sender may be aware of the risk that the e-mail may be obtained or tampered with by a third party, just as with telephone and mail communication, e-mails are not intended by the recipient to be intercepted. Unless there are unusual circumstances whereby a person is or should be aware that his or her e-mails will be obtained by a specific third party, e-mail should be considered confidential information.

Interesting issues arise where the client's e-mail address is his or her place of employment, and the employer's e-mail policy prohibits the client from sending and receiving personal e-mail. Often the policy will allow the employer to 'monitor' staff e-mail. It may be that the client should be aware of such unusual circumstances and will lose any privilege which would otherwise attach.

THE AUSTRALIAN POSITION

With certain qualifications, the rule in Australia relating to privilege is that a party to litigation who has obtained a privileged document, or a copy of it, from the opposing party, whether by accident, trickery or theft, may tender that document in evidence.[15] This is subject to applying the test of 'fairness' to determine whether legal professional privilege has been lost as a result of an inadvertent disclosure.[16] Usually the party applying for privilege in respect of evidence will seek an injunction preventing its disclosure.[17]

It is uncertain whether the Australian position will support privilege in an intercepted e-mail.

The test for privilege in *R v Uljee* (see ***The New Zealand position*** , below) perhaps allows more scope for a claim of privilege, but has not received support in Australia.[18]

A further issue to be aware of in the context of e-mail is that a document that has been reproduced in full (or in part - where it is a significant part) in a pleading or affidavit may result in a waiver of the privilege that attaches to that document.[19] By analogy the same may apply to documents disclosed in an e-mail.

Lawyers should seriously consider this issue when disclosing documents in e-mails where such documents may have a valid claim of privilege attached to them. Such disclosure could occur by:

1. attaching a scanned document;
2. attaching a draft document, such as pleadings, especially where that draft document discloses the actual content of another document to which a valid claim of privilege would attach; or
3. rewriting (or cutting and pasting) the contents (or significant extracts) of a document to which a valid claim of privilege would attach within an e-mail.

THE NEW ZEALAND POSITION

The New Zealand Supreme Court's decision in *R v Uljee*[20] provides a slightly different test for privilege.

In that case, a police officer overheard a conversation between a lawyer and client whilst standing outside the door of the room they were in. Neither the lawyer or client were aware that the officer was listening to their conversation. The court concluded that the officer could not give evidence of what he had overheard. The conversation was intended to be confidential and the presence of the police officer outside the room did not change that intention.

McMullin J made the following comment in the course of his judgment:

> 'If deliberate and careful steps have been taken to keep the communication secure from others it seems wrong that it should lose its protections because some eavesdropper has either chanced upon it or taken deliberate steps to listen to it.'[21]

It can be argued then, that e-mails attract privilege despite being intercepted by a person taking deliberate steps to do so. But in the context of e-mail, what 'careful and deliberate steps' should the parties take to protect it?

Certainly the implementation of security measures for e-mails may be a 'deliberate and careful step', but it is uncertain whether anything less will protect privilege.

As a preventative measure, it is prudent for lawyers to implement e-mail security measures, or introduce and enforce an e-mail policy, as the courts may not automatically grant privilege to e-mails.

BREACH OF CONFIDENCE

Lawyers have a duty to their clients to protect any confidential information obtained from their client.[22]

The duty of confidence is based in a combination of contract law and equity and arises from the peculiar relationship of lawyer and client.[23] The duty is also found in the professional rules of each state.[24]

The standard of the duty of confidentiality is high. The client-lawyer relationship is necessarily a relationship of confidence, and the obligation upon lawyers to maintain that confidence is 'in the eyes of the law the very highest...'.[25] As such, the standard imposed by the courts on lawyers to maintain client confidentiality 'is higher than it would be practicable to exact from persons in other types of confidential relations'[26].

The duty is much broader than that relating to legal professional privilege, as it potentially applies to all communications between the solicitor and client, which are presumed to be confidential[27], as well as any documentation received from the client. Confidentiality will therefore apply to most, if not all, e-mail communications between the solicitor and client.

It has been suggested that the only conduct required to fulfil a lawyer's

duty of confidence to his or her client is to take measures that would indicate to a recipient that the information is not for general perusal.[28] The recipient must then act conscientiously and the duty not to disclose without authorisation should apply. The question then arises - what measures are reasonable to put an unauthorised recipient on notice? A standard written warning on the e-mail may not be enough. Given that a lawyer's duty of confidence to his or her client is 'in the eyes of the law the very highest...', the minimum measures may be use of encryption or digital signatures.

It is not unreasonable for a lawyer to be informed about confidentiality issues involving e-mail, and to protect the client's interests in that regard. A court may not be sympathetic to a lawyer who claims he or she wasn't aware of the possibility of a breach of e-mail security and the software available to prevent it, particularly in light of the increasing availability of information on the subject.

In short, a breach of the lawyer's duty to keep the client communications confidential will expose the lawyer to claims for damages by the client.

DISCLAIMERS AND E-MAIL POLICIES

Some Australian law firms have been attempting to shift liability for e-mail security to the client or to employees. The methods used commonly include:

- a standard disclaimer which warns the client only to rely on an e-mail if the advice is confirmed by a signed hard copy letter from the firm and the e-mail has been checked against the hard copy letter and confirmed;
- a standard warning on e-mails that the contents may be privileged and confidential and unauthorised use is prohibited;
- a firm e-mail policy which prohibits employees from transmitting confidential information via e-mail;

The above measures may protect a firm against spoofing of digital signatures (as distinct from spoofing of e-mail), however, they may not be enough to protect a firm against a claim from a client in respect of sniffing or spoofing of e-mail. It is likely that a court would look at whether reasonable measures were taken by a firm to avoid the act that caused the client damage (see above - ***Breach of confidence***).

In relation to e-mail policies, it is unlikely that a court will shift liability to employees for transmitting confidential information via e-mail if the evidence establishes that the policy was commonly being ignored with the firm's actual or constructive knowledge. An e-mail policy would need to have a history of being actively enforced to be effective.

It is also unlikely that a written warning along the lines that the e-mail is not intended for general perusal will save a lawyer from liability for a breach of e-mail security (see above - ***Breach of confidence***).

CONCLUSION

Many firms have introduced e-mail policies prohibiting employees from sending confidential information via e-mail, and are not enforcing them, or have added standard disclaimers and warnings to e-mails in respect of privilege and confidentiality. It is doubtful whether these measures will be effective in allowing lawyers to avoid liability. Certainly they are ineffective in actively preventing e-mail security breaches. At best they are 'stopgaps' and the prudent lawyer should take steps to maintain a higher standard of e-mail security.

One available option is to avoid sending confidential information via e-mail, which may involve introducing and enforcing an e-mail policy prohibiting sending confidential information via e-mail. However, clients are likely to expect e-mail communication with their lawyer as a matter of course, and this is probably only a short term measure.

E-mail security software, such as encryption and digital signature software, is inexpensive, readily available, simple to install and easy to use. Since the standard imposed on lawyers to maintain client confidentiality is high, it would seem reasonable to conclude that, where confidential information is being transmitted via e-mail, the use of e-mail security software is the prudent course of action.

The authors would like to acknowledge the assistance of Simina Gougoulis in preparing this article.

1 available at http://www.noie.gov.au/

2 see http://www.dcita.gov.au

3 http://www.lawsocietywa.asn.au/encrypt.html (the site also contains a useful description of e-mail security and the draft protocol for the exchange of e-mail messages between practitioners, which is currently open for discussion)

4 Sections 28A(1)(b) and (c) of the *Legal Practitioners Act 1893* (WA).

5 *Commissioner of Taxation (Cth) v Citibank Ltd* (1989) 85 ALJR 588 at 596; 20 FCR 403 at 414, per Bowen CJ and Fisher J.

6 For example in *Donellan v Watson* (1990) 21 NSWLR 335 Handley JA stated (at 344): '[A] solicitor who voluntarily disclosed privileged information in court would be liable to the client for breach of contract'

7 *Grant v Downs* (1976) 135 CLR 674 at 682 and 688, per Stephen, Mason and Murphy JJ; *R v Bell* (1980) 146 CLR 141 at 144, per Gibbs J; *O'Reily v Commissioner of State Bank of Victoria* (1983) 153 CLR at 22 and 27 per Mason J; *Baker v Campbell* (1983) 153 CLR 52 at 86, per Murphy J; at 112 per Deane J; at 122 per Dawson J.

8 In WA, the definition of 'document' in Section 5 of the *Interpretation Act 1984* (WA). Section 79B of the *Evidence Act 1903* (WA) and Order 26 Rule 1A of the *Rules of the Supreme Court 1971* (WA) clearly include e-mails within the definition. Consequently, if an e-mail can be discovered under Order 26 of the *Rules of the Supreme Court 1971*, then legal professional privilege should apply to that e-mail provided the email satisfies the test laid down in *Grant v Downs* (1976) 135 CLR 674. This may be applicable in other jurisdictions as well. See:

- Cth: Section 7A *Evidence Act 1905*; Section 25 *Acts Interpretation Act 1901*; Order 1 Rule 4 *Federal Court Rules*.
- NSW: Dictionary *Evidence Act 1995*; Section 21(1) *Interpretation Act 1987*; Part 1 Rule 8 *Supreme Court Rules*.
- Qld: Sections 3 and 5 *Evidence Act 1977*; Order 35 Rule 1 *Rules of the Supreme Court*.
- SA: Sections 34g(1) and 45b(6) *Evidence Act 1929*; Rules 5 and 59.01(c) *Supreme Court Rules*.
- Tas: Sections 40B(1), 59(5) and 81A *Evidence Act 1910*, Section 24 *Interpretation Act 1931*; Order 33 Rule 11A *Rules of the Supreme Court 1965*.
- Vic: Section 3(1) *Evidence Act 1958*; Section 38 *Interpretation of Legislation Act*

1984; Rule 29.12 *General Rules of Civil Procedure 1996.*

- NT: Section 4 *Evidence Act 1939*; Rules 1.09 and 29.12 *Supreme Court Rules.*

9 *Cole v Elders Finance & Investment Co Ltd* [1993] 2 VR 356.

10 *Propend Ltd v Commissioner of the Australian Federal Police* (1995) 79 A Crim R 453.

11 *Re Griffin* (1887) NSWR 132 at 134, per Innes J; *Baker v Campbell* (1983) 153 CLR 52; (1983) 49 ALR 385; (1983) 57 ALJR 749; (1983) 14 ATR 713; (1983) 83 ATC 4606; CLR at 67 - 68, per Gibbs J; *J-Corp Pty Ltd v Australian Builders Labourers Federated Union of Workers-West Australian Branch* (1992) 110 ALR 510 at 513 - 514, per French J.

12 *J-Corp Pty Ltd v Australian Builders Labourers Federated Union of Workers-West Australian Branch* (1992) 110 ALR 510 at 515, per French J; *R v Braham & Mason* [1976] VR 547 at 549, per Lush J.

13 *R v Braham & Mason* [1976] VR 547.

14 *J-Corp Pty Ltd v Australian Builders Labourers Federated Union of Workers-West Australian Branch* (1992) 110 ALR 510.

15 *Bell v David Jones Ltd* (1948) 49 SR(NSW) 223 at 227; *Warner v Women's Hospital* [1954] VLR 410 at 421, per Sholl J; *Commissioner of Taxation (Cth) v Citibank Ltd* (1989) 20 FCR 403; 85 ALR 588 at 414-415, per Bowen CJ and Fisher J. Gibbs J in *Baker v Campbell* (1983) 153 CLR 52 at 67 - 68 reviewed the decisions in *Calcraft v Guest* [1898] 1 QB 759 and *Lord Ashburton v Pape* [1913] 2 Ch 469 but did not decide conclusively on their position in Australian. For an insightful analysis of inadvertent disclosures and its effect on the relationship between legal professional privilege and breach of confidence see: Newbold, 'Inadvertent Disclosure in Civil Proceedings' (1991) 107 LQR 99.

16 *Hooker Corporation Ltd v Darling Harbour Authority (1987)* 9 NSWLR 538.

17 For a discussion of available remedies, see Bell v David Jones Ltd (1948) 49 SR (NSW) 223; Ashburton v Pope [1913] 2 Ch 469; Baker v Campbell (1983) 153 CLR 52 at 68 per Gibbs CJ.

18 *Baker v Campbell* (1983) 153 CLR 52 at 67-68 per Gibbs CJ.

19 *Attorney General (NT) v Maurice* (1988) 161 CLR 475, which distinguished between full disclosure and a mere reference to a document.

20 [1982] 1 NZLR 561

21 *R v Uljee* [1982] 1 NZLR 561 at 576, per McMullin J.

22 *Baker v Campbell* (1983) 153 CLR 52 at 65, per Gibbs J; (1983) 49 ALR 385; (1983) 57 ALJR 749; (1983) 14 ATR 713; (1983) 83 ATC 4606.

23 Dal Pont,GE; *Lawyers' Professional Responsibility in Australia and New Zealand*; 1996; p213

24 NSW: Rule 2 *Rules of Professional Conduct and Practice* 1995.
Qld: Para 4.02.1 *Solicitors Handbook.*
SA: Rule 9 *Professional Conduct Rules.*
Tas: Rule 11 *Rules of Practice 1994.*
Vic: *Practice Rules 1998.* See also Section 64(c) *Legal Practice Act 1996.*
WA: Rule 6 *Professional Conduct Rules.*
ACT: Para 5 *Guide to Professional Conduct and Etiquette.*
NT: Rule 9 *Professional Conduct Rules.*
See also: Rule 3 in the Australian Bar Association's *Code of Conduct* and Rule 2 of the Law Council of Australia's *Model Rules of Professional Conduct and Practice.*

25 *Rakusen v Ellis, Munday & Clarke* [1912] 1 Ch 831 at 840, per Fletcher Moulton LJ.

26 *Rakusen v Ellis, Munday & Clarke* [1912] 1 Ch 831 at 840, per Fletcher Moulton LJ.

27 By virtue of the equitable doctrine of confidential information

28 Paul McGinness, 'The Internet and privacy - some issues facing the private sector', *Computers and Law*, June 1996, p26

Restricting Access to Content—Filtering, Labelling and Education

Nick Alston, Summer Clerk, Gilbert & Tobin

In mid-1999 the Federal Government, unfettered by constitutional rights of freedom of speech, led the world in passing the *Broadcasting Services Amendment (Online Services) Act*. The stated objective of the Act is to protect children from prohibited content available over the Internet and it seeks to do so by establishing a scheme of carrier liability. The Act has been the subject of intense debate within the Internet industry with many commentators criticising the approach taken. Key criticisms raised against the Act are that it imposes liability on the wrong people and that it does not achieve its stated objective.

On 30 September this year, the Australian Senate passed a motion reflecting a range of criticisms relating to the *Online Services Act*. The motion also stated that the Senate recognised the most appropriate arrangement for the regulation of Internet content is the education of users, the empowerment of end-users and the application of appropriate end-user filtering devices.

This article provides an overview of the various schemes available to prevent access by children to inappropriate material.

PICS

The Platform for Internet Content Selection (PICS) was developed by the World Wide Web Consortium (W3). PICS is an Internet protocol which allows ratings to be transferred and understood across the Internet. The software has two components - a rating system to classify content and software that uses ratings systems to filter content. PICS enables two approaches for rating of sites: self-rating and third-party rating. Once a site is labelled in a certain way, end users are then able to block material entering their computer if the material has a rating which is not acceptable. Users are able to examine each category of rating in order to choose a preferred level of information to be received for that category. Users are effectively able to define their own ratings standards. For example, a filter can be set with a value from 0 to 4 for a number of categories. Under the RSACi scheme, there are only four categories – Violence, Nudity, Sex and Language. Under one particular scheme, the "Violence" category the rating runs from "No Violence" to "Wanton and Gratuitous Violence".

Possible inaccuracy of self-ratings as well as the vast number of sites that remain unlabelled make this system problematic. All material that is