puter hardware/ software (such as back up tapes) on which emails may be stored.

Where email is used to communicate concerns about performance or conduct to the employee directly or to notify them of counselling meetings, care must be taken to ensure that the email system does not substitute for direct access to, or communication with, the employer. To do so may allow the employee to allege that they were placed at some disadvantage, for example, by preventing them from fully and frankly discussing their performance with the employer, thereby impeding their ability to meet their employer's expectations or address their concerns.

Opportunities

Emails are important, but often ignored, pieces of documentary evidence in employment law cases. The Evidence Act provides for emails to be regarded as documentary evidence: see s.4.

Emails may be a source of evidence for employers seeking to establish the conduct of employees and their intentions. Emails prepared by employees in the course of employment entitle the employer to access the employee's emails. Employers often forget to consider emails of staff who have been terminated and later bring a claim against them. Failure to do so may mean that an employer fails to consider all relevant information in its defence of a claim, as increasingly more internal communications are via the email rather than by traditional paper records maintained on files.

It has long been accepted that an employer may justify a dismissal retrospectively by relying on information not known at the time of the dismissal but discovered subsequently: see for example Shepherd v Felt and Textiles of Australia Limited (1931) 45 CLR 359 and Byrne & Anor v. Australian Airlines Limited (1995) 185 CLR 410 at 463 per McHugh and Gummow, JJ. Accordingly, it may be that information discovered by an employer in a former employee's email records may lead to a chain of enquiry that established further misconduct that can be relied upon by an employer.

E-mail transmissions to clients - a lawyer's duties

By Tim Jones, solicitor at Gilbert & Tobin and Michael Rudd, articled clerk, Minter Ellison.

With the steady advance of the information age, clients are beginning to demand instant electronic communication with their lawyer, commonly via e-mail.

In providing advice to clients by e-mail, lawyers may be exposed to legal proceedings brought by clients in cases where sensitive material falls into the wrong hands or is tampered with to their detriment.

This article draws attention to the lawyer's potential exposure to liability to a client in providing advice by e-mail, and examines the following issues:

- what 'e-mail' is and how it works;
- security issues;
- security measures;
- implications of failing to implement security measures; and
- disclaimers and e-mail policies.

What is 'e-mail' and how does it work?

E-mail is simply 'electronic mail'. It allows lawyers quick written communication with clients and lets them attach application documents (such as Word, Word Perfect and Excel) containing, for example, contracts and pleadings.

E-mail typically works as follows:

- The sender writes the message on his or her computer. By way of a dial-up modem connection, the data is sent to the mail server of his or her Internet Service Provider (ISP).
- The sender's ISP sends the e-mail out into the Internet, with larger messages split into smaller data packages that each search for the fastest way to the ISP of the addressee. In transit, the packages pass through the computers of numerous third parties, which forward them to the addressee.
- The ISP of the addressee receives the e-mail and stores it on its mail server, with the addressee usually receiving a notification of the messages arrival in his or her 'in-box'.
- The addressee connects to the mail server of the ISP and downloads the waiting message to his or her computer in order to read it.

Sensitive material

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

- In the autumn of 1993, a student at Dartmouth University sent out forged electronic mail advising that a mid-term exam in Professor David Becker's course on Latin American politics was cancelled because Becker had a family emergency. The message was sent at 11:00 pm the night before the test and, as a consequence, only half the class showed up for the exam the next morning.
- In October 1994, somebody 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 his research grants were put in jeopardy as a result of the incident.

It is easy to imagine security breaches similar to the above examples taking place in a legal context. Sensitive legal material that may be exposed includes a client's financial details, commercial or litigation strategy, adverse evidence in a criminal matter and commercial information (such as tender, merger/acquisition details and prospectus details).

Security issues

The Internet is not a secure medium, due mainly to the fact that Internet communication channels are shared. Basically,

Continued over.

that means e-mails can be intercepted and read or tampered with by third parties on the Internet. Security risks with respect to sensitive client information involve primarily integrity and authentication. Integrity has to do with whether the e-mail (plus any attachments) which reaches the client has been already read and/or tampered with, while authentication has to do with whether the e-mail the client has receives was actually sent by the person named as the author.

'Eavesdroppers' or 'spies' - those who breach e-mail integrity and authentication - are known as 'hackers', 'crackers', 'spoofers' or 'sniffers'.

Hackers engage in unauthorised entry to, or modification of, computer systems. Their main purpose is to alter the system so that they can access it at a later date for whatever means they wish. Crackers, on the other hand, are the Internet equivalent of vandals - they break into the system and damage files.

Spoofing involves an e-mail being intercepted on the Internet and tampered with without the sender's knowledge. That e-mail's recipient might then act upon the spoofed e-mail to his or her detriment. The sender has no way of checking 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, except that the sniffer reads the e-mail only and does not tamper with it. When the e-mail reaches the intended recipient, whose privacy has been invaded, that person is none the wiser.

Security measures - digital signatures and encryption

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

Digital signatures - the electronic equivalent of handwritten signatures - 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. A digital signature allows the recipient to verify the authenticity of the document. Any change, however minor (a single space inserted into the document, for instance) will change the digital signature. If the contents of an e-mail 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.

Using a digital signature involves a public key and a private key: the digital signature is created by the private key and verified by the public key. Prior to sending a message, the author of that message provides the proposed recipient with the public key - basically a small software program containing a code paired with the owner of the private key. To verify a signature, the recipient's public key software calculates the digital signature code of the sender - if the message digest and signature block are identical, the signature is valid.

Certification authorities (CAs) are third parties whose purpose is to hold public key information so that the identity of people sending public keys can be verified by recipients (in the future, law firms may well become CAs, regulated by a state agency for quality control and key integrity).

Encryption involves an entire message (rather than just the signature) being scrambled by the private key, such that it can only be unscrambled by use of the paired public key. Encryption is therefore an effective way of preventing sniffing, and perhaps more useful than a digital signature when transmitting sensitive material via e-mail.

E-mail security software is inexpensive, easy to use and readily available. For some examples, see the Web site of The Law Society of WA.(1)

Standards and legislation regarding the use of digital signatures

The *Electronic Transactions Bill 1999* was introduced into federal parliament on 30 June 1999. Currently, the subject of debate, it 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 because it took place by way of electronic communication.

On 17 September 1999, Senator Richard Alston, Federal Minister for Communications, Information Technology and the Arts, announced the membership of the National Electronic Authentication Council, a peak body to oversee the development of a national framework for electronic authentication of online activity.

The Council aims to provide:

- a national focal point for authentication matters, including coordination of authentication-related activities at both a national and international level;
- advice to Government on authentication and related matters;
- a guideline for the development by industry bodies and Standards Australia of a framework of technical standards and codes of business practice on authentication matters; and best practice information and advice to industry in respect of authentication matters.(2)

In the near future, the federal government is expected to draft legislation dealing with a uniform public key infrastructure. It is anticipated that the legislation will address uniformity of authentication technology, the apportionment of liability for security breaches, and standards for CAs.

Implications of failing to implement security measures

Lawyers who fail to implement the necessary security measures expose their e-mail to a possible security breach. As a result, clients may lose legal professional privilege over the e-mail (and attachments) or suffer damage resulting from improper use of the e-mail. Such clients may then have grounds to seek damages from the lawyer in contract, in tort or in both. Perhaps the most relevant causes of action would be:

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

Clients may also have grounds for professional sanctions against their lawyer for failure to implement necessary security measures.(3) This article, however, does not attempt to address that 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.(4) 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.(5)

Legal professional privilege covers:

- confidential communications between the lawyer and client; and
- documents made for the sole purpose of legal advice or to be used in anticipated or existing legal proceedings.(6)

E-mail can be 'privileged'

E-mail communications can potentially satisfy both of the above requirements. Prima facie, privileged communications include any communication between the lawyer and client via e-mail.(7) They may also include any printed copy of an e-mail or attachment which in itself is privileged(8) and may include any printed copy of an e-mail or attachment that is non-privileged(9).

A fundamental requirement of legal professional privilege is that the communication must be confidential (10)(that is, it took place in circumstances of confidentiality(11)). Privilege may not arise where a communication takes place between the lawyer or client in the presence of third parties (12)(but see R v Uljee, below) or where it deals with events or knowledge already in the public domain (13).

Unless there are unusual circumstances in which 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, such a policy allows the employer to 'monitor' staff e-mail. It may be that the client should be aware of such unusual circumstances and so will lose any privilege that would otherwise attach.

The Australian position

It is uncertain whether the Australian position will support privilege in respect of 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 it has not received support in Australia.(14)

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) The remedy sought is usually an injunction preventing its disclosure.(17)

Another relevant consideration is that a document 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.(18) The same may apply to documents disclosed in, or attached to, an e-mail (for example, scanned documents, draft documents).

The New Zealand position

In the New Zealand Supreme Court's decision in *R v Uljee* (19), McMullin J made the following comment:

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.(20)

In that case, a police officer overheard a conversation between a lawyer and client while standing outside the door of the room they were in. Neither lawyer nor client was aware that the officer was listening to the 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.

On this reasoning, e-mails may attract privilege despite being intercepted by a person taking deliberate steps to do so. But what 'careful and deliberate steps' to keep the e-mail secure are sufficient to support a claim of privilege? The implementation of security measures for e-mails may be a sufficiently 'deliberate and careful step', but it is uncertain whether anything less will suffice.

Breach of confidence

Lawyers have a duty to their clients to protect any confidential information obtained from their client.(21) This duty of confidence, which is based in a combination of contract law and equity, arises from the peculiar relationship of lawyer and client (22) and is also found in the professional rules of each state.(23)

The standard imposed by the courts on lawyers to maintain client confidentiality "in the eyes of the law the very highest... [and] higher than it would be practicable to exact from persons in other types of confidential relations".(24) The duty is much broader than that relating to legal professional privilege, as it potentially applies to all communications and documents passing between solicitor and client(25). Confidentiality should therefore apply to most solicitor and client e-mail communications. It has been suggested that the only conduct required to fulfill 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.(26) The recipient must then act conscientiously and the duty not to disclose without authorisation should apply. What measures are reasonable to put an unauthorised e-mail recipient on notice? In light of the high standards of confidentiality expected of lawyers, a written warning on the e-mail may not be enough.

Disclaimers and e-mail policies

Some law firms have been attempting to shift liability for e-mail security to either the client or employees. Methods used commonly include the following:

- a standard disclaimer warning the client to rely on an e-mail only if the advice is confirmed by a signed, hard-copy letter from the firm, with the e-mail checked against the hard-copy letter and confirmed;
- a standard warning on e-mails that its contents may be privileged and confiden-

Continued page 22

Family Court of Australia Practice Direction: No 3 of 1999

Applications to the court arising from traditional and customary adoption practices - Kupai Omasker

Despite any other provision of the Family Law Rules applications for parenting orders concerning residence, contact and specific issues as a result of traditional and customary adoption practices by Torres Strait Islanders (Kupai Omasker) are to be made pursuant to a Form 8 supported by an affidavit substantially in compliance with the proforma affidavits entitled:

"Kupai Omasker (affidavit of applicant)"
"Kupai Omasker (respondent's affidavit)"

Information sheets have been developed to assist in completing the affidavits:

"Kupai Omasker - Torres Strait Islander Traditional Adoption Information for Applicants"

"Kupai Omasker - Torres Strait Islander Traditional Adoption Information for Respondents"

Background information about Kupai Omasker is also available in an information sheet entitled:

"Kupai Omasker Traditional Torres Strait Islander Child Rearing Practice"

These documents will be available from Court Registries in the usual way from 4 January 2000. The purpose of the proforma affidavits and information sheets is to assist Court users and improve the focus of the information put before the Court in support of these applications. As from 1 January 2000 affidavits of this type must be used in such applications and responses.

In order to contain the amount of material and the costs associated with bringing such applications to Court it is not intended that where there is a consent agreement for the orders sought that any form other than a Form 8 and supporting affidavits will be required to be filed.

In any cases in which there is not a consent for orders to be made involving traditional and customary Torres Strait Islander practice the prescribed Rules of Court as to the preparation and filing of and affidavits will apply. To protect the privacy of the families and child involved in these matters the certification signed and sealed by the Court will be issued to the applicants in cases where orders are made.

E-mail transmissions to clients cont from page 15

tial and unauthorised use is prohibited;
• a firm e-mail policy that prohibits employees from transmitting confidential information via e-mail;
The above measures may not be enough to protect a firm from liability in respect of sniffing or spoofing of e-mail. It is likely that a court would look at whether reasonable security measures were taken by a firm to avoid the act that caused the client damage (see 'Breach of confidence' above).
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 ignored with the firm's actual or constructive knowledge. An e-mail policy would require 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 'Breach of confidence' above).

Conclusion

To date, most e-mail security measures introduced to date by lawyers are 'stop gaps'. In light of the high standards of confidentiality imposed on the legal profession, the prudent lawyer should take steps to maintain the highest reasonable 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 the sending of such information via e-mail. However, clients will probably expect e-mail communication with their lawyer as a matter of course, so this is likely to be a short-term measure only.
Another available option is to use e-mail security software, such as encryption and digital signature software. Given that the software is inexpensive, readily available, simple to install and easy to use, this may be the prudent course of action.

This article was reprinted with persmission from Brief, the journal of the Law Society of Western Australia, Volume 26, No.9, October 1999.

Acknowledgement

The authors acknowledge the assistance of Simina Gougoulis in preparing this article

Notes

1.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)
2.see http://www.dcita.gov.au
3.Sections 28A(1) (b) and © of the Legal Practitioners Act 1893 (WA).
4.*Commissioner of Taxation (Cth) v Citibank Ltd* (1989) 85 ALJR 588 at 596; 20 FCR 403 at 414, per Bowen CJ and Fisher J.
5.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'
6.*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.
7.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)
8.*Cole v Elders Finance & Investment Co Ltd* [1993] 2 VR 356.
9.*Propend Ltd v Commissioner of the Australian Federal Police* (1995) 79 A Crim R 453.
10.*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;
11.*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.
12.*R v Braham & Mason* [1976] VR 547.
13.*J-Corp Pty Ltd v Australian Builders Labourers Federated Union of Workers-West Australian Branch* (1992) 110 ALR 510.
14.*Baker v Campbell* (1983) 153 CLR 52 at 67 - 68 per Gibbs CJ.
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. See also: 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.*Attorney General (NT) v Maurice* (1988) 161 CLR 475, which distinguished between full disclosure and a mere reference to a document.
19.[1982] 1 NZLR 561
20.*R v Uljee* [1982] 1 NZLR 561 at 576, per McMullin J.
21.*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.
22.Dal Pont,GE; *Lawyers' Professional Responsibility in Australia and New Zealand*; 1996; p21323.
Rakusen v Ellis, Munday & Clarke [1912] 1 Ch 831 at 840, per Fletcher Moulton LJ.
24.*Rakusen v Ellis, Munday & Clarke* [1912] 1 Ch 831 at 840, per Fletcher Moulton LJ.
25.By virtue of the equitable doctrine of confidential information
26.Paul McGinness, 'The Internet and privacy - some issues facing the private sector', *Computers and Law*, June 1996, p26