Such problems can arise where any regulated activity takes place in an online environment).

Sensible legal opinion advocates a system of self regulation in respect of Internet activity rather than attempting to overcome jurisdictional problems through the establishment of international laws[6]. However, in view of the problems which arise when a government purports to regulate the activities of persons located beyond geographical borders of that government, some attempt needs to be made to reach an international consensus on the extent to which governments can do so. This will be no easy task given the glacial speed of the international treaty process, but it is a task which must be undertaken as the Internet will be with us forever in one form or another. The urgency of this task will become more acute if, as seems likely, governments of other Australian states and of other countries continue to attempt regulation of Internet activity.

1 "The Age" (Melbourne) 20 July 1999 "Net betting set to soar"
2 Bernadette Jew "Cyber Jurisdiction - Emerging Issues & Conflicts of Law When Overseas Courts Challenge Your Web" "Computers & Law" No 37, December 1998, p 24
3 See David R Johnson and David G Post in "Law and Borders - The Rise of Law in Cyberspace" http://www.cli.org/X0025_LBFIN.html
4 Dan Burk "Jurisdiction in a World Without borders", at par 5, http://vjolt.student.virginia.edu/graphics/vol1/vol1_art3.html
5 "Holocaust Web site in legal debate" "The Age" (Melbourne) 17 April 1999
6 Bernadette Jew, op.cit. n (i)

Understanding the Technology Legislation Onslaught

Rita Chowdhury & Christopher Wood, Young Lawyers Information Technology Committee

Computers and the Internet have received little legislative attention in the past. Traditionally, Governments have applied band-aids to existing legislative regimes rather than deal with the specific legal challenges thrown up by new technology. Suddenly, the rate at which the Commonwealth Government is introducing technology legislation makes it hard for practitioners to keep up. This article sets out the status and effect of the technology legislation that has recently been proposed or passed and looks at some of the implications of that legislation.

BROADCASTING SERVICES (ONLINE SERVICES) ACT 1999

Following a great deal of media attention, the changes to the Broadcasting Services Act to regulate 'adult material' on the Internet became law on 16 July 1999. The legislation is based on the premise that 'what is illegal offline should be illegal online'. The amendments come into effect on 1 January 2000.

Under the new scheme the Australian Broadcasting Authority (ABA) will have the power to order parties to remove or block Internet content of an adult nature. Classification of Internet material will be done by the Classification Board under the National Classification Board standards that are currently used for television, film and video games. Material that is classified Xor Refused Classification (RC) or classified R without a mechanism for verifying that the reader is an adult can be the subject of an order under the scheme (called 'prohibited content'). The Classification Board is required to take into account the literary, artistic and educational merit of the material, its general character (including whether it is of a medical, legal or scientific character) and the persons or class of persons to or amongst whom it is published. It is not just pornographic material that will be caught by the scheme, for example an article explaining how to get away with shoplifting was refused classification by the Board.

The legislation only covers content that is stored electronically and accessible to the public (both within and outside Australia). This means that it will cover technologies such as the World Wide Web, but not email, Internet telephony or chat rooms. Importantly, there is no onus on Internet Service Providers (ISP's) to actively monitor content being accessed through their service. Instead, the Act provides for a complaints-based regime where the ABA will investigate complaints about Internet content and make orders under the Act if the material is found to be prohibited.

The manner in which the ABA will deal with prohibited content will depend firstly on whether the material is stored in Australia or overseas and secondly on whether it has already been classified. Where prohibited content is stored in Australia and its classification brings it within the meaning of prohibited content, the ABA will have the power to issue an order (referred to as a 'take-down notice') requiring the host to remove the material. Where the material has not been classified but the ABA believes it would be likely to be prohibited content if classified, it

will have the power to order that the material be removed until such time as it is classified (referred to as an 'interim take-down notice').

Where the ABA investigates material that is hosted outside Australia and finds that it is prohibited, the ABA has the power to order all ISP's to take reasonable steps to prevent their customers accessing that material. This applies to both material that has been classified and is rated X or RC and material that has not been classified but the ABA believes would be rated X or RC if classified. The ABA has no power to make blocking orders in relation to overseas content that is or would be rated R, which (in light of the fact that the vast majority of pornography is hosted overseas) raises serious questions as to why the ABA will have take-down powers in relation to R rated material hosted in Australia.

Exactly what comes within the meaning of 'reasonable steps' will be a major point of contention. The Act does, however, proscribe some matters that must be taken into account in determining what is reasonable. These include the technical and commercial feasibility of a course of action, the financial and administrative burden on the ISP and the overall intention of Parliament to encourage the development and application of Internet technologies.

Contravention of an ABA order will be a criminal offence and a continuing offence for each day the contravention continues, each punishable by a fine of up to $5,500 for an individual and $27,500 for a corporation. For flagrant or recurring breaches, the ABA will be able to apply to the Federal Court for an order that an ISP cease providing an Internet service or an Internet content host cease hosting content.

Bodies and associations that represent sections of the Internet industry may develop industry codes of practice (in consultation with the ABA) to ensure that any compliance arrangements take account of the needs and capabilities of all sections of the industry. One area that will be dealt with under codes of conduct is the use of technologies and procedures for blocking notified overseas-hosted material.

The decisions of the ABA will be reviewable by the AAT. There is also a procedure for reviewing decisions of the Classification Board. However, neither the Act nor the explanatory memorandum give any indication of how the ABA or the Classification Board will handle the huge increase in workload. Without some additional resources, it seems that the entire scheme will fail from an administrative point of view.

The Act represents a complete abandoning of the self-regulatory scheme that was proposed by the Government in 1997. That scheme was designed (at least in part) to encourage Internet users to adopt procedures enabling them to filter out what they considered to be unsuitable content. This was primarily achieved through the use of various filtering programs such as Net Nanny, and did not present the seemingly insurmountable technical hurdles that the Act presents. Unfortunately, that scheme was abandoned in circumstances that had more to do with the balance of the Senate than the Internet or pornography.

The Act has been highly criticised by Internet and legal communities, primarily because it represents a movement from the traditional independence of the Internet to Government control. It is doubtful whether it is even technically possible to block overseas content in most circumstances. There is no doubt that adult material will be easily available to experienced internet users, but it seems that the Government is satisfied with making the political statement that underpins the Act.

Resistance to Internet censorship has been even stronger in the USA where the Communications Decency Act (which sought to regulate online content) was challenged by the American Civil Liberties Union (ACLU). The ACLU challenged the constitutional validity of sections of the Act which made it a criminal offence to broadcast "obscene or indecent" and "patently offensive" material via the Internet. These sections were found by the US Supreme Court to violate 1st Amendment (Right to Freedom of Speech): See Reno (Attorney General of the USA) v ACLU[1]. There is, however, no '1st Amendment' basis under which Australians can challenge this Act. We now stand with China and Singapore as the only countries in the world that seek to censor the Internet.

Those who work in the Internet industry or who publish material via the Internet should be advised to start taking measures to ensure that they are prepared when the regime comes into force on 1 January 2000. Prudent preparation will include having material classified, adopting or developing a code of practice, and (in the case of ISP's) setting up a system for blocking prohibited overseas sites.

YEAR 2000 INFORMATION DISCLOSURE ACT 1999

To encourage business to share information on the Year 2000 problem, the Commonwealth Government introduced the *Year 2000 Information Disclosure Act* 1999. The Act, based on 'Good Samaritan' legislation in the United States, protects parties from civil litigation for statements relating solely to Y2K processing, bug detection, problem prevention remediation, contingency planning or the consequences or implications of Year 2000 problems.

To attract the protection of the Act, the statement must:

(a) contain a statement that it is a Year 2000 disclosure statement under the Act and that the author may be protected from liability;

(b) be made after 27 February 1999 and before 1 July 2001;

(c) identify the person authorising the statement; and

(d) be in writing, stored on a data storage device capable of reproduction in writing or be made by electronic communication (eg email).

The protection extends to some republications of such statements.

The exceptions include known or reckless false and misleading statements, statements made to induce customers to buy the product in question or statements made under an existing obligation.

For constitutional reasons, the statements covered are limited to those involving corporations and Commonwealth authorities and statements sent by post or electronic transmission. New South Wales has now enacted corresponding legislation which, although only recently passed, is deemed to have commenced on the same day as the Commonwealth Act (27 February 1999).

The Act contains a presumption that it does not amend contracts, and imposes an obligation on the Minister to table a quarterly report on the Y2K compliance of Commonwealth entities. The Act also contains an exception to section 45 of the *Trade Practices Act* so that parties assisting one another in accordance with the legislation cannot be prosecuted for anti-competitive conduct under that provision.

The Act attempts to facilitate the resolution of Y2K-related problems by providing a framework for co-operative disclosure. Surprisingly, very few companies have made use of the new provisions and it is quite possible that the Act has simply come too late.

ELECTRONIC TRANSACTIONS BILL

The exposure draft of the Electronic Transactions Bill was released in January this year. Following the receipt of submissions, the Attorney-General's Department made some minor amendments and introduced the Electronic Transactions Bill 1999 into Parliament on 30 June 1999. The Bill is based on the UNCITRAL Model Law on Electronic Commerce.

The main aim of the proposed legislation is to encourage the use of electronic communications in commercial dealings. Where a Commonwealth law places a requirement on parties that is paper-specific (such as document, record signature or writing) the requirement is taken to have been met by an electronic communication if the criteria set out in the Bill are met. The Bill does not, however, affect evidence legislation or the practice and procedure of any court or tribunal.

For each of the paper-based terms that are covered by the Act (document, signature, writing and record) there are criteria set out to determine in what circumstances the electronic equivalent is acceptable. For example, in the case of retention of records, it must be reasonable to expect that the electronic record would be accessible for future reference (ie adequately stored so that it can be retrieved). In the case of a requirement for a written document, there must be an appropriate method of assuring the integrity of the document (ie ensuring that it is not tampered with or corrupted).

In the case of non-Commonwealth Government bodies, the recipient's consent to the use of the electronic communication is required. This limitation, which was not in the original exposure draft, means that the uptake of electronic communications will not be forced on parties by reason of the new legislation. Where the body is a Commonwealth Government entity, consent is not required but that entity can specify particular technical requirements (such as the type of software to be used). This does raise concerns about whether the Commonwealth has too much influence in determining which technologies and paradigms will be adopted in Australia's uptake of e-commerce.

While the Bill does set out circumstances where the use of a digital signature meets a Commonwealth requirement for a signature, it does not have a regime for the authentication of digital signatures. For a digital signature to be effective in identifying a person, there must be a way of verifying who holds the digital signature. The way this usually works is that a trusted third party issues a digital certificate which verifies the relationship between the signature and the person. In the author's opinion, this requires some kind of regulatory regime to be effective. This is one of the major challenges for lawmakers in the e-commerce field, and one that is being currently addressed by the National Office of the Information Economy under the Gateway scheme (www.gpka.gov.au).

(Editor's note: This legislation was passed shortly prior to printing).

COPYRIGHT AMENDMENT (DIGITAL AGENDA) BILL 1999

Digital technology and the growth of computer networks, particularly the Internet, have posed challenges to the protection and enforcement of copyright throughout the world. The purpose of this Bill is to revise copyright law so that it is applicable to the online environment. The Bill is still at the exposure draft stage and is in the Prime Minister's list of bills to be introduced in the current parliamentary term.

The Bill introduces a broadly-based right of communication which includes the technology-neutral right of electronic transmission to the public and a right of making available online to the public (both within and outside Australia). This new right replaces the existing broadcasting right and cable diffusion right, but the right in the published edition of a work is not affected. This broad-based transmission right brings Australian law in line with international standards adopted in the 1996 WIPO Copyright Treaty and Performances and Phonograms Treaty These treaties provide for new international copyright standards to improve copyright protection in the online environment.

The Bill proposes that the existing fair dealing exceptions should apply to the proposed right of communication to the public. The *Copyright Act* in its current form prescribes that copying up to 10% of the number of pages of a

work for the purpose of research or study is an example of a 'reasonable portion' and therefore the fair dealing defence will apply. Under the proposed legislation this will be extended to 10% of the number of words of an electronic work. However, the draft Bill specifies that the fair dealing defence is only available for an electronic version of the work where a hard copy of the work exists and is not conveniently available to the user. The decision not to extend the fair dealing defence to material which only exists in electronic form was, according to the explanatory memorandum, made to prevent excessive free copying of the contents of electronic resources.

Temporary copies made in the course of the technical process of browsing or viewing material on a computer screen will not be a breach of copyright under the new provisions. This change is necessary to confirm the position that the automatic copying into a computer's memory that takes place when browsing the world wide web (caching) is not a breach of copyright.

The Bill introduces new measures aimed at preventing breach of copyright. These provisions include civil remedies and criminal sanctions relating to dealings in 'circumvention devices' (any device which is primarily for the circumvention of protection measures such as software 'locks'). Civil remedies and criminal sanctions will also be available for deliberate tampering with the electronic equivalent of a watermark material which is electronically attached to the work and contains details of the copyright owner and terms and conditions for use of the material While it is difficult to see from the Bill how these measures will be enforced, ISP's are protected from liability for breach of copyright where its service is used merely to access the material and it is not responsible for the material itself. This covers the situation where the ISP provides the link to the Internet but does not have any control over the web page its customer publishes on the Internet. An ISP will continue to be responsible for copyright breaches where they determine the content.

The protection for ISP's will not be absolute because, as the Attorney-General points out in the comments to the Bill, ISP's do have some control over web sites they host. ISP's will be liable where they have authorised someone to breach copyright. The draft Bill provides a list of factors to assist in determining whether a person authorises an infringement of copyright including whether the ISP is able to prevent the infringement and whether it took reasonable steps to prevent the infringement. The exact extent of an ISP's potential liability for copyright infringement will depend on the final form of this provision and the way in which the courts interpret the criteria.

One thing that is clear from the draft Bill is that the mere provision of physical facilities will not amount to the exercise of the right of communication to the public. This will overcome the problem in the *APRA v Telstra*[2] case where Telstra was found liable for the playing of music on hold by its subscribers to their clients (even though Telstra had no control over the content) because they were held to be a 'diffusion service'.

The amendments have been a long time coming and are necessary to give copyright the most basic workability in the online environment. It remains to be seen whether the outdated copyright concepts are a workable way of protecting the rights of online publishers.

COPYRIGHT AMENDMENT (COMPUTER PROGRAMS) ACT 1999

The Copyright Amendment (Computer Programs) Act 1999 was given royal assent on 24 August 1999. The Act aims to allow users of licensed software programs to decompile computer software for particular purposes.

The process of decompilation involves taking machine-readable code (object code) and running it through a program to produce code in a computer language such as C or Java. The source code can be read and understood (and more importantly, changed) by people with a knowledge of that computer language. This involves making a copy of the program which, unless authorised under the licence, would be a breach of the *Copyright Act*.

The Act amends the *Copyright Act* by allowing users of licensed software to decompile software:

(a) in order to write another program to operate with that software (called interoperability). An example of this would be where you are writing an email program that needs to interact with a web browser such as Netscape;

(b) for testing or correcting the security of the program or its network to protect it against unauthorised access or sabotage. This would include protection from viruses and computer hackers;

(c) where the program does not operate as intended by the author or specified in the documentation and an error-free copy of the program is not reasonably available at an ordinary commercial price. This would include decompilation to remedy a year 2000 problem in the program in most circumstances;

(d) where that decompilation occurs in the ordinary running of the program; and

(e) for the purposes of studying the ideas behind the program.

The Bill also extends the copyright exemption for the making of a backup copy of a computer program to include backups made by licensees as distinct from just owners which is the situation under the current Copyright Act. The Act will also allow owners and licensees to use a backup copy and store the original.

Because a specific application of the decompilation contemplated by the changes will be the remedying of Year 2000 computer problems, the provisions, when enacted, will be

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