COMPUTERS & LAW

JOURNAL FOR THE AUSTRALIAN AND NEW ZEALAND SOCIETIES FOR COMPUTERS AND THE LAW

Print Post—PP233867/00008

Editors: Brendan Scott, Simon Pollard and Kent Davey
Number 36

ISSN 08117225
August 1998

Ecommerce: Novel issues in selling to the World—the Australian experience

Simon Pollard, Peter Leonard, Partners
& Vanessa Leong, Lawyer, Gilbert & Tobin

Part One: Introduction

Who knew our practices would all boom with Internet and electronic commerce issues?

Just three and a half years ago at a conference about electronic banking technology not one single paper even mentioned the Internet. Of course, electronic commerce is not a term of art even in the technology industries but rather is a very broad concept that denotes any transaction effected by electronic means, including facsimile, telex, Electronic Data Interchange, Automated Teller Machines and EFTPOS as well as Internet transactions.

This paper focuses mainly on commercial transactions over the public Internet (ie excluding closed or private networks, virtual private networks and private NAPs like those operated by InterNAP Network Services Corp in Seattle and Savvis Communications Corp in St Louis). This focus is determined by the consumer protection emphasis of the panel session to which this paper relates, since most (non-business) consumers engaging in electronic commerce are using the public Internet.

Focussing mainly (though not exclusively) on consumers is important because it is generally agreed that raising consumer confidence is a key dependency for further growth of the online

Continued on page 3 ☞

In this issue...

☞ *Continued from page 1*

marketplace into a truly mass market. This is true both within national boundaries and also internationally.

This paper outlines the Australian experience in online transaction issues, both in terms of regulation to protect consumers and in terms of issues for corporations which are using the Internet to market or sell their products or services.

Part Two: Selling via the Internet

Many of the legal issues associated with selling via the Internet are essentially the same as promotions that use other media such as television, magazines and newspapers. Areas that advertisers on the Internet should particularly consider in the Australian context include:

- vicarious liability for defamation by employees;
- infringement of someone else's intellectual property rights, including copyright and trademarks;
- misleading or deceptive conduct by a corporation in the course of trade, in contravention of Part IV of the *Trade Practices Act 1974*, or by natural persons in contravention of the equivalent State or Territorial uniform Fair Trading Acts (ie statutory passing off);
- compliance with any relevant industry Codes of Practice (such as the Banking Industry Codes of Practice and the Internet Industry Association *(Draft) Code of Practice* — latest draft 3 was released in February 1998); and
- compliance with any relevant government sponsored voluntary Codes of Practice (such as the *Distance Selling Code* adopted by the joint Minsterial Council for Consumer Affairs in October 1997).

There are a few basic differences between traditional advertising and marketing activities and those over the Internet which require consideration:

- Regular control procedures are often bypassed —Employees in most prudently managed corporations are used to and accept they must follow certain procedures when clearing ad copy for magazines or other written forms of

COMPUTERS & LAW

Editors

Brendan Scott
c/- Gilbert & Tobin
50 Carrington Street
Sydney 2000 Australia
Tel: (02) 9367 8964
Fax: (02) 9367 3111
e-mail: bscott@gtlaw.com.au

Simon Pollard
c/- Gilbert & Tobin
50 Carrington Street
Sydney 2000 Australia
Tel:(02) 9367 3103
Fax:(02) 9367 3111
e-mail:spollard@gtlaw.com.au

Kent Davey
c/-Australian Communications Authority
PO Box 13112, Law Courts
Melbourne VIC 3001
Tel:(03) 9963 6949
Fax:(03) 9963 6899
e-mail:kent.davey@aca.gov.au

Subscription: $32.00 per 4 issues

Advertisements: Inserts $300.00; for advertisements within the journal, rates and information will be provided by the Editors on request
Articles, news items, books for review and other items of interest may be sent to the Editors.

advertising. However, dissemination of information into cyberspace is available at the click of a mouse from an employee's desktop, facilitating and indeed encouraging easy circumvention of the usual control procedures.

- Constantly changing material — The problem with bypassed control procedures is compounded by the nature of websites, which are constantly updated, in many cases daily. The legal vetting demands are more akin to those of a broadcaster than traditional corporates. Accordingly, copy clearance policies and procedures should aim for continuous control and quality assurance, rather than the traditional method of one time review.

- Opportunity for realtime contracting and order execution — Unlike a static ad in a magazine, a website often provides an interactive interface with the consumer. This interface can range from merely providing the end user with an opportunity to make further inquiries about a product or service, to order placement or fulfilment facilities. Data protection and privacy concerns need to be considered: can customer information gathered through use of the web site be collated and used for cross marketing or sold to third parties. Procedures for contract conclusion and order execution requires consideration of law relating to electronic formation of contracts and consumer credit and consumer protection statutes. Tax issues raised by diverse requirements of different countries involved in a transaction, even for a simple retail sale, have not yet been adequately addressed by taxation authorities.

- Jurisdictional issues — Unlike other forms of media where the distribution territory is defined by the mode of distribution, eg physically, the Internet's territory is basically the world. It is not often clear whether material disseminated over the Internet is directed for use in a particular jurisdiction only. For example, if you are operating an on-line gaming service, what indications do you need to place on your website to indicate the markets from which consumers will be permitted to play on the site? If advertisements for goods must carry registration numbers or other indications as to suitability for use, in relation to which jurisdictions are these registrations or warnings to be displayed. Note that in general access to a site cannot be controlled by geographical location of the accessor. In any event, the location of parties accessing a web site often cannot be determined by the operator of the web site. Even where an address is passed with a geographical appellation — ie *spollard@gtlaw.com.au*, with the *au* suffix indicating an Australian registered domain name, the accessor may or may not be in Australia. Most web users use email addresses which are allocated by United States registration authorities and which are not geographically specific.

Litigation over jurisdiction has been a key element of the early United States litigation in relation to Internet services. Not surprisingly, courts looking at different transactions have come to different conclusions. In a number of cases courts have found that a service provider or content provider in a remote web site can be held liable under the law of the State where a person accessed the web site. Even if the only contact with the State in which the litigation is being brought is accessibility of the web site from that State, some US courts have held that the law of that State applies. Other courts however have found that more than merely offering or accessing a web site is required to ground jurisdiction, leaving the issue open for further litigation on this most fundamental of issues.

In the context of advertising a corporation's goods or services over the Net, each of the above matters will need to be considered. In addition, issues associated with links to other sites distinguishes the Internet from any other form of advertising however we will not be covering these issues here.

Part Three: The need for an electronic communications policy

In order to minimise the risks associated with this new platform for advertising and marketing, corporations should develop and implement an electronic communications policy. This policy should cover procedures for employees to submit copy for approval, procedures for continuous review, and provide examples of "prohibited" conduct so that the company can avoid vicarious liability for acts of its employees.

In some areas legal risks associated with electronic communications will differ markedly country by country. For example, most Australian States have comprehensive legislation dealing with racial and religious vilification. Many other Pacific Rim countries, whatever their cultural sensitivities to these issues, have little or no legal protection. The level of privacy protection, and the form of telecommunications interception laws, vary from inclusive to minimalist. For example, privacy law in New Zealand significantly curtails use that may be made of customer personal information gathered in whatever way, including over the Internet and including by private sector entities. Even where national laws are broadly similar, the risk exposure of employers country by country varies significantly as a result of different national or statute-specific legal theories of employer liability.

The extent to which local judge-made or statute law creates exposure to legal

liability for an employer in relation to acts of an employee depends upon the approach under local law to vicarious liability or statutory civil liability and criminal liability. Australian and New Zealand law in relation to the vicarious liability of an employer for the torts of an employee committed within the course of employment is complex and to a degree contradictory, but generally reduces to a question of whether the activity was reasonably incidental to the performance of authorised duties, in which case the employer may be vicariously liable in relation to the activity even if the activity is prohibited or involves so substantial a departure that the employee must be taken to act outside the employment.

The principle of vicarious liability may be contrasted with legal liability imposed because the employer is personally at fault — for example, where the employer authorises or ratifies conduct that is tortious — or unreasonably fails to control the conduct of an employee where it is reasonably foreseeable that harm may be sustained by a third party, or where statutory liability is imposed. Some statutes make the employer directly liable for the statutory or criminal breach, which may involve questions as to whether a corporation has requisite intent or *mens rea*. For example, an employer may be directly liable for a breach of copyright by sanctioning or implicitly approving a breach by an employee through inaction or failure to institute appropriate control or checking procedures. Many statutes in effect leave open the question of whether principles of vicarious liability should apply in relation to offences created by the statutory provisions.

For a risk minimisation strategy, corporate counsel's task in jurisdictions such as the Australian States and New Zealand is to endeavour to:

- expressly categorise certain conduct as "prohibited" and therefore outside the scope of the contract of employment, so as to avoid vicarious liability;
- institute appropriate policies and procedures to avoid direct liability under possible heads of liability, by ensuring that the corporation cannot be said to approve an employee's illegal act, or to countenance the committal of illegal acts through failure to direct and control the employee or otherwise to take effective steps to minimise the risk that these offences occur.

Both objectives will be difficult to achieve, but it will generally be easier to achieve the second objective than the first. To have a real chance of achieving both objectives under Australian law, it is probably necessary to expressly prohibit relevant conduct by description, and then ensure that contravention of the prohibition is expressed as a breach of the contract of employment.

Many corporations have already adopted marketing and advertising guidelines. Fewer corporations have developed comprehensive manuals covering communications procedures and policies, and fewer still addressed the Internet in those policies. Some subsidiaries of United States' corporations adapt and adopt manuals in use by their US parent. Unfortunately, these manuals are are generally illsuited to Australian workplace conditions and simply will not be read or observed by many Australian employees, who expect a direct style of communications coupled with reasons and examples.

A good electronic communications policy should include the following elements:

- An introductory statement as to why the recipient should take the time to read the document and discussing the status of the document. For instance, if the document is titled "guidelines", the document should make clear whether there are sanctions that will be enforced in the event of failure to comply with the guidelines, and if so, how those sanctions will be applied. (Of course, sanctions need to match statutory entitlements, agreed employment conditions and industrial awards.)
- A statement of permission for the corporation to monitor electronic communications, expressed so as to comply with local labour regulation, telecommunications interception and privacy laws.
- A statement of prohibition on transmittal or downloading of unacceptable or illegal content. This statement should specify the nature of unacceptable or illegal content in sufficient particularity as to be understood by a reader having regard to the reader's cultural background, level of language comprehension, and (perhaps limited) understanding of legal principles.
- A statement of prohibition on transmittal to external persons of any internal email message or other data prepared for inhouse use unless expressly authorised.
- A statement as to the corporation's requirements in relation to external e-mail or other postings to external addressees. This should include a simple explanation as to why communications cannot be considered anonymous even if not signed, about use of corporate identifiers, and about 'cookies' and other prospectively privacy invasive data collection by web site operators.
- A requirement to comply with corporate advertising and marketing guidelines where postings or other electronic communications relate to the corporation's products or services. The policy should, where appropriate, cross reference the corporation's policies in relation to these matters.

- A statement about the possible application of antitrust, fair trading and intellectual property laws in the country of posting and the country of receipt. This statement should also cross reference the corporation's fair trading and trade practices guidelines policies where appropriate.
- Specification of restrictions on download of material. This should state whether the restrictions are by way of absolute prohibition; or by reference to the nature or character of material downloaded; or by reference to whether the download is of executables or data files.
- Restrictions on, or requirements for, use of encryption or secure transmission channels for particular categories of content.
- Requirements for corporate warnings or notices as to privilege or confidentiality to be included in e-mails to external destinations.
- Where intranets or extranets are in use, statement of any conditions of access and/or preconditions before rights of access may be granted to third parties.
- A statement as to acceptable and improper uses of corporate system resources. These may include requirements for download to only specified machines and drives; prohibition on deployment of non-approved and/or unsupported software applications; and caution as to use of bandwidth hungry applications.
- The corporation's requirements for employees to maintain security (including passwords) and system integrity. This section of the policy should include simple examples of good and bad passwords and should be properly integrated with good system housekeeping which requires regular rotation of passwords.
- Caution to employees as to possibility of recovery of deleted files and their possible use in litigation.
- Requirements for user-defined backup and other record keeping requirements, together with a statement of the corporation's central document and file retention policies and procedures. This is necessary to ensure that employees do not abnegate personal responsibility for backup or retention by making incorrect assumptions about automatic or centralised procedures within the corporation. This may be important to ensuring that the corporation complies with local document retention requirements, such as under local taxing statutes.
- Restrictions on transfer f funds or on other transactions for value as set by the corporation's internal authority procedures and, where relevant, local foreign exchange, exchange control, or transaction reporting legislation.
- Guidelines about e-mail etiquette, including use of spellcheck, message length, content and format, appending of messages under reply and communications within a dialogue 'string' or 'thread'.

Other material may be appropriate for particular industry sectors: for example, securities dealers and investment advisers will need to take care to ensure that electronic communications conform with the extensive form and process requirements which apply under the Australian Securities Commission guidelines to those entities.

Part Four: Consumer privacy protection

Privacy in Australia at Federal level is governed by:

- the *Privacy Act 1988*;
- the *CAST Code of Conduct*; and
- the *Australian Privacy Charter* (a voluntary Code of Practice).

This paper deals only with the first of these.

The *Privacy Act* already extends (after much public debate) into the private sector. In fact, it extends to a larger class of persons than many think. Under the Act, a "credit provider" is defined to include a corporation determined by the Privacy Commissioner to be a credit provider. The Commissioner has determined that a credit provider is any corporation which sells goods or services and allows payment to be deferred for at least 7 days. As you can see, this applies to virtually every corporation in Australia (since common payment terms are 30 days from date of invoice). The consequence is that a private corporation can obtain personal credit information from credit reporting agencies about its customer in relation to the sale in question, but is bound by the *Privacy Act* in relation to its use of that information.

The Information Privacy Principles under the *Privacy Act* do not otherwise apply to the private sector. However, it is easy to see how the definition of a "credit provider" can catch unsuspecting companies with rules they are ill-prepared to comply with.

In September 1996 the Attorney-General's Department of the Federal Government released a discussion paper called *Privacy Protection in the Private Sector*. This paper recommended extension of application of the 11 Information Privacy Principles to the private sector in Australia. The paper suggested the development of industry codes of practices developed in consultation with the Privacy Commissioner and administered by

the industry, subject to statutory backing. These suggestions were adopted as part of the policy platforms of both major political parties. If enacted, they would have had a substantial impact on the ability of Australian corporations to store and use the personal information of individuals. However, on 21 March 1997 the Prime Minister of Australia, Mr John Howard, announced that the *Privacy Act* would not be extended to the private sector, citing a need to avoid the resulting "regulatory burden" on small business.

This has led to speculation that Australia's privacy laws will not satisfy international norms, such as the European Union's directive on transborder data flows. Information privacy is protected internationally by:

- the Organisation for Economic Co-Operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980);
- the Council of Europe's *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (No. 108 of 1981)* ("Council of Europe Convention"); and
- Article 17 of the *International Covenant on Civil and Political Rights*.

The *OECD Guidelines* and Article 17 of the *International Covenant on Civil and Political Rights* have been incorporated into Australian law under the *Privacy Act* 1988 as the Information Privacy Principles (IPPs) under that Act.

OECD Guidelines

The OECD Privacy Guidelines state that:

- Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Central to the OECD guidelines (and the IPPs under the Federal *Privacy Act*) is the principle of informed consent. That is, only using personal information for the purpose for which it was provided or some other lawful purpose to which the individual concerned gives his or her informed consent.

The OECD Guidelines were developed at a time when all you had to do to control a particular body of data was to identify a single record keeper. The convergence of technologies has led to an increasing number of personal linkages and means of transferring information on networks, and hence to the rapid diffusion of personal information. This lack of control appears clearly in the controversy surrounding a number of recent technological developments. Those developments include:

- calling line identification/ calling number display (the display of a caller's number on the phone of the person receiving the call);
- use of automated calling equipment for telemarketing; and
- reverse telephone directories (which are computerised directories for which a person's name and address can be identified from the telephone numbers and, in some cases, searches conducted to discover the names and telephone numbers of all persons in the same street or suburb).

Privacy as a legal constraint on cross-organisational data-sharing

Information in computer storage systems (even more so than manual storage) is particularly vulnerable to unauthorised access and misuse. This is because an individual generally does not know what information is available about him or her, who is accessing it and for what purposes. Also, an individual does not usually have the opportunity to verify and correct information about him or her; it is easier for errors to be introduced (whether inadvertently or on purpose) into computer databases and for those errors to be perpetuated and distributed.

In that context, the main factors which increase the likelihood of infringement of the Information Privacy Principles are:

- limited or poor security design and capability of the architectures;
- lack of integrity or lack of supervision of personnel who have access to the information;
- faulty or poorly maintained log-ons, password allocation and rotation systems and other identifier protocols;
- faulty or poorly maintained encryption systems;
- lack of regular or adequate monitoring;
- failure to take appropriate action when a security breach is detected and to publicise the action as a deterrent.

The EU Data Directive

The EU *Directive on Data Protection* (now being progressively adopted by EU member countries) imposes a number of requirements on the transfer of data between members and to non-member countries. Member countries are required to ensure a certain level of protection for temporary and permanent data and the Directive applies to both private and public sector entities. The requirements are similar to the Information Privacy Principles set out in the *Privacy Act* 1988 in Australia.

How might the EU Directive affect your business?

It would appear (because of the Federal Government's reluctance to extend the *Privacy Act*) that Australian privacy laws are unlikely to impact on the operation of a private sector website unless that operation is connected with the collection or assessment of personal credit information.

However, it is important to bear in mind the jurisdictional issues raised

earlier and consider overseas privacy laws. Further, privacy is increasingly under public scrutiny, particularly as many menders of the public view the Internet as privacy intrusive. Many Australian corporations are instituting privacy protection programs, as 'good corporate citizens'.

The risk for businesses operating in Australia is that the failure of the Federal Government to legislate to extend the *Privacy Act* to regulate the private sector (unlike in New Zealand, Hong Kong, the UK and elsewhere) means that Australian laws will not meet the requirements under the EU Data Directive. This may prevent European companies from transferring data to Australian companies, effectively placing Australian businesses at a comparative disadvantage.

Part Five: Ecommerce consumer protection national principles

While general privacy principles may offer limited protection to consumers in the electronic environment, the National Advisory Council on Consumer Affairs issued *Consumer Protection in Electronic Commerce Draft Principles and Key Issues* (October 1997) which aims to offer consumer protection in the buyer/seller relationship in the electronic age.

Although Australian consumers purchasing goods and services from sellers based in Australia are protected by the *Trade Practices Act*, they are not guaranteed such protections when dealing with suppliers outside Australia. The draft Principles were developed by reference to the United Nations *Guidelines for Consumer Protection* and the issues identified in the Organisation for Economic Cooperation and Development (OECD) publication *Distant Selling in a Global Marketplace: Codes of Conduct*, (DAFFE/CP[97]8), Paris, March 1997. The Principles are:

- Protection — Consumers using electronic commerce are entitled to the same protection as provided by the laws and practices that apply to existing forms of commerce;
- Identification — Consumers must be able to clearly establish the identity and location of businesses they deal with;
- Information — Consumers must be provided with clear and comprehensive information before and after any purchase of goods and/or services;
- Clarity — Sellers must state contract terms in clear simple language;
- Confirmation — Sellers should ensure they receive confirmed consent from consumers for a purchase of goods and/or services;
- Payment — Consumers are entitled to receive clear information about the types of payments which will be accepted;
- Complaints procedure — Consumers are entitled to have their complaints and enquiries dealt with fairly and effectively;
- Dispute resolution — Sellers should provide information to consumers about affordable and effective dispute resolution arrangements, where they are available;
- Privacy — Sellers must respect customer privacy;
- Code compliance — Industry code administration bodies must closely monitor the application and effectiveness of their codes and be able to correct any deficiencies which are identified
- Confidence — Each code operating body should strive to maintain and promote consumer confidence in the global marketplace; and
- Regulation — Governments should actively develop their consumer protection responsibilities.

The Principles are also reflected in the *Model Code on Distance Selling* launched in November 1997 by the Ministerial Council on Consumer Affairs.

The Principles are not intended by themselves to be enforceable, but the Council considers they should form the basis of rules or codes of practice which are enforceable by consumers both domestically and under co-operative international arrangements.

Part Six: Ecommerce legislative regulation

Expert Group Report

The Federal Attorney-General has just released the Report of his Expert Group on Electronic Commerce. The Expert Group was established to consider generally the legal issues arising from electronic commerce and to report on the form and scope of appropriate regulation, if any, of electronic commerce. The starting point was the issues raised by the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce.

The Expert Group's Report takes a minimalist position; namely, that legislation specific to electronic commerce should be considered only where absolutely necessary to facilitate the implementation, growth and conduct of electronic commerce in Australia. To this end, the Report recommends:

- legislation as the best option (above common law and regulation inter partes by contract) to resolve the legal issues raised by the Model Law and the UNCITRAL discussion papers that preceded the Model Law;
- a minimalist legislative model for digital signatures (ie rejecting the Utah model and more along the lines of the *Electronic Financial Services Efficiency Act* 1997 introduced into Congress on 8 November 1997 (the Baker Bill) — that Bill remains with the House

Committees on Banking and Financial Services, Commerce, Government Reform *and* Oversight, Judiciary and Science);

- that any legislation should be Federal (rather than State based, which would require co-operative enactment of uniform State laws to achieve the same result); and
- the legislative scheme should be technology neutral, with broad application (applying for example to data messages in trade or commerce and with government), again unlike the Utah model.
- that there should not be a general repugnancy exception to the digital signature legislation, but rather a series of specific exceptions related to particular instruments or transactions, together with a regulation-making power to introduce additional exceptions in unforeseen cases.
- in line with the UNCITRAL Model Law, there should be a balance between mandatory provisions and those which can be varied by agreement between the parties. Specifically, provisions based on Articles 5 to 10 of the Model Law should provided mandatory minimum standards, with variation from the remaining Articles subject to a reasonableness test.

The Expert Group's Report should be read in conjunction with the upcoming NPKI Working Group Report (discussed below) and the Standards Australia report on PKAF, and of course the Model Law itself.

NPKI Working Group Report

In late 1997 the Federal Government, through the Department of Communications and the Arts (DOCA) and the new interdepartmental National Office of the Information Economy (NOIE), established the National Public Key Infrastructure Working Group to examine issues relating to setting up a peak body for a public key authentication framework (PKAF).

At the same time, the Federal Office of Government Information Technology (OGIT) is preparing a report on Project Gatekeeper, which aims to rationalised voluntary mechanism for implementation of public key technology by Federal Government agencies.

Both of these initiatives are significant for public (consumer) confidence in the authentication, security and integrity of Internet transactions.

Part Seven: Protection of shareholders and investors as consumers of corporate information

I do not propose to go into detail about the requirements under the *Corporations Law*, but it is worth raising a couple of matters.

The *Corporations Law* requires that an organisation's Australian Company Number (ACN) or Australian Registered Body Number (ARBN) be displayed on all public documents. It is likely that a website will constitute a public document for these purposes, so we recommend including this information on your website after every mention of your company or registered body name.

There are also issues relating to putting securities information on the Internet, especially laws relating to issuing a prospectus and giving investment advice. Many of these are addressed in the Federal Government's Corporate Law Economic Reform Program (CLERP) Proposals for Reform: Paper No. 5 entitled *Electronic Commerce — Cutting Cybertape — Building Business (1997)*. That Paper proposes reforms to the Corporations Law in relation to electronic commerce which will:

- focus on the actual information required to be provided to the Australian Securities Commission (ASC), rather than on the format or physical media in which that information is stored;
- give the ASC greater flexibility to receive documents in electronic form;
- facilitate electronic communication between companies and shareholders and other consumers of corporate information via the Internet or other electronic media, and between the ASC and the public;
- facilitate the retention of company records only in electronic form;
- alter the current fee collection structure of the ASC to accomodate the use of communications technology; and
- recognise the financial market's netting practices.

Part Eight: Consumer protection through industry self-regulation

In place of failed attempts to impose prescriptive legislative requirements on the Internet industry, attention in Australia has turned towards greater self-regulation by the industry. Although most of the debate about Internet content regulation has focussed on obscene material, and therefore is generally not relevant to companies promoting their goods and services, there are some developments which are of broader interest.

The *Principles for a Regulatory Framework for Online Services in the Broadcasting Services Act* which were published for comment by the Federal Minister on 15 July 1997 endorse a self-regulatory approach, established in the Broadcasting Services Act and overseen by the Australian Broadcasting Authority (ABA).

Codes of Practice

The Principles provide for a tiered regulatory structure. The first tier consists of Codes of Practice to be formulated by the industry in conjunction with the ABA and other relevant bodies, and which would apply to the whole on-line service

provider industry or to any industry sector. Once the ABA is satisfied that a Code provides appropriate community safeguard, and there has been consultation on the Code, the ABA registers the Code of Practice.

Codes of Practice will cover matters such as reasonable procedures to prevent the on-line publication of content that would be refused classification under the general censorship guidelines where the on-line service provider is made aware of the existence of the objectionable material being hosted on their system. Codes will also address encouraging content providers to display appropriate warnings on material, ensuring on-line access by minors occurs only with parental permission, and the development of an Australian on-line labeling scheme. The provision of adequate information to users about content filtering software will also be covered in the Codes.

Where a consumer believes a Code of Practice has been breached, the first step is to complain to the on-line service provider. Where there is no reply or no satisfactory response the consumer can then request the ABA to investigate the complaint.

Service Provider Rules

The second tier of the regulatory scheme is the establishment of a set of service provider rules which may be contained in the *Broadcasting Services Act*, but which may also be determined by the ABA in the form of disallowable instruments. The rules will include, for example, that an on-line service provider may not knowingly allow someone to use their service to publish content that would be refused classification under the censorship guidelines or otherwise be illegal, and that an on-line service provider not use an on-line service in the commission of an offence.

Standards

The third tier of the regulatory scheme is the provision for the ABA to develop standards, which would apply to on-line service providers in relation to matters where a Code of Practice fails or when no Code has been developed. Again such determinations are to be subject to public consultation and to be disallowable instruments.

The three tiers of the regulatory scheme are also inter-related. Where a Code has not been developed, the ABA may request the industry body to develop a Code of Practice on particular matters. The ABA can also determine a standard where it is satisfied that the existing Code does not provide appropriate community safeguards, as long as the ABA has requested the body that developed the Code to address those deficiencies. The ABA may then determine an ABA standard about the matter to apply to a specified sector of service providers.

Complaints

A complaints procedure is also proposed for the legislation. Breach of a registered Code of Practice results in a complaint to the Code Subscriber concerned, including content providers and webpage developers. If there is no satisfactory response or no reply, a request can be made to the ABA to investigate the matter. Complaints about offences under the Act or a breach of a rule may be made directly to the ABA.

The Principles proposed by the Minister confirm the central role that the ABA will play in relation to on-line services. The ABA has the task of reviewing Codes to determine whether they provide appropriate community safeguards, receiving complaints on some Code breaches, developing standards and receiving complaints about breaches of standards, developing additional on-line service provider rules, and responding to possible offences by service providers who are breaching those rules, right up to the application for a Court order relating to a service.

Industry Code of Practice

The Internet Industry Association released a third draft of its proposed *Industry Code of Practice* on 2 February 1998. The Code aims to support a system for the classification of content on the Internet as well as management of access to content, and to set down standards for complaint handling in the Internet Industry.

The Code covers not just Internet service providers, those providing connectivity or hosting web pages, but also content providers, whether they are advertisers, vendors, information providers or someone who controls a web site, as well as software creators and web page developers. The Code is drafted to cover all participants in the industry who choose to agree to be bound by the Code and display the code compliance symbol.

All Code subscribers agree to general standards of conduct, which include not engaging in misleading or deceptive conduct or inaccurately representing the benefits of a product or services, or knowingly exploiting the lack of knowledge of Internet users. The Code also imposes secrecy obligations and limits the collection and use of data by Code subscribers, providing for example that data relating to users can only be used for marketing or billing purposes related to the provision of the service or other purposes to which the user consents.

Despite the fact that pornography and erotic material appears to be the primary concern driving the process of Internet regulation, the Code also establishes rules which relate to, for example, methods of payment chosen in relation to purchasers made over the Internet. Vendors are required to make certain information available to users, including offering the user cancellation of the order and a refund if delivery is not made within 28 days of the promised delivery date.

The degree to which the Australian scheme, whatever its final form, can be successfully imposed to restrict the conduct or material provided by service providers who are not located in Australia remains to be seen. In theory, the Code will apply to every Code subscriber service or content provider. In practice, enforcement will present new obstacles.

Responsibility of ISPs for Illegal Content

In the Draft Code of Practice and at law, there is no protection for service providers who host sites containing illegal material. "Illegal Content" is defined in the Code as "content, the mere possession of which is illegal under an applicable State, Territory or Commonwealth Law". However, if the service provider has taken reasonable steps to ensure illegal content is not transmitted by them, including if it becomes aware such material is available through them and they take steps to remove it, the service provider will not be liable.

Although the definition of "illegal content" does not cover misleading information, there is a separate principle governing conduct of all Code Subscribers stating that they will not inaccurately represent the benefits of their product or service, or engage in misleading or deceptive conduct within the meaning of the Trade Practices Act.

CONCLUSION

I noted at the start of this paper that many of the legal issues associated with advertising and marketing via the Internet are essentially the same as promotions that use other forms of media such as television, magazines and newspapers.

However, the characteristics of the Internet give rise to a number of novel concerns, and should particularly focus the attention of corporate counsel on the need for employee training and a continuous legal quality assurance programme. These programs need to be appropriately tailored to your corporation's activities and procedures. Their design and implementation does not require close familiarity with the underlying technologies, but should take account of issues associated with electronic commerce. The task is not huge, but relatively few corporations to date have given the task a high priority. No doubt electronic communications policies will suddenly become attractive once Internet-based litigation achieves a higher public profile in Australia, just as Year 2000 compliance strategies and programmes have suddenly come under corporate and public scrutiny.

The writers gratefully acknowledge the assistance of their colleagues Brendan Scott, Kate Harrison and Angus Henderson for their assistance in preparation of this paper.

The Liability of Internet Service Providers for Copyright Infringement in relation to Music Transmitted through their Networks

Karen Amos, Francis Abourizk Lightowlers

I Music and the Internet

A Introduction

This article discusses the potential liability of Internet Service Providers ('ISPs') for breach of copyright, in music passing through their networks. It begins by describing the availability of music on the Internet and how music is transmitted on-line, the participants involved in such on-line transmission (with particular emphasis on the role of ISPs and the level of control they have over their subscribers' actions) and the subsistence of copyright in music.

The potential liability of ISPs for direct infringement of copyright in music, by exercising the copyright owner's exclusive rights of reproduction, performance, broadcast and diffusion rights, is considered in light of the recent cases involving allegations by the Australasian Performing Rights Association ('APRA') of copyright infringement by Telstra[1] and OzEmail.[2] It is concluded that ISPs may be directly liable for the infringement of copyright in music transmitted through their networks.

This article then discusses the potential liability of ISPs for indirect infringement of copyright in music on the Internet pursuant to the law of authorisation and concludes that, in most instances due to ISPs' lack of control over their subscribers' actions, they would not be liable for authorising their subscribers' breaches of copyright.

Finally, this article looks at policy issues, international copyright developments and reform of copyright in the new communications environment. It is concluded that the *Copyright Act* 1968 (Cth) (the 'Act') should be amended to reflect developments in communications, that ISPs should not be directly liable for copyright infringements where they are merely acting as a conduit for the transmission of music and other material on the Internet and that the law of authorisation provides an appropriate and flexible measure of liability for ISPs for their contribution to copyright infringements in material passing through their networks.

B Music On-line

The Internet is a worldwide 'giant network which interconnects innumerable smaller groups of linked computer networks'[3], that is a