

THE CONCISE E-COMMERCE UPDATE

Shane Barber, Partner, Truman Hoyle Lawyers

INTRODUCTION

1. *Structure*

In this paper we will briefly canvass the existing law regulating e-commerce in Australia as well as look at the current trends and legislative developments occurring in this field of law.

As recently as the late 1990s much of the law described below was in its embryonic state, with legislature and regulatory bodies around the world scrambling to keep up with emerging technologies for communication and doing business. While the last 5 years has seen many of the gaps and uncertainties filled and addressed, e-commerce law is ever evolving to match the continuing change in technology.

In this paper we will look at 5 areas of law in particular which relate to e-commerce as follows:

- (a) electronic contracts;
- (b) jurisdiction issues;
- (c) online security;
- (d) online content regulation; and
- (e) intellectual property issues as they impact the online environment

We will conclude with a brief look at a current key online business focus, being online advertising and how it can be more effective.

2. *Current Internet Trends*

In a little over a decade, the Internet has not only connected people and opened up access to the world's information, it is rapidly becoming the planet's operational infrastructure. It is linking people, businesses and institutions, as well as billions, ultimately trillions of devices – not only computers, satellites and telephones, but also cars, medical and production equipment and household appliances.

It is at once facilitating and transforming transactions of all kinds – from commerce, government services, education and health care to entertainment, conversation and public discourse.

What is remarkable is just how quickly this is happening.

Consider in 1993 there were about 15 million Internet users. Ten years later, in 2003, there were 723 million. Six months ago there were 840 million. Today there are approximately one billion online users, three times as many as at the beginning of the decade.

What's significant is the remarkable potential for still further expansion as although the Internet's global reach is immense, only about 15% of the world's population is online.

On 12 August 2005, The Australian Bureau of Statistics released its latest *Internet Activity Survey* (“IAS”). The IAS is a census which collects details on aspects of Internet access services provided by internet service providers (“ISPs”) in Australia. The IAS contains results from all identified ISPs operating in Australia as at 31 March 2005 and the next survey will be conducted in March 2006.

The IAS identified, among other things, the following:

- While the total Internet subscribers in Australia increased during the period September 2004 to March 2005 by 4%, growth had slowed following a 10% increase recorded for the six months to the end of September 2004.
- The increase in overall subscriber numbers was again driven by growth in non dial-up subscribers with non dial-up subscribers representing 30% of total Internet subscribers in Australia at the end of March 2005 compared with almost 23% at the end of September 2004.
- Most of the growth for non dial-up was in the household subscriber sector with an increase of 42% in household non dial-up subscribers from the number recorded at the end of September 2004.
- The total number of ISPs only increased by 2 over the six month period from the end of September 2004, however, there was more volatility when viewing ISPs by size category with the largest growth was in the Very Small size category, those ISPs with 100 or less subscribers.

3. *What is e-commerce?*

E-commerce simply means use of the expanding infrastructure referred to above to conduct business. Electronic communications networks are no longer limited to the internet but may include other third generation technologies typically operated by mobile telecommunications companies.

Typically, e-commerce transactions are categorised in four ways being:

- (a) consumer to consumer transactions;
- (b) business to consumer transactions;
- (c) business to business transactions; and
- (d) many to many transactions (e-markets or exchanges).

In the early 2000s, there was a rapid appreciation of the potential of e-commerce transactions to create efficiencies for business, resulting in a frenzy of activity in all of the above areas but particularly in relation to e-markets. As many anticipated at that time, there has been a rapid rationalisation with many e-markets, often promoted by third parties, simply not getting off the ground. While many e-markets still exist, they have not replaced the bilateral transactions referred to in (a) to (c) above to the extent anticipated.

At the height of the frenzy, third party promoters went about the business of promoting both vertical (industry specific) and horizontal (cross-industry) e-market lines. E-markets typically integrate the e-sale and the procurement systems of all parties creating a single digital standard for transacting business. E-markets enable the minute to minute connectivity required to exploit the efficiencies created by early e-sales and procurement systems, while allowing companies and their suppliers to begin creating integrated industry wide supply chain. For example, assuming 10,000 suppliers deal with 1,000 manufacturers

who deal with 10,000 retailers, in an each to each system 100 billion electronic data interface connections may be required. Where 1 hub is used acting as a central conduit, this is reduced to 21,000 electronic data interface connections.

As an example of current e-market activity, on 12 May 2005, the Australian Competition and Consumer Commission (ACCC) announced its draft determination on changes to the *National Electricity Code* concerning business-to-business (B2B) communications. The features of the proposed changes include:

- the creation of a new central B2B electronic hub to handle all the relevant customer and site information;
- the standardisation and automation of B2B activity to address jurisdictional inconsistencies including protocols and mechanisms intended to support the information requirements and transactions of retail competition;
- the creation of an Information Exchange Committee to act as a governing body and provide clearer management and direction;
- the enforcement of participation through the creation of obligations by replacing the state-based jurisdictional arrangements.

At the time the changes were proposed, B2B communications involved manual processes such as telephone, email and manual file transfer. The changes are designed to address perceived inefficiencies in the current processes at the time, including:

- inefficiencies and inconsistencies arising from different specifications and information exchange protocols that existed between different jurisdictions for the same or similar B2B communications;
- limited enforceability as compliance with B2B arrangements was voluntary in all states except Victoria;
- inadequate management and direction arising from an arrangement whereby the national B2B working group developed national B2B specifications and jurisdictional B2B specifications that were in turn considered by state-based committees.

The ACCC issued its final determination on changes to the National Electricity Code relating to B2B communications on 22 June 2005. The ACCC determined that net public benefits were likely to flow from the implementation of the new B2B governance arrangements.

4. *Continuing Co-ordination*

The Office for the Information Economy in the Department of Communications, Information Technology and the Arts (“DOCITA”) plays a major role in the uptake of e-commerce in Australia by facilitating a wide range of projects aimed at developing e-commerce in Australia with a key emphasis on B2B e-commerce .

On 13 July 2004 the Commonwealth Government released “*Australia’s Strategic Framework for the Information Economy 2004-06*” (“**Strategic Framework**”).

The Strategic Framework identifies four key priorities to ensure the ongoing development of Australia's information economy, as follows:

- (a) ensuring that all Australians have the capabilities, networks and tools to participate in the benefits of the information economy;
- (b) ensuring the security and interoperability of Australia's information infrastructure, and support confidence in digital services;
- (c) developing Australia's innovation system as a platform for productivity growth and industry transformation; and
- (d) raising Australian public sector productivity, collaboration and accessibility through the effective use of information, knowledge and information and communications technology.

The Strategic Framework aims to ensure the ongoing and effective delivery of public sector services and information across all tiers of government.

ELECTRONIC CONTRACTS

1. *Electronic Transactions Act*

The *Electronic Transactions Act, 1999* (Cth) (“**ETA**”) (which is mirrored by legislations in states and territories) governs electronic transactions in Australia and provides for contracts transacted electronically to be legally enforceable as a written contracts.

The ETA is largely based on the *United Nations Commission on International Trade Law’s Model Law on Electronic Commerce* (“**UNCITRAL Model Law**”) which was drafted in 1996 to assist countries in the framing of legislation which would enable and facilitate electronic contracting and eliminate the need for trading partner agreements.

The ETA, like the UNCITRAL Model Law, is not intended to govern every aspect of e-commerce, rather it provides general procedures and principles for electronic contracting.

In addition to Australia, many countries have adopted the UNCTRAL Model Law as the basis for their electronic transaction legislation, particularly the countries in the European Union and in Southeast Asia.

A high level analysis of the *Electronic Transactions Act’s* key provisions is contained in the following table:

Section	Title	Effect of Provision
Section 5	Definitions	The term “electronic communications” as used in the ETA means: <ul style="list-style-type: none"> (a) a communication of information in the form of data, text or images by means of guided and/or unguided electro magnetic energy; or (b) a communication of information in the form of speech by means of guided and/or unguided electro magnetic energy where the speech is processed at its destination by an automated voice recognition system.
Section 3	Object	The Act cites its objects as being to: <ul style="list-style-type: none"> (a) recognise the importance of the information economy to the future economic and social prosperity of Australia; (b) facilitate the use of electronic transactions; (c) promote business and community confidence in the use of electronic transactions; and

		(d) enable business and the community to use electronic communications in their dealings with governments.
Section 8	Validity of electronic transactions	This key clause provides that a transaction is not invalid simply because it took place wholly or partly by means of electronic communications.
Section 9	Writing	<p>If a Commonwealth law requires someone to give information in writing, that obligation has been performed if the person gives the information by means of electronic communications where certain conditions are met. Examples are:</p> <ul style="list-style-type: none"> (a) whether information will be readily accessible for subsequent reference; (b) if the requirements of a particular Commonwealth entity are met; (c) if the verification requirements of any particular Commonwealth entity are met; and (d) where the information is not being given to a Commonwealth entity, where the person to whom the information is required to be given consents to the information being given by way of electronic communication. <p>Examples of “giving information” include making applications, lodging claims, sending notifications, lodging returns, making a request, making a declaration, lodging an objection etc.</p>
Section 11	Production of documents	<p>If a Commonwealth law requires you to produce a document in paper form, that obligation is performed if it is provided in electronic form where certain conditions are met, including:</p> <ul style="list-style-type: none"> (a) the method of generating the electronic form of the document is a reliable means of assuring the maintenance of the “integrity” of the information contained in the document; (b) if, when it was sent, it was reasonable to expect the information contained in the electronic form of the document could be readily accessible so as to be usable for subsequent reference; and (c) similar constraints as referred to in section 9 above if the information is required to be given to a Commonwealth entity. <p>The “integrity” of information contained in the document will be considered to be maintained if the information has remained complete and unaltered apart from the inclusion of any endorsement or immaterial change which arises in the normal course of communications, storage or display.</p> <p>If any other law of the Commonwealth requires a more specific method of producing a document then that law will prevail.</p>

Section 12	Retention	<p>If a law of the Commonwealth requires you to retain information, that obligation is met where it is reasonable to expect that the information could be readily accessible so as to be later usable, and where any specific regulations have been met.</p> <p>There are also some specific rules regarding retention of otherwise written documents in electronic form and the retention of documents which were otherwise always in electronic form.</p>
Section 15	Attribution of electronic communications	<p>This provision provides that, for the purposes of Commonwealth law, unless the parties agree otherwise, the purported originator of an electronic communication is bound by that communication only if the communication was sent by that purported originator or with its authority. Section 15 then states that this general principle is not intended to affect the operation of general principles of agency law regarding actual and ostensible authority.</p>
Section 14	Time and place of dispatch and receipt of electronic communications	<p>To inject certainty into electronic transactions, this provision provides that the time of dispatch, unless otherwise agreed, occurs when the electronic communication enters the single information system outside the control of the originator or, if it enters successively two or more systems outside the control of the originator, when it enters the first of those systems.</p> <p>The time of receipt will either be:</p> <ul style="list-style-type: none"> (a) if the addressee of an electronic communication has designated an information system for the purpose of receiving the communication, when it first enters that system; or (b) where the addressee has not designated such a system, when it first “comes to the attention of the addressee”. <p>Unless the parties otherwise agree, the place of dispatch and receipt will be the place where the originator has its place of business (in the case of dispatch) and where the receiver has its place of business (in the case of receipt). Where there are multiple places of business of their originator or receiver, then the place of business that “has closer relationship to the underlying transaction” will be the relevant place. If that analysis does not work with the relevant transaction, then the originator or a receiver’s principal place of business will be the relevant place. In circumstances where the originator and the receiver or the receiver don’t have a place of business, then their ordinary residence will suffice.</p>

While the ETA provides considerable clarification, what can be seen is that the normal rules of contracting and doing business (subject to the jurisdictional issues discussed below) will continue to apply.

For instance, if the transactions involved relevant individuals then the consumer protection provisions found in legislation such as the *Trade Practices Act, 1974* (Cth) will apply. The Australian government has recognised particular challenges which may apply for businesses conducting transactions online in complying with the *Trade Practices Act* and has published “*Building Consumer Sovereignty in Electronic Commerce: Best Practice Model for Business*” in May 2000.

From a general contracting point of view, when undertaking online transactions consideration will always be required as to whether a web vendor is issuing an offer or a mere invitation to treat, what the terms of the online contracts are, and when and how acceptance occurs. In most situations, a web vendor will be simply providing an invitation to treat. When the consumer fills out any online form, it will normally activate a button labelled “I Accept” or “Submit” or “Purchase” or some other phrase. While the word “Accept” is used, this act on the part of the Purchaser will normally only constitute an offer. If that is the case, the terms of the contract will need to have been clearly established prior to that offer being submitted.

This often poses a challenge to legal advisers when assisting clients structure these contractual arrangements, with online vendors seeking to minimise the amount of terms and conditions a customer must scroll through before making the offer. This of course needs to be balanced with the requirement that all the terms of the contract must be brought to the attention of the parties before the contract can be formally concluded. The dangers of incorporating the terms and conditions on a separate page, rather than being embedded on the contract page, are clear. A compromise is usually to provide in the order form for customers to tick a box, or click on an acknowledgment that the terms and conditions have been read. Prudence requires that those terms and conditions, or at least the location of them, must be clearly apparent and be easily accessible if they are not contained on the contract page.

In addition, the *Vienna Convention on the International Sale of Goods* (“**CISG**”) signed in 1980, automatically applies to international sales contract involving Australian companies unless it is contractually excluded.

2. *Current Activities*

On 19 March 2004, the Working Group on Electronic Commerce of UNCITRAL, the chief United Nations body overseeing international trade law policies, announced that it had adopted draft text that would create a unified legal regime for worldwide electronic commerce, removing barriers and lowering costs for companies using the Internet to conduct business and overcome the perceived shortcomings in the CISG and the UNCITRAL Model Law.

On 23 November 2005 the United Nations General Assembly adopted the resulting *Convention on the Use of Electronic Communications in International Contracting* (**Convention**).

The Convention aims to remove obstacles to the use of electronic communications in international contracting (as opposed to domestic contracting which is the focus of ETA) by increasing certainty where electronic communications are used in international contracts, for example by establishing rules to determine a party’s location in an electronic environment and the time and place of dispatch and receipt of messages, clarifying the use of automated message systems for contract formation and providing guidance on electronic authentication methods.

The Convention is subject to ratification, acceptance or approval by the signatory states, with a signatory event expected to take place in New York from 19 June to 7 July 2006.

JURISDICTION

1. *The nature of the problem*

It is trite to say that one of the key legal issues with which courts around the world have been grappling in recent years is the analysis of their scope and derivation of power to hear particular disputes regarding online transactions and to compel those people involved to obey its commands.

This issue is exacerbated online as participants may not even be aware of the location of the person with whom they are dealing. Much of the law and jurisdiction is invalid in an environment which also lacks physical boundaries and communities.

2. *Australian Case Development*

(a) *Macquarie Bank Limited & Anor v Berg [1999] NSWSC 526*

In this case, Macquarie Bank Limited and Mr Berg were in dispute in relation to a number of matters arising from Mr Berg's employment (or consultancy) arrangement with the bank.

During 1999, material started appearing on a website at www.macquarieontrial.com which related to that relationship. Macquarie Bank sought to restrain the publication of that material. The court was satisfied that the material and the site conveyed imputations defamatory to Macquarie Bank. The court presumed that the material had been prepared, or had been facilitated, by Mr Berg who was not physically present in New South Wales (the natural jurisdiction of the court), it being presumed that he was located in the United States.

The court was satisfied that it was empowered to restrain conduct occurring or expected to occur outside the territorial boundaries of its jurisdiction and it could exercise this power in its discretion. That discretion involved consideration of the potential enforceability of any orders made and whether another court was a more appropriate forum. The court could only enforce any order if the defendant voluntarily returned to New South Wales and the court could not compel him to do so. The court however was concerned to exercise its discretion in circumstances where the order's effectiveness was solely dependent upon the voluntary presence, at the time of his selection, of Mr Berg.

Moreover, the court was troubled by the nature of the internet given that information on the internet can be received by anybody anywhere. The order sought by Macquarie Bank could have the effect of restraining publication of all the material then presently contained on the website in any place in the world. It was not possible to simply ensure that the information could not be seen within New South Wales. The court held:

“An injunction to restrain defamation in New South Wales is designed to ensure compliance with the laws of New South Wales and to protect the rights of plaintiffs as those rights are defined by the law of New South Wales. Such an injunction is not designed to superimpose the law of New South Wales relating to defamation on every other state, territory and country of the world ...”

It should be noted, however, that the decisions of the Federal Court in 1999 in *Australian Securities and Investments Commission v Matthews* [1999] FCA 164 and *Australian*

Securities and Investments Commission v Matthews [2000] NSWSC 390 proffered a different result from a similar facts and circumstance.

(b) ***Gutnick v Dow Jones & Co Inc [2001] VSC 305***

Dow Jones is the publisher of the *Wall Street Journal*, and another magazine called *Barrons*. In late 2000, *Barrons* published a story relating to Mr Joseph Gutnick's business affairs to which Mr Gutnick took objection. Mr Gutnick is primarily resident in Victoria although he conducted some affairs in the United States where *Barrons* is published. *Barrons* was also published online, with the server hosting the website being located in New Jersey. The court was satisfied that Victorian readers downloaded the relevant article.

In its defence, the publishers of *Barrons* proffered that the article was published in New Jersey, the place of location of the server, and not in Victoria and was therefore beyond the jurisdiction of Victorian courts.

The court was of the view that the law in defamation cases has been for centuries that publication takes place where and when the contents of the publication, oral or spoken, are seen and heard and comprehended by the reader or hearer. On that basis the court was of the view that publication of the relevant article occurred in Victoria when it was downloaded by the Dow Jones subscribers who had met Dow Jones' payment and performance conditions and by the use of their passwords. The court did not support the argument that the publication occurred when and where the material was uploaded in New Jersey.

In relation to arguments advanced by Mr Berg's Counsel, the court held that:

"Counsel was free to say what he chose when deploring the possibility that the court should reach a conclusion that threw a cordon sanitaire around the country to prevent its citizens from receiving information available everywhere else. But this claim is an overstatement. About this relatively self indulgent submissions, the court says nothing, having neither the power or inclination to censor anything. The point simply is that if you do publish a libel justiciable in another country with its own laws ... then you may be liable to pay damages for indulging that freedom."

(c) ***ACCC v Worldplay Series Pty Limited (2004) FCA 113***

In *Australian Competition and Consumer Commission v Worldplay Services Pty Ltd [2004] FCA 1138* the ACCC alleged that, among other things, Worldplay Services Pty Ltd ("**Worldplay**") had breached section 65AAC(1) of the *Trade Practices Act 1974* (Cth) by participating in a global online business that was in fact a pyramid selling scheme. The business in question provided gaming services in over 50 countries, trading under the name World Games Inc. ("**World Games**").

However, Worldplay argued that as the scheme could not be accessed using an internet connection provided by an Australian ISP, the scheme operated outside the territorial boundaries of Australia and was therefore beyond the application of the *Trade Practices Act*. This raised the question of the extent to which operators of internet-based pyramid selling schemes could use Australia as a haven (either wholly or partially) in circumstances where the Australian public cannot gain internet access to such schemes through Australian ISPs.

Justice Finn held that the case essentially involved the application of Australian law to an Australian registered company engaging in conduct within Australia and that, as the relevant

conduct occurred at Worldplay's Queensland office, Worldplay was participating in a pyramid selling scheme in contravention of the *Trade Practices Act*.

SECURITY

This area of e-commerce law deals with issues such as:

- (a) online privacy;
- (b) encryption and electronic signatures;
- (c) protection from cyber crime.

1. *Privacy*

When the *Privacy Act*, 1988 (Cth) was first introduced, it applied only to the public sector. The legislation represented the Federal Government's recognition of the need for limited data protection measures. It largely arose out of a failed attempt to implement a national identification scheme (the Australia Card). Originally the *Privacy Act* regulated Commonwealth agencies in their processing of personal data and did not regulate the private sector except for their handling of tax file numbers and consumer credit information.

In February 1998, the Australian Privacy Commissioner issued *National Principles for the Fair Handling of Personal Information (NPP)*. This is a set of 10 principles based on OECD Guidelines. The NPPs, although useful in the private sector environment, did not specifically deal with electronic commerce or telecommunications.

In December 1998, the Federal Government announced its intention to legislate support and strengthen self regulatory privacy protection in the private sector by way of legislation based on the NPPs (which NPPs were revised in January 1999). The result was the *Privacy Amendment (Private Sector) Act*, 2000 (Cth) which establish a national scheme for the handling of personal information by private sector organisations. The Act took effect on 21 December 2001.

As a result, the NPPs became the legislative bench mark, with the legislation allowing for organisations to develop privacy codes approved by the Privacy Commissioner. If an organisation chooses not to adhere to the NPPs but to develop its own privacy code, this will need to be approved by the Privacy Commissioner and must meet or exceed the standards set out in the NPPs.

As a result, any use in Australia of information collected from customers will need to comply with these arrangements. The NPPs covers such issues such as:

- (a) collecting information only to the extent necessary for one or more of the organisation's functions or activities, and then only by lawful and non-intrusive means and in a manner in which the individual is aware of what is occurring;
- (b) prohibitions on the use and disclosure of personal information other than for the primary purpose for which it was collected unless certain conditions are met;
- (c) ensuring that personal information is accurate, complete and up to date;
- (d) protecting personal information held from misuse and loss and from unauthorised access, modification or disclosure;

- (e) an organisation must have clearly expressed policies for the management of personal information;
- (f) an individual must be provided with access to information about him or her on request except in certain conditions;
- (g) the organisation must not adopt as its own identifier of an individual an identifier of an individual that has been assigned by certain statutory bodies;
- (h) wherever it is lawful and practicable, individuals must have the option to not identify themselves when entering into transactions with an organisation;
- (i) restrictions are placed on certain transborder data flows;
- (j) prohibitions are placed on organisations collecting certain information which is “sensitive” unless certain preconditions are met.

Some organisations are exempted from compliance with the scheme.

2. *Encryption and Electronic Signatures*

A tool used to achieve privacy on the internet is encryption. Encryption also plays a significant role in relation to authentication of participants in e-commerce transactions as discussed further below.

Given the nature of the internet, information being communicated as part of an e-commerce transaction may move through innumerable separate computers called routers on a route that is never pre-ordained and is decided according to traffic flows of information across the internet. As a result, the likelihood of interception is great if the information is not first encrypted.

As a result, increasingly in online transactions various encryption techniques are applied. One of the most prolific is asymmetric public/private key cryptography, which uses two different but mathematically related keys to encrypt and decrypt information at high speed, but also to incorporate a technique which assists in verifying the identity of the sender and receiver.

One of the keys is called the public key while the other key is called the private key, both of which can encode and decode. While the public key is a unique individual key, it is designed to be freely distributed to anyone who requires it. The private key however is kept securely by the individual.

When a third party wants to send a message to another key holder, they encode their message using the freely available public key. Once it is encoded with a particular public key, only the associated private key can decode the message. As a result, anyone can send the message but only the intended recipient can read it.

One part of the message sent by sender (the signature) is encoded using the sender’s private key. This can only be decoded using the associated public key. While anyone can view the contents of this part of the message, the system can guarantee the authenticity of that signature provided the sender has held its private key securely.

The public keys are held by some trusted authority, for example, Australia Post, so that they may be generally available. That authority may also issue private keys. It is the

responsibility of the authority to verify the identity of the person to whom keys are issued in order for the system to retain its integrity. The issuing institution will take the issued public key and digitally sign it with that institution's own key in a tamper proof way to prove that the institution has verified that the key belongs to its owner.

There are some circumstances however where the use of encryption must be regulated. As a result the *Customs Act, 1901 (Cth)* provides to the government power to prohibit the exporting of certain goods from Australia. One of those goods is asymmetric algorithms used for encryption and decryption.

As noted above, in addition to preserving privacy, encryption techniques assist in identifying and authenticating participants in e-commerce transaction.

There had been a number of private sector moves to establish a ubiquitous electronic signatures protocol in Australia. An example is the establishment of a public key infrastructure project for doctors known as Health e-Signature. As the Health e-Signature authority, the government established its own public key infrastructure frame work for the public sector known as Gatekeeper. This PKI was designed to facilitate the production of government services online.

While the government appears to be leaving authentication technology to the market, it is noted that in the ETA, clause 10 relates to the requirement for a signature. It provides that if, under the law of the Commonwealth, a signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if:

- (a) a method is used to identify the person and to indicate that the person's approval to the information communicated;
- (b) having regard to "all the relevant circumstances at the time the method was used" the method as reliable as was appropriate to the purposes for which the information was communicated; and
- (c) some other Commonwealth entity specific requirements are not.

On 21 March 2005, the Australian government launched its *Australian Government Authentication Framework (AGAF)* which represented a consistent whole of government approach to authentication for online dealings between business and government.

The purpose of AGAF was to increase the level of security and trust in online transactions and reduce associated compliance costs. AGAF encompasses principles providing guidance on verification and risk reduction of online transactions in the areas of:

- (a) transparency;
- (b) cost effectiveness;
- (c) risk management;
- (d) consistency;
- (e) trust; and
- (f) improved privacy.

At the same time, various check lists for government and business, implementation guides for government and business, and detailed guides to authorisation and access management are provided.

3. *Cyber Crime*

Broadly speaking, there are three distinct types of criminal activity that the online environment is often subject to, being:

- Targeting other computers – this occurs when computers are used for the creation and proliferation of computer viruses, worms, Trojans or other programs designed to cause damage to computers or for hacking into other systems;
- Ancillary purposes – such as storing information concerning other criminal activities like the pirating of software or pornography; and
- Committing an offence – credit card fraud and the distribution of child pornography are commonly cited examples.

(a) Targeting other Computers

Computers may be used unlawfully to compromise the confidentiality, integrity or availability of a computer system by the following means:

- hacking computer systems to obtain information without authorisation;
- hacking computer systems to control the computer system without authorisation;
- transmitting a computer virus or other program intended to harm, control or otherwise disrupt another computer or system.

(b) Computers to Store Information of Criminal Activities

Computers may be used to further criminal activity and store information pertaining to that unlawful activity. For example, a person might store stolen credit card details on a computer.

(c) Computers to Perpetrate Crimes

Many crimes traditionally committed offline are now being committed online due to the ease of communication and the Internet's ability to allow a perpetrator to be in touch with a broader community.

(d) Response to Cyber Crime

The need for co-operation between the law agencies of multiple jurisdictions has been highlighted by the increasing use of the Internet in relation to many illegal activities. An example of this was Operation Falcon, a major US investigation into Internet child pornography announced on 16 January 2004 which required the assistance of law enforcement agencies in a number of other countries including France, Spain and Belarus and was the catalyst for Operation Auxin in Australia concerning the same credit card fraud and pornography ring.

In 2001, amendments to the *Crimes Act 1900 (NSW)* were enacted through the *Crimes Amendment (Computer Offences) Act 2001*.

The amendments are designed to tighten the penalties for prohibited acts relating to computers, with specific provisions relation to viruses and hacking. The new provisions prohibit:

- any unauthorised access to data held in any computer;
- any unauthorised modification of data held in any computer;
- any unauthorised impairment of electronic communication to or from any computer;
- the possession or control of data with the intention of committing a serious computer offence or with the intention of facilitating the commission of a serious computer offence; and
- producing, supplying or obtaining data with the intention of committing a serious computer offence or with the intention of facilitating the commission of a serious computer offence.

The Federal Government has also introduced significant amendments to the *Criminal Code 1995* by way of the *Crimes Legislation Amendments (Telecommunications Offences and other Measures) Act (No. 2) 2004* (“**Crimes Amendments Act**”) which came into effect on 28 September 2004.

The *Crimes Amendments Act* repeals some of telecommunications offences in the *Crimes Act 1914* and replaces them with new and updated telecommunications offences in Part 10.6 of the *Criminal Code*. Significantly, the *Crimes Amendments Act* creates new offences concerning the access, production, supply and obtaining of child pornography and child abuse material using new technological tools, such as the Internet. The legislation also targets online ‘grooming’ activities by sexual predators. The offences established under the new laws will allow Australia-wide prosecution of internet pornography offenders and include tough penalties of up to 10 years imprisonment.

The *Crimes Amendments Act* also creates “Financial Information Offences” in Part 10.8 of the *Criminal Code*. These amendments criminalise dishonestly obtaining, or dealing in, personal financial information without the consent of the person to whom the information relates and also criminalises possession, control or importation of a thing with the intention that the thing be used to commit the offence of dishonestly obtaining or dealing in personal financial information.

The introductions of the “Financial Information Offences” are a response to the Model Criminal Code Officers’ Committee’s (MCCOC) March 2004 discussion paper on credit card skimming offences. Credit card skimming is the process by which legitimate credit card data is illicitly captured or copied, usually by electronic means.

Certain aspects of cyber crime have also been the subject of reports released by a number of Australian agencies. The Australian Institute of Criminology’s (AIC) report *Online Credit Card Fraud Against Small Businesses* released in 24 February 2004 which revealed that less than one third of incidents uncovered by the survey were reported to police. In contrast to over-the-counter credit card transactions, where businesses are generally not liable for fraudulent purchases, online traders are responsible for recouping losses associated with online credit card fraud. This national survey of small businesses found:

- one third of online traders have been a victim of online fraud;
- over half of those businesses hit became repeat targets of fraudsters; and,
- average losses ranged from \$100 to \$3,500.

On 1 September 2005, the Minister for Communications, Information Technology and the Arts, Senator Helen Coonan, launched *Taking Care of Spyware*, a guide to help Australians

protect themselves against spyware on the Internet. The Minister also released submissions received in response to a recent Government review on spyware.

The Minister reported that:

“The feedback we received from members of the public and industry stakeholders highlighted a need for the public to be aware of the threat of spyware. The Taking Care of Spyware brochure tells consumers how they can identify spyware on their computers and remove it, or protect their computers against it.”

The Government will now follow up on courses of action identified in the consultation process.

“This will include things like working with e-security companies and law enforcement agencies to target spyware,” Senator Coonan said. *“The Government will also continue to work with the Internet industry to ensure that consumers know what is installed on their computers and what information they are making available online to others.”*

CONTENT REGULATION

Faced with inconsistent laws across jurisdictions, the problem of regulating content creates a conflict between the historical, cultural and societal basis of the laws of each jurisdiction.

An example of the difficulty regulating content is the law concerning defamation. In the United States, freedom of speech is protected by the *First Amendment* and is considered to be pro-defendant. However, in Australia a right to freedom of speech is not assumed and the law is considered to be pro-plaintiff. As a result, content which may be acceptable in the United States might be considered to be defamatory in Australia.

1. *Spam*

Another area where conflict arises is the issue of Spam. Both Australia and the United States have introduced substantial legislation prohibiting the dissemination of spam. However, countries such as China and Russia risk becoming havens for creators of Spam due to an absence of legislation in those countries.

In Australia, Spam is now regulated by the *Spam Act 2003 (Cth)* which seeks to combat spammers and the techniques they use.

Spam became a problem for both technical and non-technical reasons. Technical reasons include:

- ♦ costs;
- ♦ the burden imposed on ISPs;
- ♦ Spammers disguising the origin of unsolicited bulk e-mail; and
- ♦ techniques such as “bombing”.

Non-technical reasons include:

- ♦ inconvenience and frustration;
- ♦ fraud, deception, indecency and privacy.

The main features of the *Spam Act* include:

- a prima facie ban on the sending of unsolicited commercial electronic messages, to be enforced by the Australian Communications & Media Authority (“**ACMA**”);
- a prohibition on the sale, supply or use of electronic address harvesting software and lists generated from these for spamming purposes.

In accordance with Part 2 of the *Spam Act*, all commercial electronic messages must:

- only be sent with **consent**;
- contain **accurate information** about the sender; and
- contain a functional **unsubscribe facility**.

(a) Consent

Consent may be express, conferred or implied.

(b) Identity

People who receive electronic messages should be able to know who the sender is and how to contact the sender from the information contained in the message.

(c) Unsubscribe

The choice to opt-out of, or unsubscribe from, future electronic messages must be provided. A functional unsubscribe facility should be included in all commercial electronic messages and unsubscribe requests should be dealt with promptly.

Pursuant to the Act, a person or company is not considered to have ‘sent’ a commercial message if they only supplied a carriage service that allows the message to be sent.

A public consultation version of a *Draft Spam Code* (“**Draft Code**”) applying to Internet and Email Service Providers was released on 26 July 2004. The Draft Code is designed to compliment the *Spam Act*.

The Draft Code seeks to define best practice standards for ISPs and email service providers (**ESPs**) in their spam management, as well as assisting their customers to exercise greater control as users.

On 11 August 2004 the *eMarketing Code of Practice* was released by the Australian Direct Marketing Association (“**ADMA**”). On 16 March 2005, the former ACA registered the code under section 117 of the *Telecommunications Act 1997* with the effect that compliance with the code is mandatory and enforceable by ACMA.

The *e-Marketing Code of Practice* establishes comprehensive, industry-wide rules and guidelines for the sending of commercial electronic messages in compliance with the *Spam Act 2003*. The Code provides detailed guidance about acceptable eMarketing practice, particularly with respect to issues such as consent and viral marketing. The Code also provides a framework by which industry can handle complaints about Spam and monitor industry compliance with code provisions.

2. *Online Gambling*

Online gambling is another area where the laws of different countries differ greatly. Again, many countries have not legislated in any way against online gambling and some even encourage the activity. Australia, however, has taken a strong position against online gambling. This is evidenced by the *Interactive Gambling Act 2001* (Cth) (“**Gambling Act**”), the key legislative instrument in relation to online gambling in Australia. The *Gambling Act* represents a uniform approach taken throughout Australia in relation to online gambling and sets out certain restrictions and a complaints process in relation to interactive gambling services.

The *Gambling Act* regulates interactive gambling services by:

- prohibiting interactive gambling services from being provided to customers in Australia;
- prohibiting Australian-based interactive gambling services from being provided to customers in designated countries; and
- establishing a complaints-based system to deal with Internet gambling services where prohibited Internet gambling content is available for access by customers in Australia.

The Act specifically prohibits a person providing “*prohibited Internet gambling services*”. Pursuant to section 6 of the Act, the definition of a “prohibited Internet gambling service” is very broadly defined to be a gambling service where:

- “(a) *the service is provided in the course of carrying on a business; and*
- “(b) *the service is provided to customers using an Internet carriage service; and*
- “(c) *an individual who is physically present in Australia is capable of becoming a customer of the service.*”

For the purposes of paragraph (c) above, the Australian-link will be deemed to be present if, and only if, any or all of the customers of the service are physically present in Australia

INTELLECTUAL PROPERTY

1. **Legislative Developments**

In order to more adequately deal with the protection of intellectual property rights in the online environment, changes were required to Australia’s legislative regime.

While the problems associated with protecting copyright and moral rights are not unique, the Internet provides greater ease for an author’s rights to be contravened. In response to this, the *Copyright Amendment (Digital Agenda) Act 2000* (“**Digital Agenda Act**”) was introduced in March 2001.

The *Digital Agenda Act* contained amendments to the *Copyright Act 1968* designed to achieve, among other things, the following:

- to improve the protection for owners of copyright in relation to the use of their copyright material on the Internet and through other new communications technologies while still facilitating the growth of the information economy;

- to replace technology-specific rights with technology-neutral rights so that amendments to the *Copyright Act* are not needed each time there is a development in technology;
- to ensure that copyright law provides carriers and carriage service providers (including ISPs) with reasonable certainty about liability for infringements that occur on their facilities or infrastructure; and
- to ensure that the legislation is consistent with the international obligations in the *WIPO Copyright Treaty* and *WIPO Performances and Phonograms Treaty* in relation to the digital agenda

The key amendments made by the *Digital Agenda Act* include:

- a new exclusive right of communication to the public in place of the existing broadcast right and the right of transmission to subscribers to a diffusion service;
- a new extended definition of “broadcast” to include cable transmissions and to bring it within the meaning of the *Broadcasting Services Act 1992*;
- the expansion of an author’s exclusive rights over use of their material, particularly on the Internet;
- new enforcement measures in relation to circumvention devices and services, rights management information, and broadcast decoding services.

The amendments also make it clear that a copyright owner has the exclusive right to convert copyright material into electronic form as part of the existing exclusive reproduction right.

Since the implementation of the *Digital Agenda Act*, the *US Free Trade Agreement Implementation Act 2004* (Cth) (“**Act**”), the legislation implementing the *Australia-United States Free Trade Agreement* (“**AUSFTA**”), has also been introduced and includes a number of provisions amending the *Copyright Act 1960* (Cth).

A significant amendment to the *Copyright Act* is the creation of the new Part V, Division 2AA which deals with safe harbour provisions and a take-down notice regime for ISPs in connection with copyright infringement claims. These amendments seek to align certain aspects of Australian copyright law with those of the US.

The amendments contained in the new Part V, Division 2AA of the *Copyright Act* limit the remedies available against a carriage service provider (including an ISP) for copyright infringements that relate to certain online activities provided the ISP complies with a number of conditions.

The first two general conditions that an ISP must satisfy are:

- the adoption and implementation of a policy of terminating the accounts of users who are repeat infringers; and
- accommodating and not interfering with any technical measures used to protect and identify copyright material.

If the threshold criteria above are satisfied, certain additional conditions must be satisfied depending on the category of the services offered by the ISP:

Category	Activity	Conditions
A	Providing facilities or services for transmitting, routing or providing connections for copyright material, or the intermediate and transient storage of copyright material in the course of transmission, routing or provision of connections.	<ol style="list-style-type: none"> 1. Any transmission of copyright material in carrying out this activity must be initiated by or at the direction of a person other than the carriage service provider. 2. The carriage service provider must not make substantive modifications to copyright material transmitted. This does not apply to modifications made as part of a technical process.
B	Caching copyright material through an automatic process. The carriage service provider must not manually select the copyright material for caching.	<ol style="list-style-type: none"> 1. If the copyright material that is cached is subject to conditions on user access at the originating site, the carriage service provider must ensure that access to a significant part of the cached copyright material is permitted only to users who have met those conditions. 2. If there is a relevant industry code in force—the carriage service provider must comply with the relevant provisions of that code relating to: <ol style="list-style-type: none"> (a) updating the cached copyright material; and (b) not interfering with technology used at the originating site to obtain information about the use of the copyright material. 3. The service provider must expeditiously remove or disable access to cached copyright material upon notification in the prescribed form that the material has been removed or access to it has been disabled at the originating site. 4. The carriage service provider must not make substantive modifications to the cached copyright material as it is transmitted to subsequent users. This does not apply to modifications made as part of a technical process.
C	Storing, at the direction of a user, copyright material on a system or network controlled or operated by or for the carriage service provider	<ol style="list-style-type: none"> 1. The carriage service provider must not receive a financial benefit that is directly attributable to the infringing activity if the carriage service provider has the right and ability to control the activity. 2. The carriage service provider must expeditiously remove or disable access to copyright material residing on its system or network upon receipt of a notice in the prescribed form that the material has been found to be infringing by a court. 2A. The carriage service provider must act expeditiously to remove or disable access to copyright material residing on its system or network if the carriage service provider: <ol style="list-style-type: none"> (a) becomes aware that the material is infringing; or (b) becomes aware of facts or circumstances that make it apparent that the material is likely to be infringing. <p>The carriage service provider does not, in an action</p>

		<p>relating to this Division, bear any onus of proving a matter referred to in paragraph (a) or (b).</p> <p>3. The carriage service provider must comply with the prescribed procedure in relation to removing or disabling access to copyright material residing on its system or network.</p>
D	Referring users to an online location using information location tools or technology	<p>1. The carriage service provider must not receive a financial benefit that is directly attributable to the infringing activity if the carriage service provider has the right and ability to control the activity.</p> <p>2. The carriage service provider must expeditiously remove or disable access to a reference residing on its system or network upon receipt of a notice in the prescribed form that the copyright material to which it refers has been found to be infringing by a court.</p> <p>2A. The carriage service provider must act expeditiously to remove or disable access to a reference residing on its system or network if the carriage service provider:</p> <p>(a) becomes aware that the copyright material to which it refers is infringing; or</p> <p>(b) becomes aware of facts or circumstances that make it apparent that the copyright material to which it refers is likely to be infringing.</p> <p>The carriage service provider does not, in an action relating to this Division, bear any onus of proving a matter referred to in paragraph (a) or (b).</p> <p>3. The carriage service provider must comply with the prescribed procedure in relation to removing or disabling a reference residing on its system or network.</p>

2. Prominent Cases

Metro-Goldwyn-Mayer Studios Inc., et al. v. Grokster, Ltd., et al

In this US case, MGM alleged that by distributing peer-to-peer file sharing software on the Internet, enabling users to make files available for download on the Internet by anyone else who has a copy of the same P2P program, Grokster had knowingly and intentionally distributed its software to enable users to contravene the *US Copyright Act*.

Grokster argued that it should not be liable for copyright infringements committed by its users.

The decision was an appeal from an earlier US Federal Court decision, which held, applying the 1984 decision in *Universal Studios v Sony* (the BetaMax case), that Grokster and StreamCast would not be liable for copyright infringements committed by their users as their software had *substantial non-infringing uses*. In particular, the Federal Court had relied on the fact that numerous independent bands voluntarily distributed their music for free using the services, so as to gain exposure and attract new listeners.

In its unanimous decision the US Supreme Court reversed the US Federal Court decision, holding that Grokster and Streamcast could be held liable for copyright infringements committed by users of its software.

Universal Music Australia Pty Ltd v Cooper [2005] FCA 972

This case addressed the liability of operators of Internet sites and ISPs for providing links to Internet sites that made available infringing copies of sound recordings.

Stephen Cooper was alleged to have authorised breaches of copyright by users of the website he owned and operated by enabling users to click on hyperlinks that led to other websites from which the users could access music files and music in MP3 format.

The Federal Court of Australia held that while merely providing a link to copyrighted material was not an infringement, Mr Cooper had sufficient control over the website and could have prevented the infringements by removing, or overseeing the insertion of, the hyperlinks.

Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242

This is the first Australian case to consider the legality of peer-to-peer file-sharing systems and copyright infringement by operators of those systems for the infringing conduct of users of those systems. The decision involves an important consideration of the issue of authorisation liability and the Digital Agenda amendments to the *Copyright Act 1968* and followed the decision of Justice Tamberlin in *Universal Music Australia Pty Limited v Cooper [2005] FCA 972*.

The case, involving the provision of copyright material owned by record companies, considered a range of complex technical and legal issues under the *Copyright Act 1968*, including provisions of the Act that were introduced by the 'Digital Agenda' amendments that came into force in 2001.

Along with his finding that the six respondents authorised the infringement of copyright by users of the system, Justice Wilcox declared and ordered that:

- the respondents threatened to infringe the copyright of the record companies in other recordings that were not the subject of the case;
- the respondents be restrained from authorising users to do in Australia any of the infringing acts in relation to sound recordings controlled by the record companies;
- the continuation of the system (known as Kazaa) shall not be regarded as a contravention of the preceding order if the respondents modify the Kazaa system under a filtering protocol to be agreed between the parties that will exclude infringing copies of recordings (by title, artist name, etc) from appearing in search results, along with placing maximum pressure on users of the existing Kazaa versions to upgrade to the modified version. Justice Wilcox believed that there needed to be an opportunity for the respondents to modify the Kazaa system in a targeted way, so as to protect the record companies' copyright interests (as far as possible) but without unnecessarily intruding on others' freedom of speech and communication (eg the sharing of non-infringing material);
- the infringing respondents pay 90 per cent of costs incurred by the record companies; and
- the record companies' claim for damages will be determined at a later date.

The case is currently being appealed by both parties.

Shane Barber
Partner
Truman Hoyle Lawyers
sbarber@trumanhoyle.com.au
Tel: 9226 9888
Fax: 9226 9899

Truman Hoyle is a Sydney based boutique law firm specialising in six complex and dynamic areas of law, being corporate law, communications law and regulation, technology law, energy law and regulation, industrial law, and property and infrastructure law. It was named *Australian Law Firm of the Year in 2005* for firms with under 50 lawyers. At the Australian Law Awards in 2005, it was named in the top two telecommunications law firms in Australia.

21 February 2006
© Truman Hoyle, Lawyers 2006