Fair Trading Laws in Victoria" held on 13 May 2005 with the speaker being Dr Elizabeth Lanyon and presentation notes accessible from www.consumer.vic.gov.au.

[4] Registered under the *Telecommunications Act* in May 2005; it can be located at http://www.acif.org.au/documents_and_lists/codes/C620.

[5] http://www.consumer.vic.gov.au/CA256F2B00224F55/page/Publications-Reports+%26+Guidelines?OpenDocument&1=80-Publications~&2=955-Reports+%26+Guidelines~&3=~.

[6] "Preventing unfair terms in consumer contracts - Preliminary guidelines for suppliers (November 2003), page 4, accessible at http://www.consumer.vic.gov.au/CA256F2B00224F55/page/Publications-Reports+%26+Guidelines?OpenDocument&1=80-Publications~&2=955-Reports+%26+Guidelines~&3=~.

[7] *Director General of Fair Trading v First National Bank plc* [2002] 1 AC 481.

[8] According to this decision "good faith" includes an assessment of the form of a contract. The relevancy of the presentation of the contract with respect to what is an unfair term is reflected in section 163(3) of the FTA which provides that a consumer document must be easily legible, a minimum of 10 point font generally and clearly expressed. Section 163(3) is not part of the unfair contracts provisions but nonetheless it was introduced as another relevant aspect in protecting consumers with respect to fair contractual terms.

[9] Footnote 7 at [17].

[10] Footnote 7 at [17].

[11] Footnote 6 at page 17.

[12] Footnote 6 at page 20.

[13] Footnote 6 at page 14.

[14] Section 32Y(1) of the Fair Trading Act 1999 (Vic) (**FTA**).

[15] Section 32Y(3) of the FTA.

[16] Section 32ZA(1) of the FTA.

[17] Section 32ZA(4) of the FTA.

[18] Section 32Y(2) of the FTA.

[19] Section 32Z(1) of the FTA.

[20] section 32Z(2) of the FTA.

[21] Media release dated 14 December 2004 "AAPT taken to court on mobile phone contracts" accessible at www.dpc.seek.gov.au.

[22] ACIF C620:2005 Consumer Contracts accessible at www.acif.org.au/documents_and_lists/Codes/C620 (**Code**)

[23] The Code at 6.2(b)(i). Specific exceptions can be found at 6.3.

E-Commerce Developments

Shane Barber and Bridget Edghill review the current trends and developments in relation to regulation of e-commerce in Australia.

Introduction

This article briefly canvasses the existing law regulating e-commerce in Australia and looks at the current trends and legislative developments occurring in this field of law. The article coincides with the new E-Commerce guidelines issued in March 2006 by the Australian Government.

As recently as the late 1990s much of the law described below was in its embryonic state, with legislatures 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.

This article updates activities in Australia over the last 18 months in 4 areas of law in particular which relate to e-commerce as follows:

(a) electronic contracts;
(b) jurisdiction issues;
(c) cybercrime; and
(d) spam.

Current Trends

In a little over a decade, use of the Internet has increased significantly.

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. The next survey is currently underway.

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 platform for e-commerce then, continues to expand, demanding constant legal and regulatory attention.

What is E-Commerce?

E-commerce simply refers to 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 pro-

moters 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 chains. 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 recent 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.

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:

- ensuring that all Australians have the capabilities, networks and tools to participate in the benefits of the information economy;
- ensuring the security and interoperability of Australia's information infrastructure, and support confidence in digital services;
- developing Australia's innovation system as a platform for productivity growth and industry transformation; and
- 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

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 table on pages 24 and 25.

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 in May 2000 published *"Building Consumer Sovereignty in Electronic Commerce: Best Practice Model for Business"* (**2000 Model**).

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.

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*

Section	Title	Effect of Provision
Section 5	Definitions	The term "electronic communications" as used in the ETA means: (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 ETA cites its objects as being to: (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	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: (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. Examples of "giving information" include making applications, lodging claims, sending notifications, lodging returns, making a request, making a declaration, lodging an objection etc.
Section 11	Production of Documents	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: (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. 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. If any other law of the Commonwealth requires a more specific method of producing a document then that law will prevail.
Section 12	Retention	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. 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.

Section	Title	Effect of Provision
Section 15	Attribution of Electronic Communications	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.
Section 14	Time and Place of dispatch and receipt of electronic communications	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. The time of receipt will either be: (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". 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.

(**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.

On 17 March 2006, the Australian Government published its updating replacement of the 2000 Model *The Australian Guidelines for Electronic Commerce* (**Guidelines**). Accompanying the Guidelines was a *Check List for Business to Consumer E-Commerce in Australia.*

The new Guidelines are designed to enhance consumer confidence in electronic commerce by providing guidance to businesses on how to deal with consumers when engaging in business to consumer e-commerce. While the principles set out in the Guidelines are not mandatory, compliance with them is strongly encouraged. The Guidelines seek to address those areas of e-commerce which may be different to the consumer's experience face to face. It covers issues such as security of payments, privacy of personal information and access to their address. The Guidelines provide guidance to:

- fair business practices;
- accessibility and disability access;
- advertising and marketing;
- engaging with minors;
- disclosures of businesses' identity and location;
- disclosures of contracts terms and conditions;
- the implementation of mechanisms for concluding contracts;
- adopting privacy principles;
- using and disclosing information about payment, security and authentication mechanisms;
- the establishment of fair and effective procedures for handling complaints and resolving disputes; and
- law and forum for the resolution of contractual disputes.

The Guidelines, among other things, reinforce general contractual principles in relation to ensuring consumers can access a clear and complete text of a transaction's terms and conditions both easily and in a printable forms. This is a particular reminder to legal advisers of companies undertaking online transactions given the common insistence by clients to "remove all the legal stuff" from relevant page set ups.

A full copy of the Guidelines is available at www.treasury.gov.au.

Jurisdiction

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 regarding jurisdiction is invalid in an environment which also lacks physical boundaries and communities.

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.macquar-

ieontrial.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 about exercising 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 sanitare around the country to prevent its citizens from receiving information available everywhere else. But this claim is an overstatement. About these 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*.

Cybercrime

Broadly speaking, there are three distinct types of criminal activity to which the online environment is often subject, 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.

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."*

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 in now regulated by the *Spam Act 2003* (Cth) which seeks to combat spammers and the techniques they use. The Spam Act has been examines in detail elsewhere and is beyond the scope of this article.

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.

Shane Barber is a partner, and Bridget Edghill is a lawyer, at Truman Hoyle, Sydney.