Cyberlaw and E-Commerce in Australia

Sam Berner

29 August 2002

"There is a certain hankering in the Government for more control of what happens on the Internet than is likely to be implementable… It takes time for the legislators actually to appreciate how the Internet works."

Vinton Cerf (in Needham, 1997)

1. The Research Problem

The e-commerce environment can be said to be characterised by a form of lawlessness, just like the American frontier. It is a relatively new territory occupied by agile entrepreneurs who are each staking a claim to a piece of the territory in the hope of making a fortune. Some of the pioneering entrepreneurs are engaging in illegal activities. Many others are testing the boundaries of what society and the law will permit to be done in the new territory. Some of the pioneers are attracted by the anonymity which the internet gives them; others are attracted by the ability to move quickly from jurisdiction to jurisdiction. Authorities have difficulties in enforcing laws across borders-in this case country borders, while individuals may feel that a sense of lawlessness pervades the space because of the difficulty in enforcing personal rights.

The issue of online or computer-related criminal activity in Australia is one fraught with much uncertainty, particularly since authorities such as the Federal Police are unsure as to the actual extent of the problem, or even of how to define "cyber-crime".

However, as in any new territory laws will develop to deal with these sorts of issues. It is also likely that in some areas laws will work in conjunction with technology to allow traditional rights to continue to be enforced. For example, in the case of copyright, software will be used to track and manage the use of digital information which will, if the use is unauthorised, assist the owner in bringing a breach of copyright claim to establish ownership and the unauthorised use.

This Research Report aims at providing a brief overview of the current legislation regarding e-commerce in Australia. It does not attempt to cover all the issues involved, but only to show that what ever laws are in place now are less than adequate to protect the businesses and consumers from practices done in bad faith.

2. Cybercrime Down Under

In a report submitted by the Australian Federal Police (ACPR, 2000), it stated that although there was a greater degree of co-ordination between national authorities, the level of the problem in Australia is not fully understood. In an article based on the report, which appeared in the AFP's journal, Platypus, Steve Jiggins (2000), director of the AFP's media and public relations, highlighted the issues of attempting to measure the problem.

> *"Electronic crime varies in its manifestations, so it is difficult to discuss in terms of aggregate incidence and impact. As a result, definitive information on the present extent and impact of electronic crime in Australia, New Zealand and overseas is not available." But it is often the victim of these crimes that are resistant to informing authorities of electronic crime. "A significant amount of this crime is simply not reported. This is in part... to avoid any potentially adverse impact on*

> *consumer confidence, or perhaps because of a lack of confidence in the capacity of law enforcement to deal with such issues in a timely way."*

Only two major Australian studies had been done previous to the ACPR report to establish the extent of the problem--one conducted by the Office of Strategic Crime Assessments (OSCA, 1997) and the Victorian Police, and one by the Victorian Police and Deloitte Touche Tohmatsu (1999). The study from 1997 concluded that 37 percent of businesses had been subjected to some form of electronic attack or unauthorised computer access. Of those that were attacked, 90 percent experienced some breach from within the organisation and 60 percent were external. The 1999 study offered similar results but also concluded that of those organisations that were attacked, 42 percent didn't even report the breach. Also, of those companies that experienced a breach, one third refused to provide a dollar value on what damage or loss had been incurred. A third report was published by Victorian Police and Deloitte Touche Tohmatsu this year.

Another issue which complicates the matter is that cybercrime, or rather computer-related crime, covers so much ground that it can't necessarily be covered under one banner for protection. The AFP outlines several electronic crimes including: theft of telecommunications services (much like the phone phreakers of old), communications for the advancement of criminal conspiracies, piracy, dissemination of offensive material (which often relates to offences such as cyberstalking), electronic money laundering and tax evasion, electronic vandalism and terrorism, sales and investment fraud, illegal interception of telecommunications signals, and electronic funds transfer fraud.

Nevertheless, one of the important facets of what is outlined in the report is that the majority of electronic crime revolves around traditional forms of criminal offence. The report explains, "While some behaviour is new, such as hacking and denial of service attacks, the majority of offending involving the use of technology is traditional crimes where the computer is an instrument/tool or a target." Although it's easy to blame hackers for breaches in business technology security, it's often the victim that should wear much of the blame. There is certainly no simple answer to avoiding hacks and potential security problems, but a reasoned and well-thought out policy can save you money and time in the long run. Perhaps one of the greatest risks to your data and to your network is what your own staff may tell someone else. First and foremost, it seems that the protection of one’s company's data is not a simple issue and should not be brushed aside by merely throwing money at it and hoping it will go away. There are certain priorities that need to be addressed. Corporate data has become more valuable in the information and Internet age, and businesses need to make the mental shift between protecting physical assets to protecting their intellectual capital and investment. Another major security issue for online Australian and international businesses is the privacy of its clients. This has been exacerbated by the bad press surrounding dot-com failures that pursue "names for sale" type liquidations. Companies need to realise that having an enforceable privacy policy is one of the key things consumers to e-commerce sites look for before transacting online. But it seems that it is the human factor that has one of the most profound effects on the security of businesses in Australia. David says that security has never just been a technical issue, since there is always a human element to consider. Often the human response to emails is the primary reason companies are still vulnerable to virus attacks.

The breadth of offences that are encompassed by the term "cybercrime" or "e-crime" is a complicating factor in attempting to police it. In fact, no single authority has absolute control of the issue and some state police departments have developed their own strategies regarding particular elements of cybercrime. The Victorian Police Service, for example, has had a Computer Crime Investigation Squad (CCIS) in place since 1993 and its task has been to aid in the discovery and handling of technology-related offences. It liaises with Internet Service Providers (ISPs) and is primarily responsible for developing computer crime investigation and computer evidence handling procedures, as well as Internet investigation practices. Interestingly, a special section of the NSW police, the Child Protection Enforcement Agency, has established the Child Exploitation Internet Unit to help with the crackdown on Net-related offences regarding children. These

include offences relating to child paedophilia and child pornography. It tends to take a more proactive approach with this problem by analysing Web sites and newsgroups which could lead to possible offenders. All state police departments have units that handle several types of fraud, including those that are technology related. South Australia's Serious Fraud Investigation Branch handles the state's problems relating to cybercrime offences that have a white-collar aspect, including fraud and false pretences, theft, breach of trust and secret commissions.

The widely varying types of cybercrime tend to be reflections or instantiations of "real" world crimes. A particularly disturbing variant of this is the offence generally referred to as cyberstalking. A brief report issued by the Australian Institute of Criminology (Ogilvie, 2000) examined the complex issues surrounding this new form of stalking. The report identifies three major forms of cyberstalking: email stalking, Internet stalking and computer stalking. Email stalking is similar in many respects to traditional forms of stalking "*In many ways, stalking via email represents the closest replication of traditional stalking patterns."Given that the most common forms of stalking behaviour are telephoning and sending mail, the adoption of email by stalkers is not surprising."* Email combines the immediacy of a telephone call with the separation entailed in a letter, and is often used to threaten or traumatise a person. Fortunately, it is this particular type of cyberstalking that tends to get prosecuted. Ogilvie believes that, while some may think that email communications are "less-invasive" than telephone calls, "*email harassment constitutes an uninvited and arguably threatening incursion into private space*".

Internet stalking is a much broader method and generally moves from the private sphere to the public realm. Offenders might choose to take on the identity of the person they are stalking in chat rooms or they might publish to a Web site personal details of the victim. Ogilvie explains that this form of cyberstalking is the one most likely to spill over into the real world. The final form of cyberstalking, computer stalking, requires a reasonably high level of technical knowledge and is not as common--or distancing--as the other forms. Essentially this form of stalking results in the offender somehow being able to control the victim's computer via the Internet, using various software tools and scripts. This is not a common form of stalking and, in fact, there only appears to be one recorded instance of this type of offence. While Ogilvie accepts that these offences impinge on personal freedom in "cyberspace", she also notes that the most effective means of control is prevention, either through personal protection or using technological solutions such as filtering.

3. State of E-Commerce in Australia

The Internet, a network of computer networks that has no central control or organisation, is changing the way people think about and do business. From its military, research and academic background, it has evolved into a serious business tool. In Australia organisations are using the Internet to satisfy communication, network and research needs and increasingly to sell goods and services on-line to consumers able to pay using secure credit cards and digital cash. The Global Internet Banking Report: An Asia Pacific Japan Perspective (Hickman, 1997) showed that Australia and Canada have the most advanced on-line banking capability. There has been an explosion of names to identify doing business electronically, such as electronic commerce, eCommerce, iCommerce, Internet commerce and digital commerce. In this book we will use the terms `electronic commerce' and `Internet commerce' interchangeably. Electronic commerce can be defined as the buying and selling of information, products and services via computer networks today and in the future, using any one of the myriad of networks that make up the Internet. However, Kalakota and Whinston (1996) point out that electronic commerce has many definitions depending on the perspective from which you view it. These ideas have been summarised in Table 1.

Perspective	Description
communications	to deliver information, products/services and payments over the telephone, communication networks or other means

business	to automate business transactions and work flows
service	to cut service costs while improving the quality of goods and increasing the speed of service delivery
on-line	to provide the capability of buying and selling products and information over the Internet and other on-line services

Table 1. Electronic commerce from different perspectives

While the Internet was established in the 1960s in the United States of America, it was not until the 1990s that its commercial potential started to be realised. Prior to that, the Internet was an academic and research tool for government, educational and non-profit organisations that was subsidised by the government and kept strictly out of reach of the business community. In the mid-1980s the National Science Foundation created a high-speed, longdistance telecommunications network into which other networks could be linked. (Other organisations now support this link.) By 1991 the National Science Foundation dropped its restrictive usage policy and allowed in many commercial sites (McKeown and Watson, 1996). This development, along with the arrival of the World Wide Web, caused the business community to take notice of the Internet. The Web is a graphical hypertext environment that operates within the Internet. It supports multimedia presentations, which include audio, video, text and graphics. The protocol (a set of rules, procedures and standards) that underpins the Web is Hypertext Transfer Protocol (HTTP) and the protocol for doing business on the Web is Secure Hypertext Transfer Protocol, which provides a basis for secure communications, authentication, digital signatures and encryption.

Electronic data interchange (EDI) and e-mail have been used for years in work flow and re-engineering applications. Many large businesses and government departments in Australia have insisted that their suppliers use EDI if they wanted to continue supplying them. As a result some companies who could not afford such expensive hardware and software lost contracts. However, the Internet combined with EDI offers businesses the opportunity to become part of the digital commerce phenomenon in the nineties. Harris Technology in Sydney has a successful Web site and also uses EDI to communicate with its supplier.

Automation in the financial services industry began with back office functions (e.g. cheque processing in the 1960s), followed by new systems for credit card processing and wire transfers. Next, teller stations in local branches were automated to allow direct entry of particular transactions and direct access to customer account information. In the 1980s automation went from behind the counter to the customers via automatic teller machines (ATMs). In Australia the customer acceptance of ATMs was not particularly fast, but ATM-style banking is now very popular. The concept of digitally transferring funds (electronic funds transfer or EFT) between banking institutions has expanded to personal banking with ATMs, ATM cards and point-of-sale machines. In the 1990s the personal computer moved from the office to the home, and financial institutions are extending their technology to bring services to customers' personal computers (or telephones) at home and at work. The institutions have found such facilities lower the cost of servicing customer transactions, while increasing revenue sources. These facilities also make the institutions more competitive in customer service, which leads to increased customer loyalty (Flanagan, 1997)

The Internet commercial domain (indicated on a URL by ‘.com') was the fastest growing segment over the last two years. In Australia there are now so many commercial domains registered that some companies are going offshore to Norfolk Island to register their domain names. Many Australian companies are also registering their business names in the United States where it is cheaper and where a country code (e.g. Australia's country code is ‘.au') is not added. Some Australian cyber businesses believe that having a `.au' on their domain name could deter overseas shoppers from dealing with them. New domains are being set up as well, such as `.firm' and

`.store'. Obviously for businesses it is important to have a URL that reflects the business name. For example, an Internet/ internet consulting and training business called Cyber.Consult has a registered domain name and virtual server at http://www.cyberconsult.com.au. Thus, it is easy for people to quickly work out what a business address is, whether it is for BHP, David Jones or Cyber.Consult. It is vitally important for companies to register their Internet addresses as there have been cases of `forward-thinking' people registering well-known brand or company names and then asking the legitimate company for money to buy the `Net' name. Registration of commercial domain names in Australia has been characterised by some problems, especially "cyber-squatting" (Lowe, 1997)

A paradigm shift is driving new business practices within the financial services industry. Financial institutions desire to build new computer systems across an open platform to handle the shift to secure digital transactions. Four critical issues are impacting the speed of the evolution:

- the need for improved technology to ensure the security of the transaction
- the availability of a variety of payment protocols
- system reliability for twenty-four hours a day times seven days a week operations
- the flexibility of the platform to absorb new capabilities as they become available. (Coleman, 1997)

Just as the banks have seen how computer networks improve their viability, businesses have started to recognise that the Internet allows:

- company and consumer transactions over public networks for home shopping and banking
- transactions with trading partners using EDI
- information-gathering, such as market research
- information distribution transactions. (Kalakota and Whinston, 1996)

Ways of doing business have been dramatically changed by the use of information technology - old ways of dealing with customers, suppliers and employees have been destroyed and replaced by radical new ways. Harvard economist Joseph Schumpeter called this creative destruction. He believed, more than 50 years ago, well before the Internet was even a dream, that what has been destroyed is more important than what has been retained and that only by destroying old ways of doing business, can we create new ways (McConnell and Brue, 2001). Let us consider an example that is very common in Australia in the 1990s. With the restructuring of businesses in Australia, many middle managers found themselves without jobs. These were often people in their late-forties who had identified closely with firms for which they had worked over the past 20 years. Many of these people had to destroy their way of marketing themselves as potential loyal employees and become sole practitioners. They could no longer find positions that would enable them to have secretaries, assistants and various support mechanisms to get them through the working day. For such people to survive, they had to reinvent themselves and become proficient in the use of information technology themselves. If they obtained a private consulting job, they had to do all the parts of the job themselves, such as typing the report, preparing the invoices, doing their own research and running the modelling software.

Old business practices had to be thrown out and new information technology practices brought in. It is important for businesses to have an idea of what Internet commerce can offer them before they try it. Below are some of the key points of what Internet commerce can mean for business:

- Strategic competitive advantages: The Internet and Intranets give businesses the opportunities to improve their internal business processes and customer interfaces to create a sustainable, competitive advantage. If businesses take up the challenges quickly, they have the opportunity to leapfrog over the competition. Many Australian employment agencies have been quick to see the potential of listing job vacancies on-line. Morgan and Banks encourage on-line resume applications. This has in turn led to a radical rethink on how to write resumes and has led to

specialists setting up businesses to advise on resume construction for the Web. Such resumes should contain key words that will be picked up by Web search engines.

- Managers need to be aware of the potential: Managers must be educated so they can see the possibilities of the Internet. In Australia managers are often technically illiterate and proud of it. If this is the case, it is difficult for them to see the advantages that are offered by the Internet. It is important that executive education on the Internet be put in place to ensure that opportunities are not lost. Under Corporations Act 2001, sections 180 and 189, a dirtector is required to exercise his/her duties with a degree of care and diligence that a reasonable person would exercise if they were a director of a corporation in the corporation's circumstances and occupied the same position, and held the same responsibilities as the director in question. It also provides that it is possible for a director to rely on information or professional expert advice, provided that reliance is in good faith and occurs after the director has made an independent assessment of that information/advice having regard to the director's knowledge of the corporation and the complexity of the structure and operations of the corporation. This is a roundabout way of saying that a director is obliged to act competently and use his/her brains to the best of his/her ability. This means that a manager can expose himself/herself to legal liability if the corporation is not even considering the impact of the internet on its business, or if its value diminishes through lack of protection of its intellectual capital, or because an internet opportunity was not taken up or invested in with proper diligence, or even if that manager did not ensure that there is an adequate flow of information from the management team to himself/herself on these issues.

Different companies in Australia have undertaken different tactics to ensure that their staff becomes aware of the potential of the Internet. After a series of seminars, a Vocational Education Training Accreditation Board (VETAB) accredited introductory course on the Internet and the Web was offered to all members of corporations. This course forms part of the corporations' strategy of upgrading their staff's information technology skills. A course in electronic commerce on the Internet has been developed by Cyber.Consult as corporations are interested in exploring the possibility of using the Internet commercially. Sydney-based Karen Scott of Internet Training & Support designed its course 'Untangle the Web' specifically for business people who are apprehensive about using the Web and need to gain confidence and competence quickly. They use games, music and advanced learning techniques to convert fear into fun in their Internet courses.

In Australia some organisations have merely set up a Web site to demonstrate that they are technically `with it'. This was a reasonable strategy in 1995, but by 1998 it was vital to be more than a mere presence. Organisations started transforming themselves into new digital commerce centres and opened digital markets. This digital marketing opportunity provide sellers with the opportunity to personalise their goods and services to one consumer at a time - the antithesis of mass marketing. Netscape's browser cookies (files that a Web server stores on a user's computer) allow companies to create a more personalised Web interaction for consumers, but this is fraught with danger if companies don't ask users for permission first.

Some Australian companies have shied away from the Internet because they had security fears but at least they have seen the value of the internet within the organisation. Use of Intranets to enable employees to carry out tasks such as ordering hardware or software or requesting time off demonstrates the value of such a user-friendly interface. It can also pave the way for the organisation to communicate with the outside world on the Internet and communicate with suppliers and customers via Intranets. A NOIE report (NOIE, 2000) focuses upon what difference greater use of e-commerce will make to current forecasts of economic outcomes. The study therefore concentrates on activities that are viewed as being likely to experience significant change. This includes impacts brought about by the emerging widespread potential for consumers and businesses to undertake electronic transactions over the Internet. This is a new and rapidly growing activity that is not likely to have been fully factored in to most economic forecasts. Other aspects of e-commerce, including electronic transactions undertaken over less accessible or

proprietary networks such as the payments system, the use of EDI, ATMs or EFTPOS are already largely factored in to the economic outlook. The net benefits will be realised if, as expected, widespread adoption of e-commerce proves to be a more efficient mode of doing business and the benefits exceed the costs. If this is the case, it could produce a growth dividend as a result of freeing resources that can be used in other parts of the economy. The main sectors that expand are expected to be those that offer products and services that are amenable to e-commerce. This includes sectors such as media and entertainment, and banking and finance. Some sectors will be larger because of flow-on effects as changes ripple through the economy; housing is one example. Industry sectors that are essentially 'disintermediated' by the use of e-commerce (such as retail and wholesale trade) may have lower output than otherwise. Industries involved in commodity exports may be sensitive to flow on impacts (particularly higher real wages and a higher real exchange rate). The efficiencies brought about by e-commerce are expected to result in changed employment opportunities. Some sectors will expand and increase job numbers, others will be smaller than otherwise. Overall, employment will expand. Demand is likely to be strongest in occupations that are related to tourism and associated support services. It is possible that a flow on impact of the productivity gains and growth could be a temporary minor deterioration in the balance of trade. Looking into the medium term, the export enhancing benefits will outweigh other factors and the trade situation will improve.

Another interesting report (NOIE, 2000b) seems to assert that all medium-sized businesses and over 80 per cent of small businesses in Australia use personal computers. Over 35 per cent of all businesses have an online presence—a comparative business advantage that translates into Australia being consistently rated in the top ten nations globally for its e-commerce environment. Over half of Australian households have personal computers and close to 35 per cent have Internet connections with penetration rates increasing rapidly. Five per cent of Australian adults shopped via the Internet in the 12 months to February 2000, and 74 per cent paid for their purchases online. Take up rates of other kinds of e-commerce—such as telephone banking and electronic funds transfer—were even higher. E-commerce creates a powerful capacity to open up new markets and to create unprecedented efficiencies. The landmark E-commerce Beyond 2000 report released in February 2000, found there are significant net benefits from the impact of e-commerce—for instance, Australia's GDP is expected to increase by 2.7 per cent ($AUD 15 billion) by the year 2007.

4. Current Legislative Ventures and Government Stance

In Australia the Federal Government is taking the general view that while it should facilitate and enable e-commerce to take place, it should allow the market to regulate the standards which are going to apply.

Several pieces of legislation have now been passed by the Federal Government which relate to e-commerce. The Electronic Transactions Act 1999 was the first. It was designed to enable, or facilitate, the development of electronic commerce in Australia (whether occurring over the internet or other media) by 'removing existing legal impediments that may prevent a person using electronic communications to satisfy obligations of the Commonwealth law'.

Due to the constitutional limitations which restrict the operation of legislation passed by the Federal Parliament, each Australian State and Territory will be required to enact mirror legislation to the Electronic Transactions Act if the Act is to have ubiquitous coverage throughout Australia. The State and Territory governments have agreed to do this and, at the date of publication, similar legislation has been passed in the Northern Territory and all of the remaining States, other than Western Australia.

The legislation which is being promoted by the State and Territory governments is similar but not identical to the Federal legislation. The term 'Electronic Transactions Legislation' is used from now on to refer generally to the Federal and State legislation. The comments which follow summarise the effect of the legislation rather than precisely reproducing the provisions of each Act.

The Electronic Transactions Legislation is only an enabler of electronic commerce. It does not regulate electronic commerce and cannot be relied upon to provide an answer if you have forgotten to consider the legal issues which might apply to the operation of your website. In the absence of special purpose legislation (in the Wild West) you are responsible for ensuring your own safety. Indeed, it is probably not going too far to say that you ought to trust no-one in this space. This is not to say that everyone else is untrustworthy-rather, in the absence of a well established body of law there is greater scope for uncertainty to arise which those with whom you are dealing may seek to turn to their commercial advantage. Australia was hailed as "one of the first in the world to pass comprehensive legislation designed to remove the legal uncertainties relating to electronic transactions. The combination of this bill with privacy legislation will serve to encourage the uptake of e-commerce in Australia." (Ralston, 1999).

Under the Electronic Transactions Legislation paper-based commerce and electronic commerce are to be treated as equivalent. The Legislation is technology neutral so that it does need not be continually updated in order to keep up with advances in technology.

The keystone of the Legislation is the provision that a transaction will not be invalid because it takes place by means of one or more electronic communications. An 'electronic communication' means a communication of information in the form of data, text or images by means of guided or unguided electromagnetic energy. 'Transaction' is defined as including a transaction of a commercial nature. This means that transaction will be given its ordinary commercial meaning. In brief, where you are not dealing with the Commonwealth Government, the Electronic Transactions Legislation provides that (AGD, 2000):

- a requirement under the Legislation to give information in writing, provide a signature, produce a document, record information or retain a document can be met in an electronic form;
- the purported originator of an electronic communication is bound by it only if the communication was sent by the purported originator or with the authority of the purported originator;
- for information given by means of electronic communication to be acceptable, it must be reasonable to expect that the information will continue to be accessible for subsequent reference and the recipient of the information must consent to it being given electronically;
- where a person is required to give a signature, he or she is entitled to use an alternative means of authenticating their identity. In order for the alternative means to be acceptable, it must identify the person and indicate the person's approval of the information being communicated, and it must be as reliable as is appropriate for the purposes for which the information is communicated. The recipient of the information must also consent to the use of the means. This will enable different levels of authentication protocols to be used depending on the nature of the transaction;
- if documents are stored electronically the information should continue to be accessible for future reference and the method for storing the information must comply with any specified requirements as to the device or media on which the information is stored. The method for retaining information must provide a reliable means of assuring that the integrity of the information will be maintained;
- the Legislation also provides rules relating to the time and despatch and receipt of electronic communications:
  - despatch occurs at the time when the communication first enters an information system (a term which is not defined) outside the originator's control;
  - receipt occurs at the time at which the communication first enters an information system designated for receipt by the addressee (if no information system is specified) the time at which the communication first comes to the attention of the addressee;
- the place of despatch and receipt is generally taken to be the place at which the originator of the communication or the recipient of the communication (respectively) has its principal place

> of business. However, if either party has more than one place of business then, if one of those places has a closer relationship to the underlying transaction, that place of business is the relevant place of business for the purpose of determining the place of despatch or receipt. [The physical location of information systems is often irrelevant to the purposes of electronic communication because an information system can be in a different place to that where the parties to the communication are located. It is often easier to determine the place of business or residence of a party than to determine the location of an information system from which that communication was sent or received.]

In dealing with the Federal Government the same provisions apply but there is also the need to comply with any specific requirements imposed in each case by the Government.

Developments in ICT had exposed gaps in copyright protection under the Copyright Act. The Digital Agenda Legislation recognised that creators and owners of copyright material need to protect their rights on the Internet and that large users of copyright materials (eg. libraries and universities) need to be able to maintain a reasonable access to copyright material in a digital form. This legislation amended the Copyright Act by – among other things:

- permitting temporary reproductions to be made as part of the technical process of making a communication – i.e. temporary reproductions made in the course of browsing or viewing copyright materials online and in certain types of caching;
- imposing criminal sanctions against the manufacture, commercial dealing, importation, advertisiing, marketing and supply of devices used to circumvent technological protection measures such as program locks or encryption;
- creating new criminal offences and civil remedies regarding the intentional removal and alteration of electronic rights management information or the commercial dealing with copyright material where that information has been removed; or
- permitting an owner of copyright to make a digital copy of that work.

Rights management information refers to information about the ownership of the work which is embodied in a copy of a work electronically and which cannot be read visually (IFPI, 2001)

5. Cyberlaw and Electronic Commerce

In the new millennium, electronic commerce is emerging as a key engine of economic growth in developed economies. Electronic commerce provides opportunities for business to reach global customers and gain access to new markets; create new products and services; realise new sales opportunities; lower costs; reduce inventories and cycle times; provide more efficient and effective customer service and increase productivity.

With our increasingly computer literate society and advanced telecommunications infrastructure, Australia is well placed to `punch above its weight' in the information economy. The Federal Government is committed to building:

- a technologically literate workforce and consumer population with access to competitively priced and world-class infrastructure, hardware and software;
- a commercial culture, extending to smaller firms, of identifying and maximising the beneficial potential of on-line business;
- compatibility between Australian and international technical and regulatory standards; and
- business and consumer confidence in electronic commerce.

Whilst changes must be made to laws and regulations to accommodate electronic commerce, there need not be a legal revolution to match the technological one. In many areas of law and policy, only minor changes are called for to allow electronic commerce to progress along the same lines as traditional commerce.

In the process of developing an appropriate level of regulation, governments need to be guided by certain principles and objectives:

- all citizens, regardless of where they live and work or their economic position, should have equitable access to the information economy;
- industry self-regulation and competitive market based solutions are preferable to government imposed regulation, unless there are overwhelming reasons for government intervention;
- government should intervene in the market place only to ensure that the Internet is a safe and secure place to do business, for example, by protecting the intellectual property of material provided on the Internet;
- consistency of national approaches with agreed international positions.

The global network technologies which underpin electronic commerce create a borderless world which challenge our existing national policy frameworks. This was recently highlighted at the OECD Ministerial Conference in Ottawa, *A Borderless World: Realising the Potential of Global Electronic Commerce* (Dryden, 1998). OECD Ministers concluded that international cooperation is an important aspect of policy development for the digital age and that "whether the action is domestic or regional, private or public sector, all electronic commerce policies and activities will have limited impact unless they facilitate a global approach." Ottawa conference participants discussed the issue of trust in electronic commerce, recognising that consumers and business will not fully embrace electronic commerce until they are confident that services and networks are secure and reliable, that transactions are safe and private, and that redress mechanisms are available. A key theme which emerged from Ottawa was the tendency towards hybrid regulatory solutions which balance social and equity principles with economic concerns about regulatory burdens. For example, in the area of consumer protection, various approaches are being developed to implement and enforce consumer protection principles in the on-line environment, including legislative or regulatory, self-regulatory, technological or contractual mechanisms.

The Australian Government's overall regulatory objective is an internationally consistent legal framework that will:

- remove existing uncertainties affecting electronic commerce;
- put electronic commerce and paper-based commerce on the same legal footing;
- not discriminate between different forms of technology.

This framework brings together many policy areas for addressing the interests of business and consumers, all of which I am pleased to see are covered in this special edition of the Law Journal: security, privacy, electronic signatures and authentication, protection of intellectual property (while guaranteeing important educational benefits from free Internet access), consumer protection, Internet content standards and taxation administration.

Some of the approaches being adopted by the Australian Government to increase confidence of Australian consumers and businesses in electronic commerce. The Federal Government is:

- proposing to legislate for the recognition of electronic signatures and related aspects of evidencing and recognising on-line contracts, broadly consistent with the Model Law proposed by the UN Commission on International Trade Law;
- facilitating access to and use of authentication and encryption technology and systems, recognising that consumers and business (especially smaller firms) expect to have confidence in knowing the identity of other on-line parties.
- the Government proposes to establish itself as an example of good practice, with the GATEKEEPER project for authenticating on-line parties doing business within government or with government purchasing agencies.
- consultations with industry are proceeding on Commonwealth initiatives for developing confidence in authentication processes being offered by e-commerce intermediaries.
- government adoption of the OECD Encryption Guidelines.
- encouraging the production and use of on-line content through proposed amendments to the *Copyright Act* 1968 (Cth) to:

  - create a right of communication to the public to cover the transmission and making available of copyright material, for example on the Internet.
  - make exceptions to the communication right for fair dealing, and access by libraries, archives, galleries, museums, schools, colleges and universities.
  - improve enforcement measures targeted at protecting copyright material made available on-line.

- encouraging business to implement the *National Principles for the Fair Handling of Personal Information*, released in February this year by the Privacy Commissioner.
- committed to enhancing on-line consumer protection. The recently released *Principles for Consumer Protection in Electronic Commerce* will be complemented by further guidelines on best practice approaches to dispute handling and industry conduct, greater cooperation in enforcement activity involving electronic commerce, and readily available on-line consumer related information.
- addressing community concerns about objectionable on-line content through a national industry based regulatory scheme for service providers, a consistent State and Territory legislative framework to guide content providers, the promotion of content labelling and filtering technologies, and educational campaigns.

In Australia, commercial transactions are subject to a comprehensive system of controls consisting of

- the common law
- legislation at the State, federal and international levels
- industry codes of practice.

These controls have been established over time in an ad hoc fashion in response to the need to provide a high degree of certainty in contractual relationships and to give the consumer confidence that he or she will obtain `a fair deal' in any spending decision. Both of these are necessary ingredients in the promotion of trade and commerce, upon which modern economies depend. The controls have evolved and have been adapted to new technologies as they arise, although there is always a time lag before the controls ‘catch up' with the latest technology. Just as the internet is challenging business practices so too is it presenting challenges for the law. Some new laws will need to be introduced and some existing laws will need to be modified to accommodate the new technology. It will take time for this to occur.

We are still at an early stage in establishing controls over commercial transactions on the Internet despite the large volume of transactions taking place daily. Unique features of the Internet compared with previous technological changes are:

- its rapid proliferation
- the multiplicity of communication channels
- the enormous volume of information and range of services available
- the ease with which trans-border transactions can be conducted.

All of these pose a unique set of problems. Although international agreements do exist for the regulation of international trade, they are not keeping pace with commercial realities. The principal problem is that existing agreements, and even those proposed, deal only with business or trade transactions. They do not deal with consumer purchases, which are responsible for the huge growth in transactions over the Internet.

However, for the most part fundamental legal principles will continue to apply to the use of the internet in commerce. It is still commerce, only the medium through which it is conducted has changed. In most cases one only needs to go back to the basic legal principles in the offline world) and apply them to the new medium. As the judge who heard the Gutnick vs Dow Jones case forthrightly said "Bold assertions that the internet is unlike other [information repository and

delivery] systems do not lead to the abandonment of the analysis that the law has traditionally and reasonably followed to reach just conclusions." For example, the traditional principles which regulate the formation of a contract can be applied to contracts formed over the internet without much adjustment. In getting a business online some of these principles may (and often are) overlooked. They may be forgotten because of the apparent ease of setting up a business online or because of the desire to get it done quickly. These principles should not be overlooked unless you want to be remembered for attempting to change a well-established legal principle through protracted and costly litigation.

Even though the law applies in cyberspace, the risks of doing business are probably greater. Doing business in the so-called Wild West of cyberspace need to exercise more care in their relationships with business partners and need to guard even more against the loss of their intellectual capital. The need to do these things results from a combination of the digitisation of information, the speed at which commerce occurs over the internet and the global reach of the internet. Major concerns include how the security of commercial transactions over the Internet can be maintained and how the consumer's interests can be protected, including the individual's rights to privacy. Added to these are issues associated with protecting a society's values, exemplified by government's role in controlling content on the Internet, particularly in relation to censorship. Intellectual capital has been described as the business asset of the 21st century. In an environment where there is less employee loyalty, more employee mobility, an increasing amount of digitised information and (often) easy access to computer systems, there is a greater risk of loss of intellectual capital. Business needs to manage its intellectual capital in a way which sees that capital preserved for its benefit rather than for the benefit of its customers, suppliers or employees.

One of the first steps in trying to establish a legal framework for any new technology is to classify it in order to establish how existing legislation may be made to fit the new technology. Although the Internet service provider has become the major focus for attempts at legislative controls, there is a wide variation between each country's approach (Vaughan, Sewards and Kelso, 1997). An International Working Group has been established to consider controls on content rating (Lawrance, 1997). Commercial interests have also established the Platform for Internet Content Selections (PICS) developer group to provide a rating system for home pages.

In Australia, the no longer existing Senate Select Committee Report (SSC, 1997) has argued that Internet content should be treated in the same manner as a broadcast medium such as television. One of the outcomes of the report is to make the Federal Government's Telecommunications Industry Ombudsman available to hear complaints from users of the Internet (however, not about content). A number of recommendations in the report are designed to restrict the use of the Internet for transmission of objectionable material, including, most importantly, pornography, and to promote measures to protect children from viewing such material. The Department of Communication and the Arts (DCA, 1997) wants the Internet service providers to establish an industry-wide self-regulation system of content control to be supervised by the Australian Broadcasting Authority. However, some user groups disagree [see, for example Electronic Frontiers Australia]. In the face of increasing regulation, the Internet industry has set up the Internet Industry Association of Australia to present a united front to protect its interests.

As an example of issues pertaining to legislation with regards to electronic commerce, we will now take a look at jurisdiction and copyright.

5.1. Jurisdiction

The term ‘jurisdiction’ describes a system under which laws are administered (Mgabadeli, n.d.). Every country has established its own network of laws governing most aspects of private and commercial life in response to the country's social, political and commercial circumstances. A few legal systems prevail across groups of countries. Australia, together with most of the English--speaking countries, has the `common law' system inherited from England. However, although this leads to some similarities, any dispute may receive a different interpretation and have a different

outcome depending on which State of Australia the dispute occurred in. Laws established at international forums have been adopted by many national governments, but these represent only a small part of each country's legislative base. There is a large body of law called Conflict of laws, which is directed toward identifying which jurisdiction's law is to be applied to any dispute. That is, whether the dispute has broken State, national, foreign or international law, and which is the most suitable court, or 'forum' in which the dispute is to be heard.

In order for a court to hear a matter with a trans-border dimension, various tests have to be applied to determine the appropriate, jurisdiction. A key consideration is that one party to the hearing or the subject matter of the hearing must have some connection with its jurisdiction; for example, that a contract was signed within the jurisdiction. However, all manner of complications can occur. The other party may be resident overseas and may decide not to appear to defend the proceedings. In that case, even if the court were to make a judgment in the plaintiff's favour, the plaintiff may not he able to enforce the judgment. It is possible to enforce judgements outside Australia only in a limited number of countries (such as the United Kingdom) under reciprocal arrangements. Alternatively, the aggrieved party may have to take action in the defendant's jurisdiction by commencing new proceedings. The other party may even initiate counter proceedings in a foreign jurisdiction. Further complications arise when evidence required for the hearing is outside the court's jurisdiction and it may not be possible to compel the evidence to be made available, effectively bringing the action to a halt. These are the sorts of problems that can occur in the more conventional modes of commercial transactions. They are increasingly likely to occur also with transactions conducted over the Internet because much of the trading is conducted outside the existing legislative framework. Although it may be thought that laws are slow to develop, the very medium of the internet has enabled court decisions, particularly from North America, to be disseminated around the world very soon after the decision is made public. To date there have been few judicial decisions in Australia on internet disputes. The dissemination of judicial decisions, even if they have arisen in other countries, will help to speed up the development of the common (or judge-made) law in Australia when internet disputes do arise.

The nature of disputes may also differ depending on the identity of the claimant (private consumer/commercial customer/government body/etc.) Unless the parties to an electronic transaction have thought through the issues involved in the transaction, it may be difficult to pinpoint the applicable legislation to cover the rights and obligations of all parties involved. This applies especially to contracts made over the internet. The two most important issues to consider in cross-border disputes (and many internet disputes are cross-border) are: which law applies and in which court has the jurisdiction to hear the claims.

While before the internet age, companies wanting to expand usually established subsidiary offices or some other form of representation in the host country, and thus became liable under the laws of that country, e-commerce presents more difficult issues to deal with. These include:

- risking legal liability in a country in which the corporation may not have planned to make sales and has not therefore undertaken a pro-active risk management strategies;
- the inability to successfully block customers from embargoed countries, or countries with which commerce is not desirable, because of the difficulty of correctly identifying the customer’s location;
- risking a far greater number of claims due to the worldwide expansion of the Internet business
- goods being classified differently in the country of offer from the country of origin, and tax issues arising from this difference
- difficulties in identifying the purchaser as a “consumer” in need of greater protection (underage children, for example)

Since the majority of Internet transactions currently involve relatively small amounts of cash, making litigation not worthwhile, there are few claims being made. Two good examples of how Australian courts dealt with a cross-border dispute are Paper Products v Tomlinsons Limited (1994) and Macquarie Bank v Berg (2000). In the first case, Tomilsons is a British based company

producing egg carton making machines. Paper Products, an Australian company, purchased one of Tomilsons machines using phone and fax. The machine failed to meet the specifications and representations made by Tomilsons' representatives and Paper Products litigated claiming breach of the Australian Trade Practices Act. The proceedings were brought in Australia, even though Tomilsons had no physical representation in this country. The court upheld the case and ruled Tomilsons liable to pay damages, since the representation was made in Australia. In the second case, Mr Berg, who resided in USA, provided services to Macquarie Bank, but then a dispute ensued over whether he was contracted or employed by the bank, and his services were terminated. He commenced proceeding in the Industrial Court of NSW (in Australia) seeking compensation. While the proceedings were taking place, the bank discovered a website (www.macquarieoriental.com) that had information about the bank's executives and its business practices. The court accepted that Mr Berg was associated with the website. The site resided on a server in the USA, and therefore any material published on the website was outside Australia. The bank took action to stop the defamatory material from being published, but the Australian court decided it did not have the jurisdiction to rule in the bank's favour. The court held that io grant such an injunction would interfere with Mr Berg's right to freedom of expression, as there was no way it could be limited to NSW, and especially as there was no way of ensuring that Mr Berg would ever return to NSW. This was a ruling very different to a third case, in which such an injunction was granted (ASIC v Matthews, 2001).

While Australia has arrangements in place with a few countries for the recognition of judgements obtained in Australia, it does not have these arrangements with most other countries in the world. This forces the defendant to essentially start proceedings and prove the claim for a second time in the other country. Add to this the fact that it is often very difficult to ascertain that the pursuant company has any assets which would make it worthwhile to take legal action against it. However, cooperation is happening between law enforcement and regulatory bodies around the world and therefore there may be circumstances in which a local government agency will be persuaded to take action on behalf of individuals (see ACCC v Internic Technology, 1998).

This is therefore an area of law which will need to develop to meet the challenges presented by the technology. This will take some time, and until it is done, Australian businesses will need to exercise care based on precedent and do what they can to prevent disputes from arising in the first place.

5.2. Copyright and Intellectual Property:

Copyright protects a wide array of material (including writings, artwork, music, films and computer programs) and extends to broadcast material, quite separate to the copyright in the material that is transmitted. The copyright automatically belongs to the creator, or the owner, from the time of creation of the material. International treaties, such as the Berne Convention, provide for protection of Australian copyright owners overseas and foreign copyright owners in Australia, although the rights vary from country to country according to different subject matter. The copyright notice `©' is not required for protection in Australia. The copyright owner has the right to use the material in a variety of ways and the rights may be assigned or leased with or without limitations or conditions. Use of copyright material, usually by copying without the permission of the owner, will ordinarily be an infringement of copyright. There are some circumstances in which an exception is made, such as a student copying a limited portion of a book. Essentially, the same restrictions placed on copyright will apply to copyright material placed on the Internet. In 1997, the Australian Copyright Law Review Committee has recommended that screen displays and temporary RAM storage from the Internet are not to be regarded as the making of copies, although downloading to hard disk and printing out will be so considered (CLRC, 1997). This led to the amending of the existing legislation.

The first copyright laws were passed in England in 1709 (Davies, 1994), to protect those who invested time and effort in writing and distributing written works against unauthorised printing of

their works which may bankrupt them. In time it became a statutory monopoly designed to encourage the progress of science, industry and the arts by giving authors, artists and others the exclusive right to exploit their works. In Australia, the law relating to copyright is found in the Copyright Act, which has been amended and added to over the years to deal with the introduction of new technologies. The most recent addendum is the Copyright Amendment (Digital Agenda) Act, addressing consequences of digital technology. It added the important right to "cause the work to be communicated to the public", and is intended to be technology neutral and covers making copyright material available by uploading it onto an internet server (Clarke, 1998).

How does copyright affect e-commerce? The general rule is that the owner of a copyright in a work is the creator of the work in which the copyright resides. There is an exception to this rule, however. Where the creator of the work is an employee of a business, and the work is brought into existence during the course of that employment in accordance with the fulfilment of the employee's duties, the copyright in the work is owned by the employer. However, there is always scope for the employee to claim that the work was done in their own time or not in fulfilment of their duties. Disputes have arisen in this area in regards to patents, when the employee has invented something that is – or has the potential to become – commercially valuable. Courts usually rule in the interest of the employer.

In the 21st century when more businesses rely on their intellectual assets, business needs to take care with the creation of materials, which can be protected by copyright, particularly in circumstances where employees may work from home (or telecommuting) and where job descriptions may be broad or change over time. It is better to resolve any doubt which may arise about the status of copyright materials by including appropriate provisions in employment contracts, which will need to be carefully drafted.

It is also an issue that must be dealt with in any arrangements under which someone is contracted to bring into existence material in which copyright exists. The copyright in such cases remains with the contractor unless otherwise specified in the contract. In the IT and e-commerce, much work is contracted or completely outsourced, often without adequate documentation. A few companies have found that they had to pay their web designers a fee for the assignment of copyright of their website materials when they needed to sale the business or move to a different web developer. Paying for the website to be designed only gave them the right to use the work on the site for which it was written.

Care also needs to be taken that the work with which an employee or a contractor provides a business does not infringe the copyright laws of a third party. In the case of Antiquesportfolio v Rodney Fitch (Mercer, 2000), the claimants (a UK firm) had instructed the defendants to carry out design work in relation to a web site for the buying and selling of antiques. The claimants subsequently contended that the material supplied by the defendants infringed copyright in that it was based on photographs of antiques in an encyclopaedia published by a third party. The first issue was whether any term was to be implied into the contract between the claimants and defendants in relation to the material. The court rejected the defendants' submission that the term to be implied was that the claimants would have undisturbed use of the design work supplied by the defendants so that they only had an action against the defendants if the person whose copyright was allegedly infringed brought proceedings against the claimants. In the court's judgment, there was an implied obligation to carry out the design work with reasonable care and skill and that obligation carried with it a duty on the defendants to use reasonable care not to include material knowingly copied from a third party. The second issue was the extent to which a photograph of a single static item could be said to be protected by copyright. In the court's judgment, copyright did subsist in such a photograph. In the case of a three dimensional object it could be said that the positioning of the object, the angle at which it was taken, the lighting and the focus were all matters judgment which satisfied the requirement for originality imposed by s1(1)(a) of the Copyright, Design and Patents Act 1988 (UK).

Databases form the bases of many e-commerce websites. In Australia the creation of a database can be protected as a work in which copyright exists. Often the creation of a database involves the reproduction of the contents of other databases. This may infringe the rights of the owner of the original database. Usually copying material like this necessitates obtaining permission to copy from the owner of the original database. If the new database includes a qualitatively significant change to the material which has been copied, it then becomes copyrighted in its own right. Mere copying of a database does not constitute reason enough to assert copyright. Originality is not a pre-requisite, as labour is enough in Australia to assert copyright.

Infringement of copyright occurs when a person without the consent of a copyright owner authorises someone else to exercise in Australia the owner's exclusive right to the whole or substential part of a copyright work. Under the Copyright Act, the owner of a copyright work has the exclusive right to exploit the work in various ways. Among other things the owner can publish the work, consent to it being communicated to the public or license someone else to do these things. The word 'substential' in the context of infringment does not necessarily mean a large proportion of a work. Copying the essence of another work by only copying a small part of it may be still result in the breach of copyright. The context of authorising infringement is also important because it is not limited to giving someone actual permission to infringe. Whether or not infringement has been authorised will depend on:

- the extent of your power to prevent infringement; and
- the nature of any relationship between you and the infringer; and
- whether you took any reasonable steps to prevent the infringement

The issue for those businesses which are not involved in publishing is the risk of being made liable for the infringement of copyright by employees downloading materials over the internet using the employer's computer network. Under the Copyright Act one would not be found to have authorised copyright infringement merely by providing the computer network for the employees to use, but one may be liable if you did not take any action to prevent the infringement.

6. International Attempts At Solutions

The Secretary of UNCINTRAL (UN Commission on International Trade Law) has proposed an establishment of an international dispute resolution body to assist in overcoming the jurisdictional problems surrounding e-commerce. The aim of the body would be to overcome the difficulties of establishing the correct jusrisdiction in internet commerce cases and apply the same law to all e-commerce transactions regardless to the location of the buyer and the seller. It was also suggested that the body would use the Internet as its courtroom allowing disputing parties to log into a virtual courtroom to argue their case. The judgements would be paid out of bank guarantees which the litigating parties had already agreed on before the proceedings took place.

However, this utopian solution would not be implemented quickly because of the difficulty of negotiating standards that would be acceptable internationally (Hamano, 2000). Business interests are often contradictory to consumer interests, intellectual property issues are at stake, and negotiations will be hard and protracted.

7. Conclusion

The global network of interconnected computers which comprises the Internet allows users anywhere in the world to communicate and share information. Now that the fireflies of the initial dotcom boom are dying out, business is concentrating on the uses to which this global network can be put to increase their profitability, either by increasing sales or – more likely – reducing expenses. Whatever use one is putting the Internet to, be it a shop front or a back office, there are risks with connecting a business to a fast moving global network.

The aim of this report has been to show some of the legal risks associated with connecting to the Internet network. Unfortunately, in many cases there are no ready made answers for these risks. One needs to develop a strategy which addresses the corporate environment, in which one finds

oneself and the degree of one's exposure to the particular risk. Many of the same issues arise in the offline world.

The law of the Internet, or more correctly the development of the law to meet the issues thrown up by this communication medium, is developing rapidly. Each day there are reports of new, Internet-related legal issues arising somewhere in the world. This shows no signs of abating, even though the issues are often similar.

To this end, doing business online is, for the moment, akin to exploring the Wild West. But the Wild West got tamed and legislated, and before long, so will the word of e-commerce. Until such time, common sense, business acumen and healthy risk management strategies should do, as the possibilities offered by this medium are far to great to ignore in one's timidity.

8. References

Attorney General's Department. 2000. The Electronic Transactions Act 1999 Pamphlet. [Online] Available WWW: http://www.law.gov.au/publications/ecommerce/pamphlet.html

Australasian Centre for Policing Research. 2000. "The Virtual Horizon: Meeting The Law Enforcement Challenges". Report No. 134.1. [Online] Available WWW: http://www.acpr.gov.au/pdf/ACPR134_1.pdf

Clarke, R. and Dempsey, G. 1999. Electronic Trading in Copyright Objects and Its Implications for Universities. [Online] Available WWW: http://www.anu.edu.au/people/Roger.Clarke/EC/ETCU.html

Coleman, A. 1997. Java Commerce: a business perspective. [Online] Available WWW: http://java.sun.com/products/commerce/docs/business/business.html

Copyright Law Review Committee, 1997, Legal Deposit of Copyright Material Under the Copyright Act 1968, http://www.agps.gov.au/customer/agd/clrc/homepage.html

Davies, G (ed.). 1994. Copyright and the Public Interest. London: John Wiley and Sons

Department for Communications and the Arts. 1997. Principles for a Regulatory Framework for Online Services in the Broadcasting Services Act 1992. Canberra: DCA

Deloitte Touche Tohmatsu & Victoria Police. 1999. Computer Crime & Security Survey. Melbourne: Deloitte Touche Tohmatsu & Victoria Police.

Dryden, J. 1998. "Realising the Potential of Global Electronic Commerce" In **The OECD Observer** (214). [Online] Available WWW: http://www1.oecd.org/publications/observer/214/Article6_eng.htm

Federal Court of Australia. PAPER PRODUCTS PTY LTD v. TOMLINSONS (ROCHDALE) LTD; NIGEL WATTS and DAVID MURPHY No. WAG45 of 1993 FED No. 30/94 Damages. [Online] Available WWW: http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal%5fct/unrep6625.html

Federal Court of Australia. 1998. Australian Competition & Consumer Commission v Internic Technology Pty Ltd & Anor [1998] 818 FCA (14 July 1998). [Online] Available WWW: http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal%5fct/1998/818.html

Flanagan, P. 1997. Internet Funds Transfer. Sydney: UTS. p. 27

Hamano, M. 1999. **Comparative Studies in the Approach to Jurisdiction in Cyberspace. Ch. 5. [Online] Available: http://www.geocities.com/SiliconValley/Bay/6201/indexjpn.html**

Hickman, B. 1997. "Internet banking services to soar". In **Australian**, (08.04):3

New South Wales Industrial Relations Commission. 2000. Graham v Macquarie Bank Limited [2000] NSWIRComm 253 (15 December 2000). [Online] Available WWW: http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/nsw/NSWIRComm/2000/253.html

IFPI. 2001. The WIPO Treaties: Protection of Rights Management Information. [Online] Available WWW: http://www.ifpi.org/site-content/library/wipo%20treaties%20-%20rights%20management%20information.pdf

Jiggins, S. 2000. "E-crime: a global challenge for law enforcement". In **Platypus** (December). [Online]. Available WWW: http://www.afp.gov.au/raw/publications/platypus/dec00/ecrime.htm

Kalakota, R. and Winston, A. 1996. Frontiers of Electronic Commerce. New York: Addison Wesley. p. 5

Lawrence, M. 1997, `Watchdogs on Internet content', In **Australian**, (22.07), IT section:4.

Lowe, S. 1997. 'The Domain Name Debate'. In **Sydney Morning Herald,** (28.01), Computer Section:7

McConnel, C. and Brue, S. 2001. Microeconomics. 14th ed. New York: McGraw-Hill Companies

McKeown, P. and Watson, R. 1996. Metamorphosis – A Guide to the World Wide Web and Electronic Commerce. New York: John Wiley and Sons. p. 6

Mercer, N. 2000. Antiquesportfolio.com Plc v Rodney Fitch and Co Ltd. [Online] Available WWW: http://www.lawreports.co.uk/chan_jul0.3.htm

Mgabadeli, S. n.d. Jurisdiction on the Internet. [Online] Available WWW: http://nml.ru.ac.za/carr/siki/

National Office for Information Economy. E-Commerce Beyond 2000. Canberra: Commonwealth of Australia [Online] Available WWW: http://www.noie.gov.au/publications/NOIE/ecommerce_analysis/beyond2k_final_report.pdf

National Office for Information Economy. E-Commerce Across Australia. Canberra: DOCITA [Online] Available WWW: http://www.noie.gov.au/publications/NOIE/ecommerce_analysis/eCommerceAcrossAustralia.pdf

Needham, K. 1997. "Software is the jewel of the new goldrush". In **Sydney Morning Herald**, (19.08):8C

New South Wales Supreme Court. 2001. ASIC v Matthews [2001] NSWSC 735 (30 August 2001). [Online] Available WWW: http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/nsw/supreme%5fct/2001/735.html

Office of Strategic Crime Assessments (OSCA). 1997. Computer Crime and Security Survey, Melbourne: OSCA / Victoria Police.

Ogilvie, E. 2000. Cyberstalking. Australian Institute of Criminology Report No 160. [Online] Available WWW: http://www.aic.gov.au/publications/tandi/ti166.pdf

Ralston, P. 1999. Leading the World in Online Law. In **Australian**, (14.12), IT Section:5

Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies .1997. Report on Computer On-Line Services: Part 3. [Online] Available WWW: http://www.aph.gov.au/senate/committee/comstand_ctte/online3/contents.htm

Vaughan, J., Sewards, T. and Kelso, R. 1997, The Law of Internet Commercial Transactions - Issues Analysis. Melbourne: Centre for International Research on Communications and Information Technologies. pp. 13-14.