



21<sup>st</sup> June, 2001  
Hyatt Hotel, Canberra

*Session 4b: Infoeconomy issues*

**E-commerce Law**

**by**

Dr Moira Patterson  
Law School Monash University

## Infoeconomy Issues: E-commerce Law

### *1 Introduction*

Bilateral free trade between the United States and Australia is not a new idea. It was broached many years ago but failed to proceed. What is different this time is that the mechanisms by which trade takes place are themselves undergoing a technological revolution.

While the Internet has been in existence for many years now it is only in recent times that its potential both as a powerful tool for trade and as a global marketplace has come to be understood. The Internet is especially important for a country such as Australia which is geographically remote from large overseas markets. This is because of its capacity to reduce the impact of time and distance by allowing any item which can be digitised to be displayed almost instantaneously in international markets as well as reducing the substantial overhead cost associated with transportation and distribution of goods and services to other countries. As well as providing a tool for trade, the Internet is also emerging as a global trading platform. For example, trading systems such as financial and commodity markets are now in the early stages of moving to an Internet base.<sup>1</sup>

The extent to which an Australian/US Free Trade agreement is able to produce its hoped for economic benefits will be significantly affected by the legal and regulatory framework which governs Internet transactions. Such an agreement must inevitably put pressure on policymakers and legislators to harmonize substantive legal rules and to develop legal institutions to facilitate the free flow of trade through electronic transactions. While this will pose significant challenges for regulators who are struggling to adapt to a rapidly changing technological environment, it is important for Australia to take this opportunity to fine tune its framework so that it is in a stronger position to gain market access for its exporters.

As significant trading partners,<sup>2</sup> Australia and the US already share close economic links. However the extent to which the elimination of trade barriers facilitates the flow of trade in both goods and services will be affected by the extent to which businesses and consumers are willing and able to make use of electronic mechanisms to facilitate transactions (both business-to-business (B2B) and business-to-consumer (B2C)).

E-commerce is likely to be of special value for Australia's small-to-medium businesses (SMEs) which might otherwise be hampered from engaging in overseas trade due to limited information and high market entry costs. A pilot study undertaken in 1998 by the Department of Foreign Affairs and Trade<sup>3</sup> to examine use of e-commerce by SMEs indicated that micro firms were unable to engage in export

---

<sup>1</sup> See *Creating a Clearway on the New Silk Road*  
<http://www.dfat.gov.au/nsr/clearway/index.html>.

<sup>2</sup> The United States is one of Australia's most significant market for goods and services and is also a major recipient of Australian overseas investment.

<sup>3</sup> This can be accessed at [http://www.dfat.gov.au/nsr/nsr\\_survey.html](http://www.dfat.gov.au/nsr/nsr_survey.html).

trade in the absence of the use of electronic commerce. It also indicated that those firms using electronic commerce to facilitate exports gained higher export earnings as a proportion of total turnover than firms not using electronic commerce. The relatively strong position for Australia in relation to its readiness to adopt information technology and the large proportion of the population online both within Australia and in many potential markets represents a sound foundation for maximising the benefits of the information age.

As well as being important in its own right, a comprehensive bilateral agreement with a significant trading partner has the potential to complement and provide momentum to the wider trade objectives which Australia hopes to achieve in due course through World Trade Organisation (WTO) negotiations. An Australia/US free trade agreement provides an opportunity to agree upon and include useful benchmarks for e-commerce frameworks that can act as standard setters both for other bilateral agreements and forthcoming multilateral negotiations in the WTO itself.

## ***2 Policy context***

While there is increasing worldwide agreement concerning the types of issues which need to be addressed in designing an appropriate legal and regulatory frameworks for e-commerce, there are also some significant differences in the approaches to specific issues which are favoured by different countries. Fortunately there is already a considerable level of consensus between the approaches of Australia and the US in the majority of e-commerce related matters. The signing of a free trade agreement offers a unique opportunity to enhance dialogue with a view to ensuring that both are able to have in place measures which deal effectively with global as opposed to merely local issues.

Law by its nature tends to evolve slowly but the exponential growth in the use of Internet requires rapid and well coordinated responses. This difficulty is magnified by uncertainty concerning the nature and implications of future technological developments.

The characteristic of Internet-based electronic commerce that underlies many of the policy issues to which it currently gives rise is its failure to create the level of trust that is normally found in "face-to-face" transactions. Businesses as well as consumers may be unwilling to make full use of the Internet for commercial transactions unless they are satisfied that they will be provided with similar protections in the online world to those which already exist in the physical world. Of particular concern are matters such as privacy, security, authentication, and consumer protection and, overarching all of these the question as to how legal rights can be effectively enforced in a global environment.<sup>4</sup> It is significant that while Internet usage statistics which show that, while Australian households are increasingly acquiring computers and accessing the Internet, progress has been slower in their transition to purchasing goods or services over the Internet. Likewise, while there is a high proportion of technology use and Internet connection in the business sector, the level of utilisation

---

<sup>4</sup> See the US government's Framework for Global Electronic Commerce at <http://www.ecommerce.gov/framework.htm>.

of the Internet for business transactions with suppliers and customers along the supply chain is lower.

Expanding the digital economy depends on promoting confidence in both B2B and B2C transactions. This means that shoppers must have the assurance that their communications are secure, their personal data is protected, that they will in fact receive the goods or service for which they have paid. It also requires that businesses should have the assurance that their intellectual property rights will be protected and that they can enter in to contracts with same level of certainty and security as occurs in the off line environment.

*(a) Jurisdiction and enforcement of legal rights*

It is a fundamental precondition for public confidence in any regulatory or legal framework that it should contain effective and accessible enforcement and redress mechanisms. In an Internet environment, this means that any rights or penalties must be enforceable on a global basis. This in turn requires harmonisation of legal frameworks to better enable dispute resolution and redress in respect of breaches of the rights of intellectual property owners, consumers and other e-commerce participants.

The use of Alternate Dispute Resolution (ADR) offers one possible solution, allowing consumers and merchants to resolve their disputes through a trusted third party in a low-cost and speedy way.<sup>5</sup> However, ADR is unlikely ever to fully replace litigation in the courts and it is therefore very important for both Australia and the US to work to resolve differences which are currently impeding the adoption of the Hague Convention.

Electronic commerce raises two complex sets of issues that affect the ability of consumers and businesses to protect and enforce their legal rights. The first is the question as to which laws should govern cross-border transactions and whether such transactions should be subject to national laws or dealt with by some international instrument. The second concerns the types of dispute resolution mechanisms which are made available to litigants. The ability to enforce legal rights is essential for consumer confidence e-commerce and also affects the willingness of businesses to use electronic mechanisms for business-to-business transactions.

Where a cross-border dispute is litigated in a court, the court has first to consider whether or not to accept jurisdiction and then, if it decides to do so, which country's laws to apply (choice of law). In Australia the ability to litigate in respect of an

---

<sup>5</sup> There are several overseas examples of ADR, such as BBBOnLine, part of the Council of Better Business Bureaus in the United States, and Cybertribunal in Canada. Other organizations involved in international dispute settlement for electronic commerce are the International Court of Arbitration of the International Chamber of Commerce (ICC), and the Internet-based WIPO-Net set up by the World Intellectual Property Organization (WIPO) to arbitrate intellectual property-related electronic commerce disputes. See also May 21, 2001 Draft of Preliminary Report and Concept Paper of the American Bar Association's Task Force and Advisory Committee at <http://www.law.washington.edu/ABA-eADR/drafts/2001.05.21draft.html>.

international dispute is dependent not only on whether the court has the power to hear and determine a case (jurisdiction) and also a decision about the court in which the matter can most appropriately be tried (forum conveniens). The former depends essentially on valid service of the defendant whereas the latter requires an assessment of factors affecting convenience and expense as well as a consideration of relevant connecting factors.<sup>6</sup> Choice of law will be affected by matters such as the proper law of a contract or where the wrong being litigated took place.

Where a plaintiff is successful in obtaining judgment, this can take place in a different jurisdiction subject to rules which apply there. In the case of Australia, it is possible to enforce some judgments obtained in other countries under the *Foreign Judgments Act* 1991 (Cth) or, on the basis of common law principles of recognition and enforcement.<sup>7</sup>

The issue of jurisdiction has generated considerably more litigation in the US than in Australia although most of this has arisen in the context on inter-state rather than international disputes. Under US law it is a precondition for the exercise of a jurisdiction that a defendant should have at least some "minimum contacts" with the forum state and that the defendant would have reasonably have been able to foresee being sued in that forum. The minimum contacts test requires that the defendant should have 'personally availed' themselves of the benefits of the law of the forum, that the plaintiff's claim should have arisen from the defendant's activities in the forum and that the exercise of jurisdiction over the defendant should be reasonable.

One of the more significant cases which has dealt with Internet jurisdiction issues is the case of *Zippo Manufacturing v Zippo Dot Co*<sup>8</sup>. This concerned an action for trademark dilution which was brought by a Pennsylvanian Corporation against a Californian Corporation that operated a Web site called Zippo Dot Com. It was held that there was sufficient jurisdiction to hear the matter despite the fact that the defendant's only contact with Pennsylvanian residents was through its Web because the likelihood that personal jurisdiction can be constitutionally exercised "is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet." The decision is significant for its development the following "sliding scale" of personal jurisdiction based on Internet usage:

*At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper... At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal*

---

<sup>6</sup> Relevant connecting factors include the law governing the relevant transaction, the places where the parties reside and/or carry on business, the capacity of the forum to afford a complete resolution of the parties' dispute.

<sup>7</sup> A major problem is that consumer protection is not a recognised ground of indirect jurisdiction under the *Foreign Judgments Act* 1991 or at common law.

<sup>8</sup> 952 F. Supp. 1119 (W.D. Penn. 1997).

*jurisdiction... The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site...*<sup>9</sup>

This test is quite clear cut in cases where a business clearly conducts business or has simply posted information on a passive site, the middle ground has proven to be much more complex and therefore, uncertain.<sup>10</sup>

While the rules are still evolving, it is generally true that Australian courts adopt a more conservative approach to the issue of jurisdiction than their US counterparts which may accept jurisdiction on the basis of 'minimum contact' with their jurisdiction.<sup>11</sup> Given the continuing uncertainty concerning the application of these rules there is arguably a need for legislation to clarify their application of these rules in a manner that is as far as possible consistent with the approaches taken by major trading partners.

Of primary importance in this regard is the Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters which is currently being negotiated under the Hague Conference on Private International Law. Countries which sign the convention will agree to follow a set of rules regarding jurisdiction for most civil and commercial cross-border litigation. These require member countries to enforce judgments and injunctive orders, in other member countries (irrespective of whether or not they have any connection to a particular dispute) although there is no obligation to harmonize national laws (including choice of law rules) but only jurisdiction rules. The convention was conceived in 1992 but formal negotiations did not commence until the completion of a preliminary draft treaty in 1996.

The 1996 draft was not designed specifically to deal with e-commerce and concerns have arisen concerning its suitability for addressing Internet (and more generally, information-related) disputes. There have been a number of meetings of the Special Commission and both Australia and the US have been represented at each of these.

---

<sup>9</sup> Id. at 1124.

<sup>10</sup> For a useful discussion of the relevant case law see M Dearing, "Personal Jurisdiction and the Internet: Can the Traditional Principles and Landmark Cases Guide the Legal System into the 21 st Century", 4 *J Tech. L & Policy* 1 [Internet] <http://journal.law.ufl.edu/~techlaw/>; J Kuester and J Graves, "Personal Jurisdiction and the Internet: Where is Cyberspace?", [Internet] <http://www.tkhr.com/articles/personal.html>.

<sup>11</sup> For example, the generous approach to jurisdiction exhibited in the US decision of *United States v. Thomas*, 1996 FED App. 0032P (6th Cir.), 74 F.3d 701, cert. denied, 117 S. Ct. 74 (1996) should be contrasted with the more cautious approach exhibited in *Macquarie Bank Ltd v Berg* [1999] NSWSC 526. See more generally: T D. Leitstein, "Comment: A Solution for Personal Jurisdiction on the Internet" (1999) 59 *La L Rev.* 565; E H. Findley, "Litigation on the Net: Personal Jurisdiction in Cyberspace", (1999) 62 *Tex B J* 334 (1999); R P Rollo, "The Morass of Internet Personal Jurisdiction: It is Time for a Paradigm Shift" (1999) 51 *Fla L Rev* 667 (1999).

With regard to B2C sales, the US government has opposed an article which would protect a consumers' rights to sue in their own country.<sup>12</sup> The US government and e-commerce firms are pushing for the right of the seller to determine jurisdiction in business to consumer transactions. There is also a proposal to have sellers opt out of national laws on consumer protection and privacy if they follow private industry codes of practices and provide various ADR procedures. There is also a lack of consensus on the intellectual property provisions, although there are proposals for exclusive jurisdiction based upon country of registration for patents and trademarks.

The Special Commission of the Hague Conference on Private International Law has taken the approach that specific aspects of the draft need some adjustment but that it is not possible to carve electronic commerce out of the Convention as a separate subject matter to be dealt with by other rules. This approach seems sensible but there is a danger that no consensus about these matters will be reached in the near future.

A significant policy issue that remains to be resolved is the ability of consumers and suppliers to agree to opt out of predetermined jurisdictional rules. A limitation on the ability of a supplier to agree with a foreign consumer that the courts in the supplier's jurisdiction will determine any dispute has the consequence that the supplier may be exposed to litigation in foreign courts. This may act as a deterrent to e-commerce (eg, by resulting in excessive insurance costs) and may impact adversely on Australia both by making e-commerce unattractive for Australian SMEs and by discouraging foreign businesses from engaging in commerce with Australian consumers. The problem with an ability to opt out is that it likely to have an adverse impact on the ability of Australian consumers who will generally lack the bargaining power vis a vis overseas suppliers. On the other hand, an entitlement to sue a foreign supplier in Australian courts may be of little value if the proper law is the contract law of a foreign country which lacks adequate consumer protection laws.

Another issue concerns the potential dangers of being too quick to adopt inflexible rules of jurisdiction which are inappropriate to the resolution of electronic commerce disputes.

*(b) Privacy/data protection*

Apart from jurisdiction the issue which arguably most urgently requires attention is privacy reform. Not only is confidence in privacy an essential precondition for B2C commerce but lack of adequate privacy regulation has the potential to create continuing trade barriers.

Concerns about privacy are fuelled by the ability of businesses to employ data integration technologies such as customer profiling to provide a more fine-grained approach to their marketing efforts. The use of these technologies is leading to increased awareness of potential violations of privacy rights including the misuse of personal data, the collation and use of inaccurate and incomplete information and identity fraud. A recent poll by the Roy Morgan Research Centre found that 56 per cent of Australians are concerned about invasion of privacy issues created by new

---

<sup>12</sup> See CPT's Page on the Hague Conference on Private International Law's Proposed Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters.

information technologies.<sup>13</sup> Even more significantly, a survey by the Boston Consulting Group, found privacy concerns were an issue for about 42 per cent of consumers in their decision not to give registration information to web sites.<sup>14</sup>

Privacy issues may arise in 2 separate contexts:

- the content of information sent to a seller (for example, the content of an email or of information submitted when registering at an Internet site); and
- information relating to the trails left by Internet transactions (for example, details of the parts of an Internet site visited).

One privacy issue that relates directly to the nature of the Internet itself is the manner in which information is transmitted across the Internet. An email message may travel through hundreds of computers in many countries to reach its ultimate destination and, in the absence of effective encryption, there is nothing to prevent the system operators of all of the machines through which it travels, from viewing its content. Arguably this an issue of security rather than privacy per se but, while privacy is much broader than mere security, proper security is an absolute precondition for the effective protection of personal data.

A related concern arising in relation to the Internet and other forms of digital data storage and manipulation, is the increasing amount of information that is being gathered and retained in relation to individuals. All this information can now be cross-referenced and accessed much more readily. The Internet creates the possibility of web sites both within and outside Australia that systematically (and often surreptitiously) gather, process and store personal information about Australians. For example, it is now increasingly common for web sites to gather information via technological devices such as cookies and web bugs. In addition there is a lucrative market in mailing lists.

Because of concerns about these problems (and the fact that they have not elicited similar responses in different countries) privacy protection has also become a significant trade issue. This has been most notably apparent in the context of the European Union (EU) Data Protection Directive<sup>15</sup> which restricts the transfer of personal information from its member countries to other countries that do not have adequate privacy safeguards. The effect of the Directive is that any country that trades personal information with any EU state is required to comply with the strict standards of privacy protection contained in the Directive.

Article 25 of the Directive states that a European country will not be allowed to send personal information to countries that do not maintain adequate standards of privacy. The Directive applies to both governments and corporations, providing citizens with:

- the right to access their personal data;

---

<sup>13</sup> See NOIE, *E-Australia: Australia's Ecommerce Report Card* at [http://www.noie.gov.au/projects/information\\_economy/ecommerce\\_analysis/ReportCard/](http://www.noie.gov.au/projects/information_economy/ecommerce_analysis/ReportCard/).

<sup>14</sup> *Id.*

<sup>15</sup> Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- the right to know where the data originated;
- the right to have inaccurate data rectified;
- the right of recourse in the event of unlawful use of that information;
- the right to withhold permission for the use of their data for direct marketing; and
- remedies for abuse of data include suspension of business contracts, injunctions and compensation.

This Directive caused concerns both in the US and Australia, although the responses of each have been quite different.<sup>16</sup> The US has remained steadfastly opposed to the enactment of a comprehensive legislative regime to protect personal information in the hands of the private sector. It has instead favoured a self-regulatory model for business although it has in place a complex patchwork of laws which deal with specific aspects of privacy such as children's privacy, the privacy of financial and health data and the privacy of video lending records.<sup>17</sup>

More recently, following extensive negotiations with the European Commission, it has put in place a structure which is designed to assist US businesses which need to import personal data from member countries of the EU. In a decision which is binding on all member countries, the European Commission has recognised that there is an adequate level of protection for the transfer of personal data from the EU to the US provided that receiving organisations comply with a set of agreed Safe Harbor Privacy Principles issued on 21 July 2000.<sup>18</sup> Compliance with these principles is purely voluntary but organisations which agree to be bound must publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC)<sup>19</sup> or another statutory body that will ensure compliance with the Principles. While this arrangement has been designed to facilitate trade with EU countries, it will also assist Australian consumers who will be able to check to see whether a business with whom they are dealing is on the Safe Harbor list maintained by the FTC. Businesses which do not take part in the Safe Harbor arrangement will need to enter contractual agreements to satisfy EU adequacy criteria. Such arrangements can also be used to protect the privacy of personal data originating from Australia but are less preferable due to the practical difficulties in enforcing them. Australia, like the US, has long been reluctant to enact a comprehensive private sector law. In 1996 the Government released a Discussion Paper<sup>20</sup> which mooted the

---

<sup>16</sup> For a discussion of the impact of the directive in the US see: D R Tan, "Comment: Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union" (1999) 21 *Loy. Int'l & Comp. L J* 661, 676-84; G Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards" (2000) 25 *Yale J Int'l L.* 1, 10-13.

<sup>17</sup> See, for example, Children's Online Privacy Protection Act of 1998 (accessible at <http://www.ftc.gov/privacy/index.htm>) and the Gramm-Leach-Bliley Act: Protection of Financial Privacy (accessible at <http://www.ftc.gov/privacy/glbact/index.htm>). Its constitution and common law also contain some level of privacy protection, although these in general covers aspects of privacy other than data protection.

<sup>18</sup> The text of the "safe harbor" arrangements is available at [http://europa.eu.int/comm/internal\\_market/](http://europa.eu.int/comm/internal_market/).

<sup>19</sup> The FTC performs a similar role to the ACCC in Australia.

<sup>20</sup> Privacy Protection in the Private Sector' (September 1996).

enactment of a comprehensive private sector law along the lines of the New Zealand *Privacy Act 1993*. However, in early 1997 the government decided not to proceed any further with this proposal and instead directed the Privacy Commissioner to liaise with industry with a view to developing a set of National Principles for the Fair Handling of Personal Information to form the basis of a self regulatory regime.<sup>21</sup>

More recently, in response to concerns arising from the announcement of a comprehensive PBL-Axiom database<sup>22</sup> and about the continuing threat of EU trade sanctions, the Commonwealth Parliament has enacted the *Privacy Amendment (Private Sector) Act 2000*. This extends the *Privacy Act 1990* (Cth), which was previously largely confined to the public sector, so as to create a co-regulatory scheme for the private sector. Businesses may, if they choose to do so, develop their own codes of practice subject to approval by the Privacy Commissioner. However, in absence of an approved code they are subject to a set of national privacy principles which are based on the standards contained in the Privacy Commissioner's *National Principles for the Fair Handling of Personal Information* and to a set of default complaint mechanisms contained in the Act.

The new legislation differs from the scheme outlined in the 1996 Discussion Paper in that it is more "light touch" in its approach. It contains a large number of exceptions (including a "small business" exception that applies to the majority of Australian businesses) and comparatively weak enforcement mechanisms. It is therefore doubtful whether it will achieve its goal of promoting increased consumer confidence in online transactions. It is also unclear whether it will satisfy the criterion for adequacy in the EU Directive. The Data Protection Working Party established by Article 29 of Directive 95/46/EC on 26 January 2001 has welcomed the adoption of the Act, but expressed concern about the adequacy of data transfers to Australia unless appropriate safeguards are introduced.<sup>23</sup>

(c) *Consumer protection*

The other important issue that affects confidence in B2C electronic transactions is consumer protection. Difficulties may arise due to lack of adequate information about suppliers<sup>24</sup>, the ephemeral nature of Internet trading<sup>25</sup>, failure to comply with

---

<sup>21</sup> Prime Minister's Press Release of 21 March 1997 [Internet - <http://www.efa.org.au/Issues/Privacy/pmpr0321.html> (accessed 30 June 1997)]. See also J Brough, "Another Key Election Promise Bites the Dust" *Sydney Morning Herald* 31 March 1997 at 1.

<sup>22</sup> See, eg, R Clarke, "The Packer / PBL / Acxiom InfoBase" at [www.anu.edu.au/people/Roger.Clarke/DV/InfoBase99.html](http://www.anu.edu.au/people/Roger.Clarke/DV/InfoBase99.html); B Nicholson, "Alarm at Packer database scheme" *Age*, Wednesday 1 December 1999 at <http://www.theage.com.au/news/19991201/A8664-1999Nov30.html>

<sup>23</sup> See Opinion 3/2001 on the level of protection of the *Australian Privacy Amendment (Private Sector) Act 2000*.

<sup>24</sup> Online transactions can occur in circumstances where a consumer lacks even the most basic information about a supplier (including even, in some circumstances, their geographical location).

<sup>25</sup> Virtual shopfronts can be set up and dismantled very quickly with a minimum of cost.

advertising and product safety requirements<sup>26</sup> and lack of access to consumer complaints and dispute resolution mechanisms. Australia, like the US, already has in place comprehensive consumer protection laws,<sup>27</sup> covering issues such as fraud and deception, disclosure and cooling off. The difficulty lies in ensuring their enforcement in a cross-border context.

Provision of goods and services across borders over the Internet raises a number of consumer protection issues. The Internet also magnifies the potential for false and misleading activities including deceptive advertising<sup>28</sup> and for infringement of local laws. The latter include not only specific consumer protection legislation but also other law governing matters such product safety.

There is also massive potential for fraud. Examples of Internet-related scams that have been identified by the Australian Competition and Consumer Commission (ACCC) include pyramid selling schemes,<sup>29</sup> misleading claims concerning business opportunities<sup>30</sup> and false prizes and lotteries.

As previously discussed in the context of jurisdiction and dispute resolution, enforcement creates particular difficulties. This is especially the case where commercial transactions involve downloadable goods such as software, music, or information. The difficulty with these is that there are no parties involved in physical shipment of the goods and therefore no ready targets for regulation.

In the case of B2B sales over the Internet the parties may have existing commercial practices in place, using bills of lading, letters of credit, and the other common tools of international transactions. Furthermore when disputes arise many businesses are able to resort to well-established systems of commercial arbitration. However, these tools and facilities have to date been largely the province of large businesses whereas e-commerce has the potential to open up international trade to small-to-medium enterprises (SMEs).

In terms of choice of law, B2B sales are largely governed by the law selected by the parties under the authority of the Rome Convention, the United Nations Convention on the Law Applicable to the International Sale of Goods, and established legal precedents.

---

<sup>26</sup> For example, products purchased online may be designed to meet local conditions and may not work properly or safely in a different context.

<sup>27</sup> The *Trade Practices Act 1974* (Cth) and the US *Uniform Commercial Code*, respectively.

<sup>28</sup> For example, failure to disclose the hidden costs of transactions such as delivery and handling charges.

<sup>29</sup> The promotion of or participation in a pyramid selling scheme is prohibited under the *Trade Practices Act 1974* (Cth), s61.

<sup>30</sup> Misrepresentations concerning business opportunities and employment opportunities are prohibited under the *Trade Practices Act 1974* (Cth), ss 59 and 53B, respectively while deceptive and misleading conduct in general is prohibited under s52.

Consumer contracts differ in that they are subject to mandatory rules in each jurisdiction, making it more difficult for the contract to specify alternative choices of law. Moreover when disputes arise, there is no significant history of international arbitration of a consumer's dispute with a merchant. If disputes go to court, the process may be lengthy and expensive, and there is no certainty that a judgment in Australia will be enforced in the US or vice versa.<sup>31</sup>

Two important recent government initiatives include:

- The release of a Policy Framework for Consumer Protection in Electronic Commerce.<sup>32</sup> These non-enforceable principles are designed to complement the protection under federal and state consumer protection laws and the Corporations law but promoting self-regulation, consumer protection and discussion of international regulatory mechanisms.
- Development of Best Practice Model Code of Conduct to provide guidance to business on the standards and practices that they should adopt in the area of business to consumer electronic commerce.<sup>33</sup> This was developed in response to the Overseas Economic Co-operation and Development (OECD) *Guidelines for Consumer Protection in the Context of Electronic Commerce* which were approved in December 1999.

*(d) Unsolicited commercial email*

One further issue which impacts on e-commerce is the absence of any effective regulation is the growing problem of unsolicited electronic mail. Spam, as it is commonly known<sup>34</sup>, involves the mass dissemination of email messages advertising products and/or services. It provides an inexpensive medium for advertising but can be very costly to recipients, wasting their time and placing burdens on bandwidth. Spam is frequently perceived of as a privacy invasion by individuals and concerns about generating further unwelcome spamming may act as a deterrent from engaging in electronic commerce (as well as having a significant negative impact on business recipients especially where it impacts on bandwidth).

Concerns about the increased proliferation of spam have prompted a flurry of legislative activity in the US<sup>35</sup> but has yet to receive any attention by Australian

---

<sup>31</sup> One device which is receiving increasing favourable consideration is the use of chargebacks including any laws and voluntary industry practices that allow consumers to seek redress for problems arising from online transactions through payment cards.

<sup>32</sup> The policy was released by the Australian Minister for Financial Services and Regulation in October 1999 and it is envisaged that it be adapted by Standards Australia to form an Australian Standard and ultimately even as an International Standard.

<sup>33</sup> See *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business*. This was released by the Consumer Affairs Division of the Australian Department of the Treasury in May 2000.

<sup>34</sup> Named after a canned sandwich filler product, it refers to the practice of bulk e-mailing unsolicited commercial messages.

<sup>35</sup> The regulation of spam has created particular difficulties due to the constitutional protection of free speech. However, anti-spam legislation has been enacted in several of the states and there are currently 5 new bills before the US Congress.

legislators. At this stage the only limitations on the use of spam are confined to clause 10 of the latest version of the Internet Industry Association's voluntary code of Practice and Clause 23 of the government's Best Practice Model Code of Conduct. However, while the sending of unsolicited electronic mail is not illegal in itself, it may incur criminal penalties if it involves illegal use of third party computer systems.

*(e) Intellectual property.*

A major policy issue which impacts on business willingness to engage in B2C electronic transactions over the Internet is the need to ensure adequate protection of intellectual property rights. Commerce on the Internet often involves the use, sale and licensing of intellectual property. If this is to continue and expand, sellers must be provided with the assurance that their intellectual property will not be stolen (and buyers must know that they are obtaining authentic products).

Internet commerce raises a number of potential copyright problems. For example once copyright materials has been place on the Internet its further use and dissemination may be difficult to control. Copying is simultaneously both easy and inexpensive to carry out and both difficult and costly to detect.

While technology, such as encryption, can help combat piracy, an adequate and effective legal framework also is necessary to deter fraud and the theft of intellectual property, and to provide effective legal recourse when these crimes occur. Both Australia and the US are signatories to the *Berne Convention for the Protection of Literary and Artistic Works* which was updated in 1996 to provided new protection for performers and producers of sound recordings. Copyright owners in Australia are able to enforce their rights in the US and vice versa and both countries have in place legislation which provides substantial penalties for piracy.

The issue of copyright infringement and use on the Internet is complicated by the technological factors involved in the operation of the Net and their difficult interface with copyright laws. For example, before a web page can be viewed it has to be temporarily reproduced on the hard drive of the viewer's computer. In addition, many temporary copies are made of the material as it is transmitted around the Net. These temporary copies could be seen to be an infringement of the rights of the copyright owner as a reproduction of copyright material.<sup>36</sup>

Likewise there are potential problems arising from common practice of including within a web site hypertext links to other sites. These links serve a valuable role in enabling web users to 'browse' according to interest rather than in a predetermined linear progression. Linking may be perceived as being in the interests of the site to which links are provided as it tends to attract more visitors and therefore more advertising. However, it may create intellectual property issues where links are provided to pages other than the home page of a site or where the linked material is displayed to the viewer within a frame provided by the originating site.

The provision of links to a page deep within a web site (commonly referred to as "deep linking") may mean that viewers fail to see any advertising and any links to terms and conditions, disclaimers, and privacy statements that appear on the home

---

<sup>36</sup> See: *MAI Systems Corporation v Peak Computer Inc* 991 F.2d 511(1993).

page. A frame is a device that enables a Web page to be divided into separate windows that can each display different content. They typically contain information such as logos and trademarks as well as advertisements. Frames can be set up in such a way that when a user clicks on a link to a page on another web site, the content of that other site appears within a frame surrounded by advertisements, trade marks and menu bars belonging to the originating site. This may create the misleading impression that the material originates from the site which has provided the frames rather than its true source as well as depriving the site from which the material emanated of legitimate advertising revenue.

There are grounds for arguing, at least in cases where framing leads to confusion about source, that framing contravenes consumer protection laws that prohibit deceptive and misleading conduct. It may also contravene laws which have been specifically designed to protect business reputation.<sup>37</sup> However, there is still a considerable amount of uncertainty about the exact legal status of framing and even less concerning possible grounds for redress in respect of the provision of deep links.<sup>38</sup>

Both Australia and the US have made extensive amendments to their copyright regimes to give effect to their obligations under WIPO treaties and to update to better deal with the new digital environment. The key amendments are contained in the US the *Digital Millennium Copyright Act* and the Australian *Copyright Amendment (Digital Agenda) Act 2000*,

The *Digital Millennium Copyright Act* was passed by the U.S. Congress on October 12, 1998. This Act is designed to implement two treaties, the Copyright Treaty and the Treaty Performances and Phonograms treaty, signed in December 1996 at the World Intellectual Property Organization (WIPO) Geneva conference.

The Act makes it a crime to circumvent anti-piracy measures built into commercial software and also prohibits the manufacture, sale, or distribution of code-cracking devices used to illegally copy software although it permits the circumvention of devices for the purposes of conducting encryption research, assessing product interoperability, and testing computer security systems. (There are also some exemptions from anti-circumvention provisions for nonprofit libraries, archives, and educational institutions.).

---

<sup>37</sup> Unfortunately most of the cases which would have shed light on these issues were settled prior to judgment. See; eg, *Shetland Times Ltd. v. Wills*, [1997] F.S.R. 604 (in this case the Scottish court of session was willing to grant an interim injunction to prevent the defendant from maintaining the disputed links but parties reached a settlement before the final hearing); *The Washington Post Company v Total News, Inc* 97 Civ 1190 (PKL) (S.D.N.Y) (this case was settled when the defendants agreed to stop incorporating content from the plaintiffs' sites into any frame located on their site, or to otherwise cause any plaintiffs' web site to appear on a user's computer screen with any material supplied by or associated with them).

<sup>38</sup> See Kaplan C, "Legality of 'Deep Linking' Remains Deeply Complicated", 7 April 2000, *Cyber Law Journal* at [www.nytimes.com/library/tech/reference/indexcyberlaw.html](http://www.nytimes.com/library/tech/reference/indexcyberlaw.html).

In 1999, the Commonwealth Government passed amendments to the *Copyright Act* 1968 which permit local software companies to decompile computer software in certain circumstances (for example to correct errors, to create interoperable software and to test security). This has arguably benefited the growth of e-commerce by promoting increased confidence in the security of information systems and allowing Australian firms to more readily create software that is compatible with worldwide software systems.

More recently the Australian *Copyright Act* has been further amended to extend copyright into the online environment. This initiative was designed to provide greater clarity as to how copyright owners might use the Internet to create new revenue opportunities and to provide them with strong new enforcement measures to protect their material online. The *Copyright Amendment (Digital Agenda) Act 2000*, which took effect on 4 March 2000, made a number of important changes to the Act including the creation of a new technology neutral right of communication to the public.<sup>39</sup> This applies to online transmissions, such as making material available on the Internet and communication "to the public" includes the public in and outside Australia. It also updated and extended to the digital environment exceptions relating to fair dealing and provisions governing the use of materials by bodies such as libraries and educational institutions and created new offences, sanctions and remedies to protect the use of anti-copyright circumvention devices.

New enforcement measures designed to assist copyright owners in enforcing their rights in the digital environment, including new offences, sanctions and remedies in relation to circumvention devices. Finally it also extended the exclusive right of reproduction to include digitisation and increased of penalties for unauthorised digitisation.<sup>40</sup>

One aspect of copyright enforcement which the WIPO has left to be determined by national governments is the liability of online service providers. Both Australia and the US have sought to limit the liability of internet service providers (ISPs) in a number of specified circumstances.<sup>41</sup> In Australia a carrier or ISP will not be directly liable for copyright infringement if the content of the communication has been determined by a third party. However, while an ISP will not incur any liability for simply providing the facilities for communication, it may be liable for authorising a copyright infringement in other circumstances. For example, it may be liable where it has been notified of the existence of infringing material and has failed to take reasonable steps to remove it.<sup>42</sup>

---

<sup>39</sup> This applies to all copyright material except published editions and replaces both the broadcasting and the diffusion rights.

<sup>40</sup> See Attorney-General's Department fact sheet, Copyright Reform: Copyright Amendment (Digital Agenda) Act 2000 at <http://law.gov.au/publications/copyfactsheet/copyfactsheet.html>.

<sup>41</sup> US Digital Millennium Copyright Act;

<sup>42</sup> The factors list of factors required to be taken into account in determining whether there is liability for authorisation include the extent of the power to prevent the infringement, the nature of any relationship between the ISP and the infringer and whether reasonable steps were taken to prevent the infringement.

Another issue for which there is a lack of international consensus concerns the protection of databases. The December 1996 WIPO Conference in Geneva did not take up a proposed treaty to protect the non-original elements of databases. Instead, the Conference called for a meeting, subsequently held, to discuss preliminary steps to study proposals to establish a regime for database protection which is separate from the existing copyright regime.

The use and abuse of trademarks and their interrelationship with Internet domain names also require careful regulation. Domain names simply consist of strings of letters that equate with a unique numeric address. Their key function is make it easier for people to remember addresses but they have increasingly come to be used for the purposes of advertising and promotion in a similar manner to the modern usage of trademarks. This creates difficulties both because there are likely to be many instances where two or more persons may have legitimate claims to the same domain name and also because of the potential for cybersquatting and parasitic practices.

Competing legitimate claims may arise due a range of factors including:

- the fact that trademarks are commonly more than simply words so that it is possible for several persons to have marks which contain the same words;
- the fact that trademarks are registered in respect of different categories of goods and services so that it is possible for different persons to register the same trade marks in respect of different categories; and
- the fact that trademarks are issued on a geographically restricted basis

Cybersquatting occurs when domain names are registered with a view to selling them back to businesses which are likely to want to own them. This may occur where a well known business is slow to apply for a domain name and someone registers the name with the intention of selling it to them when they come to realise that they need a domain name. While this behaviour is both unethical and undesirable it does not strictly amount to use as a trademark, passing off or even deceptive or misleading conduct, thereby making it difficult for businesses whose names are hijacked to seek remedies in the Australian courts.

While the US has enacted specific legislation to deal with this problem,<sup>43</sup> the Internet Corporation for Assigned Names and Numbers has devised a new Uniform Domain Name Dispute Resolution Policy<sup>44</sup> which has proven to be both popular and highly effective. This is essentially a contractually based self-regulatory regime that deals with potential conflicts between domain name usage and trademark laws on a global basis without the need to litigate.

The policy provides that the registered owner of a domain name is required to submit to a mandatory administrative proceeding if a complainant asserts that:

---

<sup>43</sup> For a useful discussion see: J Eisenberg, "A Guide to the Anticybersquatting Consumer Protection Act" *Journal of Internet Law* (March,2000) [http://www.gcwf.com/articles/journal/jil\\_march00\\_1.html](http://www.gcwf.com/articles/journal/jil_march00_1.html).

<sup>44</sup> See ICANN TLD Application Review Procedure (2 October 2000) at <http://www.icann.org/tlds/tld-app-review-procedure-02oct00.htm>.

- 1.the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
- 2.the registered owner of the domain name has no rights or legitimate interests in respect of the domain name; and
- 3.the registered domain name is being used in bad faith.

Use in bad faith includes activities such as cybersquatting and cyber piracy and, if proven, will result in the transfer of a domain name back to the legitimate claimant.

Parasitic behaviour differs from cybersquatting in that it is designed to make use of another's name or trademark to generate trade. It involves using some other business's name or one which is very similar (for example a common misspelling of the name) either in a domain name or in the metatags that are used by search engines to locate web sites. These activities are more easily dealt with under the Australian and US laws which protect registered and unregistered trademarks and also under consumer protection legislation.

#### **(e) Electronic transactions**

Another essential requirement for e-commerce is the existence of a structure which supports the use of contracts in electronic commerce. Internationally, the United Nations Commission on International Trade Law (UNCITRAL) model law establishes rules and norms that validate and recognize contracts formed through electronic means. It also sets default rules for contract formation and governance of electronic contract performance, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence in courts and arbitration proceedings.

The UNCITRAL model law has provided the basis for the *Electronic Transactions Act 1999 (Cth)* and complementary legislation in the States and Territories. This legislation is based on two fundamental principles- 'media neutrality', which requires that paper-based commerce and e-commerce should be treated equally and 'technology neutrality' which seeks to ensure that the law does not discriminate between different forms of technology. It allows electronic communications to satisfy existing legal requirements for writing, signature, document production and the retention of documents, subject to certain minimum requirements.

In the US, every state government has adopted the *Uniform Commercial Code (UCC)*, a codification of substantial portions of commercial law. It was originally envisaged that a new section might be drafted to deal with electronic transactions but it proved impossible to reach a consensus. Instead the *Uniform Computer Information Transactions Act (UCITA)* been developed as a proposed state contract law to regulate transactions in intangible goods such as computer software, online databases and other digital information products. However it has proved to be very controversial and to date it has been passed only by two states, Maryland and Virginia.<sup>45</sup> Its more controversial features include a delayed disclosure approach

---

<sup>45</sup> UCITA is supported by publishers and large software producers but is opposed by libraries, consumer protection groups, and a number of businesses have been

that applies to all terms—including warranty disclaimers, remedy limitations and restrictions on transfer and use and its validation of contract licence terms that take away rights users would have under federal intellectual property law upon purchase of a copy.<sup>46</sup>

Two other important developments include the enactment of the federal *Electronic Signatures in Global and National Commerce Act* (E-Sign) which went into effect in October 2000 and the approval at the 1999 Annual Meeting of the National Conference of Commissioners on Uniform State Laws of the *Uniform Electronic Transactions Act* (UETA). The latter provides a template for uniform state laws validating the use of electronic records and electronic signatures. During the past year, 18 States have enacted the UETA, and it is pending in at least another ten.<sup>47</sup> The two pieces of legislation overlap significantly, often using identical language but they are not identical either in scope or in substance.<sup>48</sup>

#### **(f) Security and Authentication.**

Finally, it is important to bear in mind that even if the legal issues just discussed are appropriately resolved, Internet users will be unlikely to use the Internet on a routine basis for commerce unless they have confidence that their communications and data are safe from unauthorized access or modification,

Confidence in the system itself depends on the availability of effective means both for protecting information systems attached to telecommunications networks and for authenticating and ensuring confidentiality of electronic information to protect data from unauthorized use. It also requires well educated users who understand how to protect their systems and their data.

Unfortunately, as noted in the US Framework document, there is no single "magic" technology or technique that can ensure either security or reliability.<sup>49</sup> Instead this requires the use of a range of technologies including encryption, authentication, password controls and firewalls as well as a trustworthy key and security management infrastructures. Of particular importance is the development of trusted certification services that support the digital signatures and permit users to verify the identity of persons with whom they are communicating on the Internet. Both signatures and confidentiality rely on the use of cryptographic keys.

Encryption products play a critical role in protecting the confidentiality of stored data and electronic communications by making them unreadable without a decryption key. In fact cryptography appears to be the only possible way to achieve security in various

---

among those opposing the enactment of businesses: see

<http://www.ala.org/washoff/ucita/what.html>.

<sup>46</sup> See <http://www.abanet.org/scotis/vol1no5.html#article3>.

<sup>47</sup> See Baker and McKenzie state by state comparison table

<http://www.bmck.com/ecommerce/uetacomp.htm>.

<sup>48</sup> See P Brumfield Fry, "A Preliminary Analysis of Federal and State Electronic Commerce Laws" at <http://www.bmck.com/ecommerce/topic-esignatures.htm>.

<sup>49</sup> See the US government's Framework for Global Electronic Commerce at <http://www.ecommerce.gov/framework.htm>.

forms on an open network like the Internet. However, the US and other governments have sought to limit the use of powerful encryption technologies because of their potential use by criminals and terrorists to reduce law enforcement capabilities to read their communications.<sup>50</sup> While there can be no doubt that the ability to intercept and read communications may assist law enforcement activities, there appears to be a broadening consensus that deliberate attempts to restrict the application of security technology to the Internet has left it insecure and vulnerable to attack by terrorists and criminals. It is therefore arguably important for the Australian government to continue to commit to the free availability of encryption technologies.<sup>51</sup>

Ensuring the authenticity of the parties involved in a business transaction and the integrity and confidentiality of the electronic correspondence that is exchanged can be provided essentially by means of encryption. This makes it possible for each person to have a reliable digital means to identify themselves. Most typically this is done using a trusted third party who verifies the identity by issuing a digital certificate.<sup>52</sup> If e-commerce is to flourish it is important to ensure that digital certificates are internationally compatible.

In enacting the *Electronic Transactions Act 1999* (Cth), Australia has made a deliberate policy choice to adopt a so-called light touch approach which is essentially limited to the recognition of electronic records and signatures. This contrasts with the more comprehensive approach taken in the Utah Digital Signature Act which provides detailed legislative provisions for the establishment of a public key authentication framework.<sup>53</sup>

It has instead established the National Electronic Authentication Council (NEAC) to provide a national focal point on authentication matters including, where appropriate, co-ordination of authentication-related activities at a national and international level. The NEAC is also responsible for overseeing the development by industry bodies and Standards Australia of a framework of technical standards and codes of business practice on authentication matters. It is very important that these developments should be consistent with and/or inform developments in the US.

---

<sup>50</sup> For the history and current state of play in the US see: Center for Democracy and Technology Encryption Page at: <http://www.cdt.org/crypto/>. See also Michael J. O'Neil and James X. Dempsey, *Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry*, 12 *DePaul Business Law Journal* 97 (1999/2000) at: <http://www.cdt.org/publications/lawreview/2000depaul.shtml#1>.

<sup>51</sup> Secure encryption is legal and readily available in Australia and its use will probably increase given the recent availability of PGP version 5 and its new "easy to use" interface.

<sup>52</sup> See M. Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce" (1996) 75 *Oregon Law Review* 49; P Moon, "Everything you always wanted to know about digital signatures" (1999) 37 *Law Society Journal* 57.

<sup>53</sup> These deal with matters such as the operation of certification authorities, issuance, expiration and revocation of a certificates, registration of revocations and suspensions, validity of certificates and obligations of issuers of certificates and of those relying upon a certificate.

### *3 Summary*

Australia, like the US, has already taken important steps to implement a legal and regulatory framework which will support the growth of e-commerce. However there is an urgent need to address the vexed area of jurisdiction and to implement a more effective framework to protect personal information. Moreover as electronic commerce is inherently global and transcends borders it is important to continue to ensure that our approach to these issues is compatible with each other's as well as with a broader global approach.

There is general agreement in both countries (and also more widely) that governments should act to meet the public interest and create a regulatory environment which is flexible, stimulates innovation, competition and business usage, and does not favor any particular technology. However, there is less consensus about some of the specifics. One of the important challenges posed by the proposed Australia-US Free Trade Agreement is to ensure that these issues are resolved as soon as possible.

Key challenges include:

- clarification and harmonisation of laws governing jurisdiction;
- working out how best to strengthen privacy protection with a view to increasing consumer confidence and minimising the potential for trade barriers;
- reducing unnecessary barriers to the use of encryption technologies: and
- coordination of authentication related activities.

If this can be achieved then there will be an invaluable opportunity to embed within an important bilateral agreement a set of clear and fair rules for electronic commerce which can form the basis for future bilateral and multilateral agreements. Our ability to contribute to an international framework which enhances the ability of Australians to benefit from the trade opportunities offered by e-commerce can only be enhanced by achieving a consensus with the US, giving the latter's economic significance and its preeminence in Internet developments.