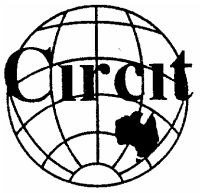


Centre for International Research on Communication and Information Technologies

Issues Analysis

The Law of Internet Commercial Transactions

by Jane Vaughan, Tanya Sewards & Ross Kelso

The Centre for International Research on Communication and Information Technologies is a research centre at the Royal Melbourne Institute of Technology.

CIRCIT was set up in 1989 to provide independent research and education on information and communication services. The aim is to create new knowledge that is relevant to the community, industry and government so as to increase the social and economic wellbeing of people in Australia and other parts of the world.

The CIRCIT research program is structured around three main themes:

1. **Use and Users of Information and Communication Services**

   The research focuses on the use of information and communication services by residential users, small businesses, corporations and government. It covers the broad area of communication in activities such as payments and finance, work, health, education, entertainment and government services.

2. **Policy and Regulation of Information and Communication Services**

   Policy and Regulation of Information and Communication Service*s* focuses on national strategies and objectives, competition, and issues of access and equity.

3. **Information and Communications Industries**

   Information and Communications Industries research deals with developments in information technologies and services, industry policy and infrastructure issues.

The CIRCIT Research Program is currently funded by:

AsiaSpace, Australian Communications Authority (ACA), Australian Information Industries Association (AIIA), Australian National Training Authority (ANTA), Australian Telecommunications Users Group (ATUG), Cable & Wireless Optus, Department of Industry, Science and Resources (DISR), Department of Communications, Information Technology and the Arts (DCITA), Education.Au, Ericsson Australia, Fujitsu, Health Issues Centre, Melbourne IT, Multimedia Victoria, National Office for the Information Economy (NOIE), Nortel Australia, Nortel Corporate, NSW Government, Office for Government Online (OGO), Service Providers Action Network, Telstra, Victorian Office of Training and Further Education (OTFE), Vodafone, WA Government.

Enquiries regarding details of the research agenda and sponsorship opportunities should be directed to:

Director, CIRCIT at RMIT,
GPO Box 2476V
Melbourne 3001, Australia
Tel: +61-3 9925 2829;
Fax: +61-3 9925 3122
Email: circit@rmit.edu.au

Disclaimer

This report is for general academic reference purposes only and should not be relied upon as a basis for legal advice. Neither CIRCIT Ltd nor its employees, agents, consultants or associates take any responsibility whatsoever for any detriment, loss or damage, financial or otherwise, arising as a consequence of reliance upon the contents of this document as a basis for legal advice.

Acknowledgments

This report, together with the associated Literature Review, was prepared under contract to Australian Multimedia Enterprise Limited.[1]

The study was project managed by Ross Kelso who also contributed the section titled *The Commercial Paradigm*. Tanya Sewards provided valuable assistance in contributing the section titled *Security and Privacy*. The remaining work, which constituted the bulk of the research and writing, was performed by Jane Vaughan, a qualified solicitor.

CIRCIT Ltd would like to thank partners of the Canberra office of solicitors Dunhill Madden Butler, and particularly Ian Cunliffe, for their critical evaluation. However, any errors or omissions which remain are solely the responsibility of CIRCIT Ltd.

[1] Australian Multimedia Enterprise Limited (AME) is an investor and financier established by the Australian Federal Government in 1995 to invest in commercially viable interactive multimedia products and services, which have a content element or which facilitate access to particular content, including online services such as the Internet. In this capacity, AME provides concept advances, project investment and secured loans.

Table of Contents

Preface

Over the past few years, the Centre for International Research on Communication and Information Technologies (CIRCIT) has undertaken studies into Australia's development of information and communication technologies, services, industry structures and associated policies. An important element has been recognition and examination of the international context of these developments.

The advent of the Internet as a world-wide delivery platform for information and communication services presents a challenging opportunity to revisit current paradigms, particularly regarding the manner in which information is accessed, services are delivered and business is transacted. Conversely, commercial exploitation of the Internet could be perceived as a threat to more conventional service delivery organisations and businesses, and to the payment mechanisms employed.

Existing laws, regulations and codes of practice serve these conventional processes reasonably well. To a fair degree, intervention of the Internet into these processes could merely call for direct analogies to be drawn between 'paper-based' and 'paper-less' transactions. Electronically delivered transactions are not new. Plastic credit cards with magnetic strips, ATMs, EFTPOS and EDI have long been accepted into business and society at large. Laws, regulations and codes of practice have adapted correspondingly, although perhaps lagging these technological changes. There are, however, some core areas of variation from current practices.

The Internet constitutes a relatively 'open' system that is directly accessible by ordinary consumers as well as businesses. New intermediaries arise creating sites on the World Wide Web that may mirror commercial offerings of others, act as agents on commission or directly tender their services. The requested services may be delivered to a consumer either electronically or by conventional means. Although conventional credit cards and cheques have been initially exploited, the greatest advantages accrue only with Internet-specific payment systems or mechanisms.

Australia's small population inevitably leads a local Web site entrepreneur to seek overseas consumers. Hence, jurisdictional issues could become of paramount concern, in addition to questions of security of communications made over the Internet.

When Australian Multimedia Enterprise Limited (AME) approached CIRCIT to undertake a study of the law relating to commercial transactions over the Internet, they expressed a particular need to appreciate the likely exposure of Web site entrepreneurs, and investors, to risks of a liability nature for sale of goods and to risks associated with ensuring international payments are realised.

Accordingly, this study focuses primarily on the legal context of commercial transactions conducted over the Internet between Australian-based Web site entrepreneurs and their customers, who are both local and overseas consumers.

The report analyses jurisdictional issues, evidentiary and contractual issues, payment systems, relevant business models, sale of goods and consumer protection, as well as security and privacy issues. Matters such as defamation, copyright, intellectual property and specific regulatory restrictions associated with merchandising items such as alcohol, shares, gambling and adult services are not dealt with. Likewise, the expected concerns of government by way of the scope for money laundering, tax and duty evasion, etc. are beyond the scope of this study.

A detailed *Literature Review* provides a valuable starting point for further studies and adopts a scope wider than that discussed above. The *Review* is separately published.

Jane Vaughan, a qualified solicitor, undertook most of the work on the *Issues Analysis* and was ably assisted by Tanya Sewards. The overall project was managed by Ross Kelso who also directly contributed. Of particular value has been the critical evaluation provided by the firm of solicitors, Dunhill Madden Butler.

The report of the *Issues Analysis* concludes with a number of areas where reform should be considered that would make Australia more competitive in the rapidly evolving Internet market place by eliminating uncertainty and closely tracking overseas developments in technology adoption, recognition of payment mechanisms, broad legislative treatment and industry codes of practice. The problems confronting Australian Web site entrepreneurs will be challenging enough without the added burden of a lagging or unresponsive legal and regulatory regime.

John Burke
Director, CIRCIT
March 1997

Executive Summary

The Internet is a worldwide web of computers, a 'network of networks'. Although originally devised for defence and academic purposes, the Internet is now accessible by ordinary computer users and its commercial potential is being exploited. In particular, it has been recognised that products may be marketed, and that information products may be distributed directly via the Internet, at a fraction of the usual cost. Various payment mechanisms are being developed to suit the requirements of the medium and to assist in realising its full commercial potential.

In a recent study by International Data Corporation, the amount of Internet commerce being conducted world-wide was estimated to be around $3 billion in 1996, growing to $100 billion in the year 2000. Of the $3 billion figure, more than one-third of online sales are thought to be now completed on the Web, as opposed to telephone or facsimile, and the study reported that by the year 2000, the proportion should be much greater than two-thirds. To a large extent, the projected increase in electronic commerce conducted over the Internet is attributed to a ten-fold increase in Web users to about 163 million by the year 2000. Of particular note, although the world-wide percentage of Internet users who buy goods and services on the Web is forecast to reach 28 percent by December 2000, in the United States of America the percentage should grow to 45 percent.[2]

Clearly, the scope for business opportunities for Australian Web site operators will be enormous, but only if overseas users visit their Web sites. Although currently most Internet sales are being generated through the delivery of easily identified items such as software services and products like audio CDs, videos and books, in the near future sales are expected to increase sharply with the advent of online catalogues which allow consumers to search for items and compare the contents.[3]

From a legal perspective, commercial transactions which take place over the Internet share many characteristics with other more traditional types of commercial transactions. However, Internet transactions also have distinguishing characteristics that may be critical in law. The focus of this study is principally on what is different about Internet commercial transactions, rather than on the characteristics shared.

The following represents a summary of major legal issues raised by commercial transactions taking place via the Internet, with particular consideration given to the international context.

i) Jurisdictional Issues

Jurisdiction

Normally, a state[4] may not exercise its own powers within the territory of another state, or in any other area beyond its own territory, without consent. There is a general presumption that the legislation and laws of a state are not intended to have extra-territorial effect and court jurisdiction is similarly limited. In cases where legislation includes provisions which give it express extra-territorial effect, there still needs to be some link or nexus between the activities and the State for the legislation to be invoked. Where an Australian court hears a case arising under legislation of that kind it will have jurisdiction to make determinations and to order remedies in respect of circumstances occurring outside Australia. However, in the absence of mutual enforcement treaties, its orders will only be enforceable within the territorial jurisdiction of the court.

The extra-territorial application of laws of an individual state assumes a special poignancy when those laws purport to extend to activities taking place on the Internet. The problem can be illustrated by the example of an Australian Internet Service Provider (ISP), merchant or user who places an advertisement on a Web site in Australia which can be accessed throughout the world. The simple act of placing information on the Internet may make the party subject to the laws of every jurisdiction in which that information can be accessed Some

---

2 IDC, 1996, *The Global Market Forecast for Internet Commerce*, Report No. W12339, November http://www.idcresearch.com/HNR/cpr4ic.htm

3 Wright, C, 1997, 'Booming Online Sales Growth Swept up in Internet', *Australian Financial Review*, 29 January, p 3.

4 In this context state means nation or law area.

states have issued policy statements which express an intention to extend the application of their civil and criminal laws to activities taking place on the Internet, regardless of the location where the activities are initiated. However, where enforcement of these laws is attempted against persons or bodies within another state's jurisdiction, the consent of that other state will generally be required.

International Treaties, Conventions and Model Laws

Because of the jurisdictional limitations of states, an effective means of regulating Internet commerce at an international level is through the adoption and implementation of international treaties or conventions. Assistance can also be provided by model laws, protocols and technical standards. One apparent shortfall in this area, which has arisen as a consequence of the dis-intermediation effect of the Internet, is the lack of international principles governing consumer transactions. Some existing treaties governing various aspects of international trade will apply to Internet commerce, provided they involve business or trade transactions. One international convention of particular significance in international trade is the United Nations Convention on Contracts for the International Sale of Goods. However, the Convention does not apply to consumer sales and hence will be inapplicable to the larger part of Internet transactions. In addition, the Model Law developed by United Nations Commission on International Trade Law (UNCITRAL) which applies to business transactions and which has yet to be implemented in Australia, has been developed to facilitate electronic commerce internationally. Amongst the many prospective international fora which could have potential impact in the field of electronic commerce is the World Trade Organisation (WTO). An area in which the WTO may provide a good forum for international initiatives is that of global Internet commerce, particularly in relation to consumer transactions.

Private International Law

Jurisdiction principles have led to the evolution of rules to deal with private transactions taking place across international borders. Disputes which arise from such transactions will bring into play the part of the national law of a country that establishes rules for dealing with cases involving a foreign element, known as private international law.

In an international context, the private international legal systems of many countries are underdeveloped. They are inadequately evolved to provide proper dispute resolution procedures, as well as in substantive terms, to properly support the rights and remedies of parties engaged in activities which take place across international borders. Quite apart from these shortcomings, the laws have historically evolved slowly to accommodate paper based transactions, and physical distribution channels and contacts. Accordingly, there is no concept in the law which can identify what constitutes an adequate link between digital or electronic activities or entities and a particular jurisdiction.[5]

Due to concerns about the effectiveness of the legal remedies available when commercial transactions cross international borders, the Australian Law Reform Commission (ALRC) recently undertook a major study of the associated legal risk.[6] The ALRC also examined electronic commerce which it referred to as an emerging priority for cross-border legal initiatives. It recommended that the Attorney General's Department work in electronic commerce, which amongst other things, involves the establishment of an expert group to examine legal issues in the area, should be given a high priority.[7] However, to date, neither terms of reference nor members of the expert group have been settled.

Conflicts of laws issues arising in Internet commerce are likely to be far more complex than those which occur in the context of physical or paper trading. This is because it will become increasingly commonplace for the manufacturer, customer, seller, and principal bank to be situated in different jurisdictions.

---

5 Rose, A, 1997, *Electronic Commerce and the Law Free Zone*, ASC Conference on Electronic Commerce, Sydney, 4-5 February.

6 Australian Law Reform Commission Legal Risk in International Transactions, ALRC 80 (1996) Commonwealth of Australia.

7 ALRC 80 Ch 5.

Even if Australian courts have jurisdiction to hear a case, the judgments of Australian courts cannot be unilaterally enforced outside Australia, a situation which would breach the sovereignty of other countries. In the context of Internet commerce taking place internationally, there are three matters to be considered. The first is that judgments of Australian Courts will only be enforceable within a few nominated foreign jurisdictions under the special legislation which provides for mutual recognition of foreign judgments, or under common law which requires the defendant to submit to the jurisdiction. The second relates to quantum of money judgments. The legislation only applies to higher courts. Judgments for sums of tens to hundreds of dollars will not be enforceable under the legislation and there is no appropriate mechanism to deal internationally with disputes of this nature. Finally, difficulties exist in the obtaining of foreign evidence, particularly documentary and electronic evidence.

ii) Contractual Issues

Electronic Contracts

The terms of an Internet contract are likely to be established under general law of contract and the principles of private international law, in largely the same manner in which terms of a contract are established in the physical world. However, some assistance in this area could be provided by a legislatively recognised 'electronic contract' which would include rules about, amongst other things, the time and place of offer and acceptance, what constitutes a valid electronic offer or acceptance, and presumptions about which law will apply to the contract.

Generally speaking, the terms of an electronic contract can be established by writing, orally, or implied from the conduct of parties. Other terms may be incorporated into contracts by legislation. However, some electronic contracts may not be enforceable by reason of legislation requiring certain contracts to be in writing or evidenced by a written note or memorandum, but this will not affect the existence of the contract. It merely means that the contract will not be enforceable by a court.

Applicable Law

In some cases coming before courts in Australia and overseas, the court has to establish which state's laws govern the terms of a contract. The proper law of a contract is the system of domestic law which defines the obligations assumed by the parties to the contract. The situation is clearest where the parties have chosen which law will apply. The parties may expressly choose the body of law to apply to all or part of their contract, but in the absence of any express choice or necessary implication from the contract an Australian court will look for the system of law with which the transaction has its closest and most real connection.

Identifying the applicable law will be important to establish the rights, obligations, enforceability and available remedies for the parties to the contract. It will establish, for example, whether provisions of legislation which purport to incorporate terms into certain types of contracts, such as the Sale of Goods legislation enacted within all Australian jurisdictions, will be applicable.

Formal Requirements

Although there is no general formal requirement of writing in the law of contract, some legislation makes it necessary for certain contracts to be evidenced by a written note or memorandum if they are to be enforceable by a Court. The statutes prescribing requirements that contracts satisfy formal requirements of writing fall into two categories: legislation derived from the *Statute of Frauds 1677* (UK) and consumer protection legislation. Thus there is still legislative insistence on paper transactions even though technology is moving to paperless transactions, such as contracts brought about by electronic data interchange (EDI).

Evidence Acts

Certain types of electronic documents can be introduced into evidence in court under the Evidence Acts in Australian Federal, State and Territory jurisdictions. The Evidence Act 1995 (Cth) has been heralded as a model law for computer evidence. Although it does not create formal recognition of electronic contracts, the Act may facilitate electronic commerce in the following three areas:

- It allows proof of the content of electronic records by a print-out of those records;[8]
- The exceptions to the hearsay rule have been widened, particularly in relation to business records. Section 71 makes telecommunications such as electronic mail exempt from the hearsay rule so far as they constitute evidence of the identity of the sender, the addressee, and the date and time the message was sent.[9] Internet contracts made by e-mail may fall within these provisions.
- It applies a statutory presumption as to the correct operation of devices and machines, in the context of proof of machine-produced evidence. This could be used in relation to authentication devices for electronic signatures and potentially to prove contracts which are initiated by computer.[10]

Signatures

Many documents still need to be signed to be valid. The new digital signatures, which are described further below, appear to satisfy the legal criteria for valid signatures under the general law,[11] even without legislative recognition.[12] However, it is more likely that the legislature in Australia will establish a specific regime governing digital signatures but as yet there has been no facilitating legislation making this possible.

Trading Partner Agreements and Other Solutions

In business transactions where the parties have an established or ongoing relationship, trading partner agreements have been used, which amongst other things can deal with:

- the law which will apply to the contract, as well as the jurisdiction where disputes can be heard;
- the requirements for paper records of transactions;
- requirements for signatures;
- record retention;
- allocation of responsibility for network security and other failures;
- applicable standards and protocols.

However, these types of agreements may not be capable of accommodating the Internet trading environment of the future which may not necessarily encompass established links between parties. In addition, these types of agreements may not be appropriate for consumer transactions.

For consumer transactions to be properly facilitated in Internet commerce, a concept of the 'electronic contract' is required.[13] Some progress towards this end has been made by the UNCITRAL Model Law described already, although this Model Law is so far inapplicable to consumer transactions. Terms may also be incorporated in Internet transactions by the appearance of terms and conditions at the time of contracting, ie. when the consumer enters his/her details onto an Internet order form. Arguably the same terms as those traditionally

---

8 This is an exception to the best evidence rule.

9 See for example, Willis, A, below.

10 Willis, A, 1996, *Legal Issues in Electronic Commerce*, IPAA/IIR Conference Rydges, Lakeside 30 May.

11 Except those types of contracts which require witnesses to be enforceable, but these could also be authenticated digitally.

12 Willis, A, 1996, p. 9.

13 Willis, A, 1996.

contained within trading partner agreements could be incorporated this way and providing they are sufficiently brought to the notice of the consumer, they should be enforceable by analogy to the ticket cases in contract law.

iii) Payments Systems

A number of payment mechanisms are being developed or adapted from existing payment mechanisms to cater for Internet commerce, including credit cards, Stored Value Cards (SVCs), digital cheques and digital cash. Satisfactory payment systems are integral to the operation of Internet commerce, and amongst other things, must be cheap to cater for smaller transactions, must be secure, and should provide a degree of privacy.

New payment systems designed for the Internet raise issues specific to themselves. These include how to classify them conceptually as legal instruments, and how they interact with the laws applicable to established payment mechanisms such as cheques, credit cards and money. Questions arise about allocation of liability between users and providers of new payment mechanisms for security system failure, including unauthorised use or fraud. Other unresolved issues which arise include how the various laws and codes, particularly those with consumer protection charters which govern payment systems in Australia and other countries, will apply to payment systems which exist in an international setting.

The SET Protocol

Although most payments on the Internet are presently being made simply by consumers providing credit card numbers to merchants, such a payment mechanism is clearly recognised as being inadequate for realising the full commercial potential of the Internet because:

- credit card transactions are too expensive to accommodate small denomination amounts down to as little as a cent;
- credit cards are considered as being too insecure, due to the present lack accepted authentication procedures worldwide across the Internet.

As a response to these concerns, card issuers VISA and Mastercard have developed the Secured Electronic Transaction Protocol (SET) which is designed to make credit card transactions over open systems like the Internet secure. At the time of writing, liability issues under the system have not been addressed. Given the estimated potential profits for card issuers and banks to flow from Internet commerce, and on the basis of the current allocation of liability in credit card regimes for non-Internet purchases, it seems likely that card issuers and banks will need to absorb a large portion of the risk in order to make the credit card system viable for Internet commerce. This will translate into an acceptance of a responsibility for the proper operation of secure systems and/or compliance with protocols which are developed to govern it. This responsibility can be shifted to insurers and other parties by contract.

Significant jurisdictional issues should not arise in relation to Internet credit card transactions because the relationships between the parties are based on three separate contracts. It is generally likely that the issuing bank or card issuer will be carrying on business in the place of residence of both the cardholder and the merchant, whether or not the latter two parties are in the same jurisdiction. The merchant needs only to seek payment from the bank or card issuer, which is guaranteed by the latter subject to certain conditions. Banks and card issuers act as intermediaries who absorb a large part of the risks associated with jurisdictional uncertainties.

Internet payment mechanisms including smart cards, digital coins, cheques and signatures are likely in the future to be governed by a variation of the EFT Code of Conduct which amongst other things, sets out rules for allocation of liability between parties. They may also be subject to legislation supported by international treaties. In addition, standards and protocols are being developed, which not only deal with security aspects of new payment systems but also have a bearing on liability issues in some circumstances.

iv) Consumer Protection

Sale of goods, consumer protection, consumer credit and advertising laws in Australia are governed by a variety of Federal, State and Territory laws and industry codes aimed at protecting the consumer from unfair practices by merchants and advertisers, and to provide rights in respect of goods, services and credit provided to consumers. Internet commerce raises issues about the application of these laws to the medium and to the various parties operating in the medium. It also raises issues about the reach of these laws to parties outside Australia, as well as the reach of counterpart overseas laws to parties situated in Australia.

Advertising

Advertising in Australia is governed by a number of Federal, State and Territory Acts and industry Codes which regulate the way goods and services are depicted and which proscribe misleading and deceptive conduct by corporations and others. The Trade Practices Act 1974 (Cth) (TPA) applies to corporations and traders involved in international or interstate business activities, and also covers all television advertising. At a State level, the various Fair Trading Acts contain mirror provisions to those contained in the Trade Practices Act, operate alongside the Federal Act, and apply to persons generally.

The TPA contains a number of defences to breaches of Part V of the Act which contains provisions dealing with consumer protection. Section 85(1) provides defences to prosecutions for criminal offences under Part V the Act.

Under s 85(1)(a) and (b) an advertiser will not be convicted of an offence if it can show that the contravention was the result of a reasonable mistake, or a reasonable reliance on information supplied by another person.

It is a defence under section 85(1)(c) to show that, despite exercising reasonable precautions and due diligence, a contravention arose because of the act or default of another person, an accident or some other cause beyond the control of the advertiser.

Section 85(3) provides a special defence for broadcasters and publishers to actions for breaching Part V. The defence is available only to people ‘whose business it is to publish or arrange for the publication of advertisements’. It applies if the advertisement has been received for publication in the ordinary course of business, and the publisher does not know or suspect that the publication would amount to a contravention of

the Act. Although the defence is available to broadcasters, it is probably not available to advertising agencies, or by analogy to Internet content creators.

Most of these defences should, depending on the circumstances, be available to Internet service providers. However, if the ISP assists in the design of the Web site which includes infringing material, the defences may not be open to them.

There is currently no specific legislation or industry codes applicable to Internet advertising in Australia, although the draft Distance Selling Code of Practice released in January this year by the Ministerial Council on Consumer Affairs is a step in the right direction. The existing voluntary industry codes will govern bodies only if they presently fall within the jurisdiction of the Media Council, which is largely limited to the proprietors of commercial media. Advertising self-regulation also relies on the submission by accredited advertising agencies of material for vetting by a representative body from each arm of the media. The same quality control cannot be enforced for Internet advertising unless a similar representative body can be brought into existence. Neither it seems will the voluntary industry Codes apply to extra-jurisdictional advertisers, unless they fall within the jurisdiction of the Media Council. This would probably require their voluntary submission.

However, Australian companies, Internet advertisers, content service providers and content creators, will always be subject to the Australian State and Federal legislation which applies to advertising, including the Trade Practices Act 1974 (Cth). As previously stated, whether any or all of these parties can avail themselves of defences within the legislation is another matter.

Australian laws may not be able to control what material is accessed from outside its borders. The extent of the application of Australian laws to overseas Internet advertisers and other parties, is yet to be determined, but even if it can be shown that the legislation has extra-territorial application, problems relating to enforcement of the legislation against overseas parties remain.

There are also further issues in relation to enforcement. For example, in the physical world, enforcement is possible because the identity of the maker of an advertisement or representation may be readily established. This is not the case with the Internet, where the identity of the party may not be known or traceable. The ease of creation and removal of Web sites also creates problems of proof.

The use of 'hyperlinks' creates a further subset of problems relating to liability under advertising laws. Controllers of hyperlinks on Web sites may be exposed to liability under advertising laws if they cannot bring themselves within the purview of defences outlined above. This is best illustrated by an example of a shopping mall Web site of a major retailer which contains hyperlinks to sub-boutiques of various brand names. If the Web sites of sub-boutiques contain material which breaches advertising laws in Australia, can the major retailer or the retailer's ISP also be liable? What if the sub-boutique Web site has been hyperlinked from another jurisdiction where the material is not in breach of the laws, but breaches Australian law, or vice versa? In this situation, there will be a number of parties, including ISPs who are exposed to potential liability. Although it is arguable that many of these parties are too far away from the locus of the infringing activity in terms of knowledge of the material facts or control over responsibility for the activity, the general law has not come close to solving any of these issues, even without regulatory intervention.

Sale of Goods and Consumer Protection

There is a three-tier system governing contracts for the supply of goods and services in Australia. These are:

- Uniform sale of goods legislation (SGA), of which the provisions may be contracted out. The sale of goods legislation will largely govern transactions which take place within the jurisdiction of each State. Some sale of goods legislation purports to have extra-territorial effect by linking at least part of the transaction to the State. This provision gives the legislation potential application to overseas merchants subject to enforcement problems outlined above.

- Consumer protection provisions of the TPA, applicable to transactions involving the supply of goods or services by a corporation to a consumer, which cannot be contracted out and which take precedence over State legislation. The Federal consumer protection provisions are contained in Part V of the Trade Practices Act 1974 (Cth) (TPA). These provisions deal with misleading statements and unfair practices by a corporation in connection with the supply of goods or services; product safety and product information; implication of certain terms in a contract for the supply of goods or services by a corporation to a consumer; the liability of manufacturers where no direct relationship applies between the supplier

corporation and the consumer ('product liability'), and strict liability on the part of a corporate manufacturer who supplies defective goods. Section 5(1) of the Trade Practices Act 1974 (Cth) confers limited extra-territorial operation by applying the Act to conduct outside Australia. Territorial nexus is provided by the requirement that the party engaging in the conduct must be an Australian citizen, a person ordinarily resident in Australia, an Australian incorporated entity or a body corporate carrying on business in Australia. Although the TPA applies primarily to corporations, it has some applications to the conduct of individuals. In particular, a number of sections of the TPA apply to conduct by non-corporates in trade or commerce between Australia and places outside Australia[14] and to conduct involving the use of 'postal, telegraphic, telephonic and like services'.[15] The latter provision relies on the words of placitum (v) of the Commonwealth Constitution which have formed the basis of federal regulation of broadcasting and telecommunications in Australia. Accordingly it may be strongly arguable that Internet commercial transactions which involve an Australian end are within the scope of the TPA.

- State legislation applicable to consumer transactions which do not fall within the ambit of the TPA. The State legislation either amends the SGA in respect of transactions within its ambit or implies conditions as to title and quality which differ from those contained in the SGA and which are similar to but not always identical to the corresponding provisions of the TPA. These provisions cannot normally be contracted out. In contrast to the TPA, the provisions of State legislation are not limited to corporations. They apply to 'persons' generally. Most of the State legislation purports to have extra-territorial application. Extra-territorial application of state laws is subject to the same enforcement considerations as outlined above. There is also State legislation which governs particular types of transactions, such as credit transactions, commercial sale of second-hand motor vehicles, door-to-door sales, lay-by sales, residential tenancy agreements and others.

At a local level, problems of enforcement of consumer protection laws in respect of distance selling and Internet transactions appear to be being dealt with, at least initially, by proposals for industry Codes of Conduct. However, these are not likely to apply to international transactions where the seller is not based in Australia or party to the Code.

On 17 January 1997 the Ministerial Council on Consumer Affairs (MCCA) released a draft Distance Selling Code of Practice and discussion paper for public comment.[16] The draft Code is designed to establish minimum standards of behaviour for distance sellers. 'Distance selling', where consumers buy goods and services without visiting a trading premises or meeting the seller, includes mail order, telemarketing, 'infomercials' and television as well as Internet advertisements.

Consumer Credit

A uniform scheme of consumer credit laws[17] for the regulation of consumer credit has been enacted in all Australian States and Territories.[18] The Code applies to all credit provided for a personal, domestic or household purpose, regardless of the amount to be provided. The legislation sets out the requirements for credit contracts, including pre-contractual disclosures, the fact that credit contracts must be in writing and that they must contain certain key material designed to ensure that 'truth in lending' is given effect to. The Code applies[19] to the provision of credit (and to the credit contract and related matters) if, when the credit contract is entered into, the debtor is a natural person ordinarily resident in the jurisdiction or a strata corporation formed in the jurisdiction. The Code also has a continuing or extended jurisdiction in certain situations. These are (a) that if the Code applies to the provision of credit or the contract it will apply in relation to all transactions or acts

---

[14] see TPA s6 (2)(c) and (h).

[15] see TPA s6(3)(a).

[16] See the Draft at the ACCC Web site: http://www.acc.gov.au/new/goodprac.html

[17] The template legislation, the Consumer Credit (Queensland) Act, 1994, received Royal Assent on 14 September 1994, but was not proclaimed to commence until 1 November 1996. The Consumer Credit Code is contained in the Appendix to that Act.

[18] In the United States, consumer credit is governed by the Consumer Credit Protection Act of 1968. This legislation is similar to the Australian legislation in that it is based on certain required disclosures.

[19] Section 6 sets out the general jurisdiction of the Code.

under the contract whether or not they take place in this jurisdiction; and (b) the Code will continue to apply even though the debtor ceases to be ordinarily resident in the jurisdiction. There are also provisions dealing with the situation where there are more than one debtor in different jurisdictions.

It is foreseeable that some credit arrangements may be entered into in the context of Internet transactions by consumers who may fall within the purview of the Code, if the debtor is or has been ordinarily resident in an Australian State. The Code seems implicitly to be based on the view that established entities in the business of providing credit to consumers in Australia are in the main also incorporated or carrying on business in Australia. One concern may be that entities which conduct business on the Internet, either based from Australia or overseas, may offer credit in a manner which could bring its activities within the terms of the Code.[20] Conversely, Australian credit providers may need to comply with similar laws which have been enacted in other jurisdictions, such as the United States. The extra-territorial application of the Code remains to be established.

v) Security

The main impediment to development of online commerce has been the absence of a secure system for conducting commercial transactions. Without secure payment tools, both customers and merchants are reluctant to trade using the Internet.

To some extent the race to provide these features and develop the means of secure electronic exchange is a race of technology - developing encryption techniques. Most of the payment schemes operating are using some form of cryptography to ensure both the security and privacy of commercial transactions.

While many security concerns will be addressed by these emerging technologies, standards and protocols, legislative measures may also be necessary. The most outstanding issues to be addressed include:

- *The Extent To Which These Encryption Technologies Can Be Used*. Australia is dealing with the issue of encryption through the use of standards. Although it has been asserted that the government has adequate power to regulate the Internet under the communications power of Section 51 of the Constitution,[21] the government claims that there is no blanket constitutional power and that there would be problems in reaching agreement with State and Territory governments on such legislation. It is presently being left up to groups such as Standards Australia to specify the standards for encryption.[22]

- *The Use Of Digital Signatures*. Digital signatures are used to provide user authentication, integrity and non-repudiation security services.[23] Electronic signatures are created through the use of encryption. A digital signature takes a different form to a handwritten signature on a paper document so that it not only provides evidence which identifies the sender, but can also ensure that the contents of an electronic message have not been altered.[24] Changes to the law will be necessary if electronic signatures are to have the same legal validity as written signatures, allowing the signing of contracts online.

- *The Introduction And Regulation Of Certificate Authorities*. To assure proper linkage of a digital signature with the owner of a distinguished name third parties are being established. These third parties are referred to as Certification Authorities (CA). A CA is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact

---

[20] These entities may also require an Australian banking licence.

[21] Part V - Powers of the Parliament in Section 51 of the Constitution states that the Parliament shall have the power to make laws for the peace, order, and good government of the Commonwealth with regard to postal, telegraphic, telephonic, and other like services. It is argued that the Internet could be classified under this definition.

[22] Orlowski, S. 1996. *Security of Government Information Infrastructure*, http://www.anu.edu.au/people/Roger.Clarke/II/Orlowski.html

[23] Standards Australia, 1996, *Strategies for the implementation of a Public Key Authentication Framework (PKAF) in* Australia, SAA Miscellaneous Publication 75 - 1996, p.21.

[24] Digicash, 1996, *Digital Signatures and Smart Cards*, Presentation delivered at the 3rd International SmartCard Conference, Amsterdam, March; *http://digicash.support.nl/publish/digsig/*

about the subject of the certificate.[25] The PKAF, established by Standards Australia provides the scheme which outlines the functions and operating environment of the CAs.[26]

vi) Privacy

Security measures, specifically the use of encryption, in addition to protecting the authenticity and integrity of data communications, are also protecting privacy over networks.

Yet while these security measures can protect the actual message, they do little to protect or hide the trail created as transactions are conducted. Information sent over the Internet may pass through dozens of different computer systems. Each of these systems may be managed by different system operators, and each may be capable of recording the transaction. Most electronic forms of commerce leave records by definition. This includes details such as the amount being spent, the date, time and location of transaction, the identities of the parties and the nature of the goods being purchased.

How this information is protected is an obvious concern, both for merchants and consumers. In Australia, there is little protection afforded to privacy in an online setting.

There is no general legal right to privacy in Australia, although there are various protections in statute and common law. The most significant of these statutes is the *Privacy Act* of 1988. The Act lays down strict privacy safeguards which Federal Government departments and agencies must observe in collecting, storing and using personal information. In 1990 the Act was amended to include the credit reference industry but the credit aspects of the Act potentially extend to most persons or bodies providing credit. This was the first application of the Act to the private sector and as such is potentially important to Internet commercial transactions. The law aims to protect information relating to the credit-worthiness of individuals and to ensure that the use of this information is restricted to assessing applications for credit lodged with a credit provider.

In September 1996 the Attorney General's Department released a Discussion Paper[27] outlining a possible co-regulatory approach to further extending privacy protection.

vii) Implications for Australian Investors in Web-based Enterprises

Protection of Merchants' Income

A guarantee of payment to merchants who operate online is heavily dependent upon the implementation of standards and protocols for new payment systems, and codes or contracts which provide for the proper allocation of liability between the parties when a security failure occurs.

Many traditional payment mechanisms such as cheques and other negotiable instruments have not been recognised as yet by legislation in electronic form. However, they may still be used in paper form and even if they are issued overseas may be negotiable in Australia. Other traditional payment systems may be adapted in the future to cater for Internet commerce which takes place internationally.

The efficiency of credit-card payment systems however, particularly as they operate internationally, is well proven. This means of payment, when extended to Internet commerce with the development of the SET protocol and other standards, should be particularly useful for international transactions. However, using a credit card becomes impractical for payments below a certain amount, under which the proportion of

---

[25] ibid.

[26] Standards Australia, 1996.

[27] Attorney General's Department, 1996, *Privacy Protection in the Private Sector: Discussion Paper*, September.

administrative costs becomes excessive.[28] Stored value cards and other new payment mechanisms are anticipated to fill this gap.

Payment system confidence will not exist until proper security standards, protocols and codes have been developed to cater for other payment systems which are suitable for transactions of a smaller denomination.

Exposure to Liability

There is no real guidance in Australian law in this area, but analogies and comparisons to overseas developments can be of some assistance. Generally speaking, all persons and bodies who are involved in the content creation process for online material, together with ISPs in various forms, will have to be mindful of the laws which relate to advertising and consumer protection in Australia. The main defences have been outlined above, and whether any particular party can avail itself of them will be a matter of fact and degree, taking into account the involvement of the party in the content creation process, or the knowledge of, control over, or other relationship with the material which passes over the network.

Parties may also be in potential breach of foreign laws which apply in these areas but enforcement of these overseas laws, against parties or bodies outside the enforcing State's jurisdiction remains doubtful.

viii) Proposals for Reform

The study has revealed the following potential areas of reform:

- The UNCITRAL Model Law governing electronic business transactions requires recognition by legislation in Australia and similar laws also need to be enacted to provide for electronic consumer transactions.
- Appropriate conventions governing consumer sale of goods and consumer protection issues need be established at an international level.
- The Federal Attorney General's work in the area of electronic commerce needs to be given a higher priority.
- An industry level advertising code needs to be developed to cater for Internet advertising.
- Minor changes in the law are necessary, for example, to legally define new payment systems and to provide for broader application of electronic documents.
- Legislation may be required at a Federal level to provide a secure framework for electronic commerce and to provide for adequate privacy protection.

[28] European Commission, 1996, *Online Commerce and the Payment Issue*, April. http://www2.echo.lu/GST/Ecash.html

1. Introduction

In a recent study by International Data Corporation, the amount of Internet commerce being conducted world-wide was estimated to be around $3 billion in 1996, growing to $100 billion in the year 2000. Of the $3 billion figure, more than one-third of online sales are thought to be now completed on the Web, as opposed to telephone or facsimile, and the study reported that by the year 2000, the proportion should be much greater than two-thirds. To a large extent, the projected increase in electronic commerce conducted over the Internet is attributed to a ten-fold increase in Web users to about 163 million by the year 2000. Of particular note, although the world-wide percentage of Internet users who buy goods and services on the Web is forecast to reach 28 percent by December 2000, in the United States of America the percentage should grow to 45 percent.[29]

Clearly, the scope for business opportunities for Australian Web site operators will be enormous, but only if overseas users visit their sites. Although currently most Internet sales are being generated through the delivery of easily identified items such as software services and products like audio CDs, videos and books, in the near future sales are expected to increase sharply with the advent of online catalogues which allow consumers to search for items and compare the contents.[30]

From a legal perspective, commercial transactions which take place over the Internet share many characteristics with other traditional types of commercial transactions. However, Internet transactions also have distinguishing characteristics that may be critical in law. The focus of this study is principally on what is different about Internet commercial transactions, rather than on the characteristics shared. Internet transactions are different mainly because they involve technologies which transcend the scope of laws that have traditionally regulated commercial transactions and because they are more likely to be trans-jurisdictional in nature.

The law has reasonably well developed mechanisms for dealing with the problems pertaining to traditional transactions, eg. by advertising codes of conduct enforced by the agreement of media proprietors, on door-to-door sales techniques, by requirements for customers to be given written records of certain traditional transactions, and by rules of evidence which have evolved to accommodate the peculiarities of traditional transactions.

However the law and legal systems do not cope well with resolving disputes with inter-jurisdictional elements. Nor have they been able to catch up with new challenges constituted by the fact that today's sharp merchandiser is more likely to be coming into your home via the computer screen than by knocking on the front door.

Although some of the old laws still apply, their coverage is haphazard and whether they apply or not is largely a matter of chance. For example, it is arguable that the NSW door-to-door sales legislation will catch certain Internet transactions, but that the ACT legislation will not.

This study, undertaken for Australian Multimedia Enterprise Limited (AME), took place during the period late December 1996 to early March 1997. It consists of three parts:

- an executive summary;
- an analysis of issues;
- a literature review.

The first two parts are published together here as the *Issues Analysis*. The *Literature Review* is separately published.

AME stated that it was less interested in either 'business/business' or 'consumer/consumer' relationships, but instead wished to highlight electronic commerce transactions of a private nature in the 'business/consumer'

---

[29] IDC, 1996, *The Global Market Forecast for Internet Commerce*, Report No. W12339, November http://www.idcresearch.com/HNR/cpr4ic.htm

[30] Wright, C, 1997, 'Booming Online Sales Growth Swept up in Internet', *Australian Financial Review*, 29 January, p 3.

realm with the main perspective taken from the 'business' end. The object of the study was to clarify the legal environment associated with commercial transactions undertaken over the Internet, so that both the Web site operators and those investing in their businesses can better appreciate risks of a liability nature as well as risks associated with achieving the projected revenue flows. The client brief particularly noted that the study should highlight commercial transactions taking place via the Internet in an international context. For all the above reasons, the study tends to focus more on private transactions between the respective parties and analyses the following:

- jurisdictional issues;
- evidentiary and contractual issues;
- payments systems;
- relevant business models;
- sale of goods and consumer protection; and
- security and privacy.

On the other hand, it should be noted that the following issues, which also may have a significant impact on Internet commerce, are not dealt with as they were beyond the scope of the AME brief:

- defamation, copyright and intellectual property;
- computer crime and money laundering;
- taxation, sales tax, stamp duties and customs;
- corporations and securities regulation;
- record retention, such as is required under the Archives Act; and
- specific regulatory restrictions which might affect the merchandising of specific goods and services (eg. alcohol, shares, gambling, adult services).

2. The Commercial Paradigm

Key Issues: *What are the major differences between Internet and non-Internet transactions? What type of goods and services are available on the Internet? What are the essential characteristics of the parties to a transaction? What are the business models which can be applied?*

2.1 Background

The Internet is a worldwide web of computers, a 'network of networks'. Although originally devised for defence and academic purposes, the Internet is now accessible by ordinary computer users and its commercial potential is being exploited. In particular, it has been recognised that products may be marketed, and that information products may be distributed directly via the Internet, at a fraction of the usual cost. Various payment mechanisms are being developed to suit the requirements of the medium and to assist in realising its full commercial potential.

For some decades, commercial transactions involving some form of electronic trading have been well advanced throughout Australia in terms of consumer acceptance, business and banking practice as well as legal recognition. In the public eye, these transactions have arisen with the advent of plastic cards containing magnetic strips (credit or debit cards) that are swiped through magnetic card readers typically found in automatic teller machines (ATMs) and electronic funds transfer point of sale (EFTPOS) locations. Although not in the public eye, large businesses and their suppliers have adopted special commercial trading procedures known as electronic document interchange (EDI).

The electronic communications supporting ATMs, EFTPOS and EDI have always been carried over telecommunications systems and networks which service only the business parties involved. For this reason these systems and networks are variously said to be 'closed', 'private' and/or 'dedicated'. As each party is well identified and known in advance, in one sense or another before initiation of the electronic commercial transaction, matters critical to business confidence such as trust, security, confidentiality and liability are both predictable and controllable, and are therefore readily manageable to the satisfaction of all business parties affected.

In contrast, the public switched and mobile telephone networks are variously said to be 'open', 'public' and to a large extent exhibit 'any-to-any connectivity'. Parties utilising these networks for business (or private) purposes are generally not well identified or known in advance to one another and therefore matters such as trust, security, confidentiality and liability are far less predictable or controllable. Nevertheless, the affected parties have generally adapted their business (or private) transactions to these limitations and where necessary have adopted certain precautions to satisfy any individual or mutual concerns.

The *Shorter Oxford English Dictionary* refers to 'commerce' as "exchange of merchandise; buying and selling together" and 'business' as "trade, commercial transactions or engagements", whereas a 'transaction' is said to be "a piece of business; the action of passing or making over a thing from one person, thing, or state to another". A straight-forward definition of 'electronic commerce' describes it as "the conduct of business with the assistance of telecommunications, and of telecommunications-based tools".[31] Clarke says that whilst the term originated in the area of procurement of goods and services, it may nowadays also refer to a broader range of business processes such as those of registration and licensing, and the administration of the courts. Nevertheless, the actions of selling and purchasing constitute the dominant form of commercial transactions in general and electronic commerce in particular. Clarke reduces such transactions to ones that are either 'deliberative' or 'spontaneous'.[32] The former is said to be the kind practised by corporations undertaking major acquisitions, a type of transaction perfectly catered for by EDI. In contrast, spontaneous purchasing (together with the associated action of selling) describes the bulk of commercial transactions in that businesses and

[31] Clarke, R, *Electronic Commerce Definitions*, http://www.anu.edu.au/people/Roger.Clarke/EC/ECDefns.html

[32] Ibid.

individuals alike, with a minimum of rational decision-making, take note of the goods or services on offer, announce an intention to purchase same and then receive the requested goods or services in return for payment.

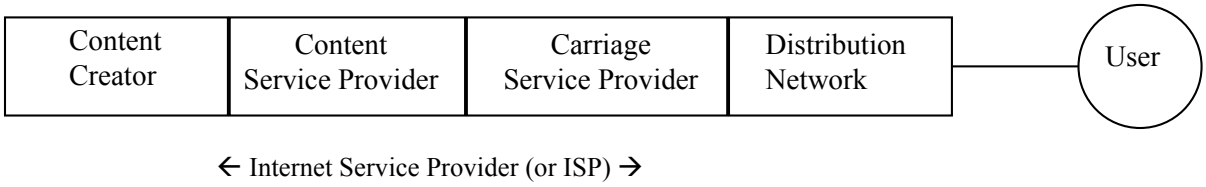
A subset of electronic commerce is that dealing with transactions made via the Internet, which (as a world-wide interconnection of networks each employing standardised protocols for data communication) involves input and output of transactional activities only via computers. Although access to these networks may be via local area networks (LANs) as well as the public switched telephone network (PSTN), the main characteristic distinguishing the Internet from any closed, private or dedicated system or network is that of being open to the public at large.[33] The Internet, effectively being a communicative layer above that of the PSTN, truly exhibits any-to-any connectivity. However, it is because of these characteristics that, during the early days of commercial transactions executed over the Internet, questions are raised about their level of trust, security, confidentiality and liability.

Any assessment of these matters and the legal issues arising first requires an appreciation of:

- the roles of various players within the Internet industry;
- the nature of the payment systems or mechanisms to be used; and
- the business models best suited for profiting from the Internet.

2.2 Structure of the Internet Industry

Determination of matters such as liability, jurisdiction, privacy, etc critically depend upon the role performed by each player providing a degree of service to one another or to an end user (consumer). Although none of these demarcations are necessarily clear cut in practice, the nominal structure of the Internet industry could be depicted as follows:



The Content Creator is contracted by the Content Service Provider (Content SP) to generate text, images and/or sound for incorporation into a Web site.

The Content SP creates, manages and/or controls the presentation of all content that is part of the Web site in a manner analogous to the exercise of editorial control by a newspaper publisher or television broadcaster. In addition, the Content SP may also provide 'hot links' to other Internet Web sites with or without their express permission. A Content SP would possess a full 'http' Internet domain address.

The Carriage SP purchases capacity from a carrier and adds a degree of service value that falls short of being regarded as 'content' and provides an access capability between subscribing users and the world-wide Internet of other users and service providers. Such added value is effected through TCP/IP protocols and associated software that establishes an Internet session. A Carriage SP would possess the highest level of Internet domain name, eg. 'connect.com.au', and would generally not be regarded as exercising editorial control. One possible exception to this, yet to be fully tested in law, is the chance that a Carriage SP may be deemed to bear some responsibility over content that is merely copied or 'mirrored' from another (distant) Content SP and made available for access by (local) users.

---

[33] Intranets, being Internet-type arrangements internal to businesses, do not constitute an exception to the above statement since once they connect to the Internet at large, those communications cease to adopt the characteristics of a closed network.

An Internet Service Provider (ISP) may in practice provide to users/consumers the functions of a Carriage SP and/or a Content SP. Depending upon the role performed by each particular ISP, the degree of liability for content-related matters would vary.

The Distribution Network acts as a mere conduit by transparently transferring the Internet service between the ISP and the User/Consumer. Such a network would be provided by a licensed carrier.

2.3 Internet Payment Systems or Mechanisms

Excluding bank monetary transfers, tokens and bartering, most conventional commercial transactions are effected through the mechanisms of cash (coins and notes), cheques and plastic cards (debit and credit). Both parties involved in each transaction appreciate and accept the concomitant advantages and disadvantages of the mechanism employed, be it one or more of: transaction cost, degree of security against fraud or default, guarantee of redemption, anonymity, record keeping (audit trail), negotiability, payment delay, etc.

Underpinning all but cash is the requirement for identification and validation by means of personal signature and/or personal identification number (PIN). Due to convenience and the absence of transaction costs, cash is typically used for small purchases and/or for larger purchases where anonymity is desired. With all mechanisms, another party is always involved such as a bank or plastic card issuer to underwrite or otherwise effect the final transaction. Standing agreements and/or precautionary practices are instituted to guard against fraud or other forms of loss. Questions of liability amongst all parties in a transaction are readily established.

With the advent of the Internet as an intervening or prime medium, all of the conventional payment mechanisms have been equivalently transformed or replicated in electronic forms, viz. digital, electronic or 'cyber' cash, cheques, credit/debit cards and signatures.[34] Other parties beyond the conventional banks and plastic card issuer then enter the scene to facilitate mechanisms such as electronic cash and signature verification.[35] A similar set of advantages and disadvantages for each Internet-based payment mechanism continues to apply. Special variants of these mechanisms, involving very low transaction costs, are being developed to facilitate micro-payments down to fractions of a cent.

The 'smart' card, being a plastic card containing a microprocessor, also constitutes a vehicle for delivering digital versions of cash, cheques, etc. When coupled with a card reader, the smart card behaves more like a highly portable and personalised PC rather than being peculiar to payments transacted over the Internet.

2.4 Business Models

Successful models for businesses to profit from transactions over the Internet are still in the early stages of development. They may be characterised in a variety of ways, depending on the outlook taken.

2.4.1 Market-Sector Focus

If treated on a market-sector basis, the business models can be grouped as follows:[36]

- business/business;
- mass (business/consumer) market;

---

[34] Peirce, M, *Payment mechanisms designed for the Internet*, http://ganges/cs.tcd.ie//mepeirce/Project/oninternet.html; also see: Tyree, A L , *Virtual Cash - Payments on the Internet*, http://www.law.usyd.edu.au/~alant/netpay.html.

[35] 'Smart' cards per se are not peculiar to Internet-based transactions as their inbuilt computational capability can be exploited as a vehicle enabling all types of electronic commerce.

[36] Yurman, D, 1996, *Internet Commerce; Emerging Business Models*, 11 December, PO Box 1569, Idaho Falls, ID 83403, USA, electronically published on the Internet by dyurman@world.std.com.

- online banking; and
- online advertising.

a) Business/Business Markets

Applications in this category will be initially dominated by existing EDI services shifting over to utilise Internet technologies. Due to the private or semi-closed nature of such proprietary business networks, the key characteristics underlying their financial transactions will be regarded with greater confidence although their market size will be inherently limited as the mass of consumers is excluded. One shining example of a successful Internet-based business model is that of Federal Express or FedEx. Customers (often but not always other businesses) can complete the entire administrative shipping function from their office or home PC with a high degree of confidence due to deployment of a proprietary authentication scheme.

b) Mass Markets (Business/Consumer)

Attracted to the ever increasing number of consumers accessing the Internet, business success will critically depend upon servicing an appropriate demographic niche. Broad examples include travel reservations and online merchandising (eg. adult entertainment, sports information). This category is further discussed in the next section.

c) Online Banking Market

This market, mainly a subset of the former, is seen both as a market in its own right and a supplement to broader business/consumer transactions. All of the above-mentioned payment mechanisms apply, although included in the term 'banking' are also the non-banks such as the issuers of plastic cards.

d) Online Advertising

Also mainly a subset of the broader business/consumer market, business models involving online advertising can operate in up to four ways:[37]

- sale of subscriptions for other online services
  (such as the business being that of an Internet service provider (ISP) who is not responsible for the content from other parties);
- sale of both connectivity and content
  (such as CompuServe, America Online who do accept responsibility for content);
- freely provided information
  (although supported by income from advertisers);
- sale of products to targeted niches
  (for products such as wines, books, music CDs, stock market data, etc. which may or may not be delivered by the Internet).

A further extension of market-sector categorisation defines two additional groupings;.[38]

e) Business/Administration and f) Consumer/Administration

where 'administration' refers to government organisations. Examples of such transactions include: government procurements, taxation payments, welfare payments and information access.

---

[37] Ibid.

[38] Esprit (European Commission), *Electronic Commerce - An Introduction*, http://www2.cordis.lu/esprit/src/ecomint.html#INTRODUCTION (section 3).

2.4.2 Transactional Focus

An alternative view of business models, expanding on the opportunities for business/consumer transactions, focuses more on the nature of the various financial transactions impacting upon the commercial prospects of a service provider on the Internet.[39] With this perspective, the following framework shows the parties involved along with possible jurisdictional challenges.

Party	Function	Jurisdiction
A	An entrepreneur seeking to gain from commercial transactions over the Internet, either as an Internet service provider (ISP) operating their own Web site or utilising the services of an independent ISP.	Typically located in Australia.
B	Consumer transacting with or through the ISP	Either located in Australia or overseas, although the enormous size of the overseas market offers the greatest scope for retail opportunities.
C	The banker, plastic card issuer and/or certification authority which together facilitate the relevant payment mechanisms employed between the above two parties.	Transactions within Australia would be typically supported by credit cards issued by major Australian banks; transactions involving an overseas consumer (the majority instance) would almost exclusively involve transnational operations.
D	The merchandiser, who may be either the Web site operator or another party, providing the actual product or service.	Either located in Australia or overseas depending on the offered product or service.

Within this transactional framework, business models can be structured either to offer free customer access or access by subscription. In reality, mixes of both may also occur during different stages of even the one commercial transaction.

a) Retail Model: Free Access to Web site

i. Direct Purchase Transaction (akin to that of a conventional retailer)

- Tangible Product or Service - not able to be delivered via the Internet;
  eg. wine.
- Intangible Product or Service - deliverable via the Internet;
  eg. software, music, text (newspaper, training course).

Here, the consumer orders the product or service from the Web site operator as retailer who either meets the requirement immediately or initiates another transaction for goods to be delivered transparently from another merchandiser.

ii. Agency Transaction (eg. a conventional commission agent, openly acting on behalf of another merchandiser)

eg. the writing of redeemable tickets, for entertainment, airflights, accommodation, etc., either separately delivered or electronically credited/vouched.

[39] Baatz , E E and L Romano, 1996, 'Does Your Business Model', *WebMaster*, December, p.12.

The consumer orders the service from the Web site operator acting as an agent who, under contract, represents the business provided by another party in writing the ticket (say) and passing on the consumer payment minus a commission.

eg. recruitment service.

Here, the consumer applies for a position with another party (a prospective employer) by electronically sending a CV to the Web site operator; upon selection by the employer, the Web site operator receives a fee whilst the consumer pays nothing.

iii. Advertising Transaction

eg. the Web site carries an advertisement for another, in like manner to a magazine publisher.

Typically on the basis of the number of 'hits' or Web site visits by consumers according to an agreed criteria, the Web site operator receives a fee for displaying the advertisement, whilst the consumer pays nothing. In a separate variant, consumers may even gain micro-credits for being exposed to advertisements.

iv. Passive Referral Service (party acting as a mere gateway)

eg. a shopping mall proprietor, such that the consumer is alerted to the existence of another merchandiser by means of a 'hot link' created at the ISPs Web site.

In addition to a possible 'spotter's fee' simply for the instance of the referral, the Web site operator could also earn a commission from any successful retail transaction undertaken between the consumer and the merchandiser.

b) Subscription Model: Fee for Access to Web site

Following payment of a fee by the consumer to the Internet service provider or Web site operator (eg. as initial registration only or as upfront subscription), either the listed services are free to access thereafter or ongoing data accessed is charged back to the consumer (perhaps on a 'pay-per-view/use' basis) by effectively decrementing an upfront subscription using one type of digital payment mechanism or another.

eg. examples include a training course provider, a newspaper publisher, an online database provider, a stockbroker, video hire.

2.4.3 Push vs Pull

Yet another approach to categorising business models, which not surprisingly overlaps with those previously discussed, is determined by how the user volunteers to receive information over the Internet. Traditional media such as broadcast television and radio, newsprint, outside advertising boards all try to get their message across to consumers in a passive mode, ie. by 'pushing' or without specific request. Web sites on the other hand are 'pull' media in that Internet users must actively seek out the information by clicking on a URL address or software icon.[40]

2.5 Practical Examples

The Kompass Web site claims to offer the latest, most accurate information on more than 1.5 million manufacturing and associated service companies in over 70 countries around the world, including 29,000 in

[40] Rothstein, E, 1997, 'The big push is coming to your monitor soon', *The Age*, 28 January , p. D5; also *Advertising Push or Pull?,* http://www.tcp.ca/April95.rtfhtml/Pushorpull.html

Australia. Although it's business plan anticipates revenues coming from two sources: advertising and subscription, access to the site will be free. Users can search the site freely, whereas subscribers can probe more detailed levels of information, such as company directors and business reports. Ultimately Kompass also aims to facilitate transactions through and offer insurance to purchasers for delivery.[41]

'Tunes.com' has pioneered a scheme that lets Web users page through a huge catalogue of virtually every music CD on the market and then allows a 3-second sample of each album to be replayed via "streaming audio". Users also get a photograph of the cover and a text file that details the artist's biographies and discographies. Upon deciding to buy a CD, the site allows for ordering by sending credit card information over a secure Internet link (as well as by traditional fax or mail order).[42]

Custom-designed news reports are being pushed into PCs, most famously via 'Pointcast', with 1.7 million users of its free software automatically getting reports from CNN, *Wired* magazine and other publications. Competitors are now offering material other than news, such as software updates, eg 'Castanet'. Because 'push' technology guarantees more visitors to a given Web site, operators such as Pointcast make their money by offering advertisers more attractive audiences. Advertiser's banners and images are inserted on the user's PC screen and are considered to have greater impact because they are part of the requested material.[43]

Microsoft is launching its 'Carpoint' Internet site designed as a used car buying guide. The listings would be updated nightly, and users could search by model, price range, mileage and location. Dealers pay an advertising fee to Microsoft to place their listings on Carpoint.[44]

The 'Electric Minds' venture claims that by sharing gossip and information in cyberspace, the virtual communities so created will offer business a new channel of communications that could dramatically increase the effectiveness of advertising. "We can produce a succinct digest for which people will be prepared to pay, rather than spending hours searching for it themselves, in the same way that many companies all over the world pay $500 or $1,000 a year for insider newsletters", its creator Mr Rheingold recently stated. Electric Minds proposes tiers of pricing depending on degree of personalisation, frequency and topic range.[45]

41 Hilvert, J, 1997, 'Kompass gets its bearings on Web', *The Australian*, 4 February, p. 7 (Computers).

42 Coates, J, 1997, 'Music buffs tune up for radio on demand', The Australian, 4 February, p. 28.

43 Rothstein, E, 1997, 'The big push is coming to your monitor soon', *The Age*, 28 January, p. D5.

44 Matassa Flores, M, 1997, 'Gates aims to net used car market', *The Australian*, 4 February, p. 33 (Computers).

45 Wright, C, 1997, 'Web the advertiser's new frontier', *The Australian Financial Review*, 13 February, p. 29.

3. The Legal Paradigm: Internet Law And Regulatory Models

Key Issues: *What are the various models or analogies applied to the Internet as a means or justification for regulation? What makes the Internet distinct from a regulatory point of view? What is the most appropriate way to classify the Internet from a legal or regulatory perspective?*

The Internet is a global medium which challenges national regulatory bodies. However, it can be strongly argued that the Federal Parliament has the capacity to make laws regulating the Internet under section 51 para (v) of the Commonwealth Constitution, which gives it power to legislate for 'postal, telegraphic, telephonic or other like services'. To date there has not been any moves to invoke this head of power to support legislation.

One of the major difficulties relating to development of laws applicable to the Internet (and resolution of questions of liability), has been the difficulty of classification of the medium. The Internet has been described as an 'electronic distribution chain' which does not reflect distribution channels for physical goods, nor does it fit comfortably into the broadcasting or telecommunications carrier models.[46] Likewise problems arise with attempts to apply publisher analogies taken from traditional defamation law for the purpose of classifying the various types of Internet service providers (ISPs) which are emerging in the medium, especially where the ISP has had no control over or knowledge of the material which passes through its service.

Internet Service Providers in their various manifestations, have emerged as the most identifiable intermediary between content and the user of the Internet, apart from the general carrier. As such they have been the focus of potential legislative control and liability. At the same time, there is no legal or policy guidance as to the appropriate classification of ISPs in Australia. A major problem of classification arises in that ISPs are emerging in a variety of forms and functions. They may be the original content creators of some material, but they also provide a launch pad for the material of a large number of other content creators. At the same time, they are an access point to material for Internet users. Given these differences, it is not surprising that judicial consideration of ISPs has led to differing results.

In an early defamation case in the United States,[47] a court found that CompuServe, as operator of a closed network, was analogous to an 'electronic, not for profit library', and had neither the opportunity nor the means to review all the material which it made available. By contrast, a United States Court in a later decision[48] has held an ISP liable as a publisher of defamatory statements on the grounds that it had used an automated content filter which screened out offensive material. The court found that the ISP, which operated over a closed network, had exercised a degree of editorial control.

However, this later decision has been overruled by legislation. The (US) Telecommunications Act of 1996,[49] which amongst others, applies to providers and users of interactive computer services, states that ISPs are not to be equated with publishers. The legislation appears to be approaching regulation of the Internet in terms of the telecommunications carrier model, a broader perspective but one which fits the overall deregulationist purport of the legislation.

On the other hand, Singapore[50] has classified the Internet as a broadcasting medium for the purpose of regulation. The Class Licensing Scheme in Singapore has been designed to regulate the broadcast of unlawful and objectionable material by requiring ISPs to be registered and to block out access to unauthorised Web sites.

---

[46] Pollard, S, 1996, *Electronic Payment Systems: the Legal Perspective,* Gilbert & Tobin, p 6 http://www.gtlaw.com.au/gt/news/updates/elecpay.html

[47] *Cubby v CompuServe,* 1991, 776 F. Supp. 135 S.D.N.Y.

[48] *Stratton Oakmont Inc., v Prodigy Services Co* 1995 WL 323710 NY Sup. May 24.

[49] In section 509.

[50] For an outline of the Singapore legislation see the *SBA Web site* at http://www.sba.gov.sg/sba.

Since the manner in which the Internet is classified from a regulatory perspective will affect the way activities ultimately take place in the medium, Internet development currently provides a degree of regulatory uncertainty for both users and service providers.

4. Jurisdictional Issues

4.1 Jurisdiction

Key Issues: *What relevance does the concept of jurisdiction have for Internet commerce? What general rules apply to the application of Australia's domestic laws beyond its own borders? In what circumstances can other nations extend their laws beyond their own borders? What nexus is required for Australian or overseas laws and courts to extend jurisdiction to Internet commerce? Can Australia 'block' the application of overseas laws?*

Jurisdiction arises as an issue in Internet commerce because of the global nature of the medium, which challenges traditional legal concepts of jurisdiction based on geographical borders. A country can readily enforce its laws within its own territory. But it has less capacity to enforce its laws against persons offshore or in respect of transactions which occur partly or wholly outside its territory. It has some capacity to enforce its laws for example by arresting executives of a company in its jurisdiction or taking action against a foreign corporation's subsidiary, but enforcement of laws outside a country's territory usually requires consent. The immediate consequence is that attempts to devise and enforce laws made by a country in respect of Internet commerce will be affected by jurisdictional constraints. At the same time in the context of international commerce, as a country's commercial activities extend beyond national borders there are growing pressures to reduce the emphasis on national sovereignty and to have an impact beyond geographical limits.[51]

The concept of jurisdiction in international law refers to the competence of a State to prescribe and apply its laws with respect to natural and legal entities.[52] It refers both to the territorial scope of the legislative competence of parliament, and the territorial limits within which the jurisdiction of a court may be exercised.[53] States establish rules of jurisdiction, both criminal and civil, as an act of sovereignty, an essential principle of which is that all states should have control over their internal affairs.[54] Prescriptive jurisdiction is the power of a state to make laws with respect to particular persons, while enforcement jurisdiction refers to the power of the state to apply those laws. Enforcement jurisdiction is territorial because a state may not exercise its own powers within the territory of another state, or in any other area beyond its own territory, without consent, unless in accordance with some principle of international law.[55]

There is a general presumption that the legislation and laws of a state are not intended to have extra-territorial effect and court jurisdiction is similarly limited. Some Australian legislation has extra-territorial application, in that it purports to apply beyond Australia's[56] geographical borders[57]. The jurisdiction of courts is determined by the original grant or statute which establishes the court together with any statute which may extend the jurisdiction of the court outside the territorial limits of the state.

For a State's laws to apply beyond its own geographical borders there needs to be some link or nexus between the activities and the State for the legislation to be invoked. Particular consideration needs to be given to whether there is sufficient connection with Australia and whether the extra-territorial provision will be

---

[51] Australian Law Reform Commission ALRC 80 p6.

[52] Chinkin, C M, *Foreign Relations, in Halsbury's Laws of Australia*, Volume 14, Title 215.

[53] Martin, EA (Ed); *A Concise Dictionary of Law* , 2nd Ed OUP 1990 p223.

[54] Subject to recognised principles of international law, which include amongst others international human rights law, and the rules proscribing the use of force.

[55] *Lotus Case (France v Turkey)* 1927 PCIJ ser A No. 10 (Judgment of 7 Sept).

[56] Australia's territorial jurisdiction includes its external territories.

[57] Unless there are clear and unambiguous provisions to the contrary, Australian trade laws are to be construed as having only territorial effect: 'Foreign Relations', *Halsbury's Laws of Australia*, Volume 14 para [215 390].

effective. Where an Australian court hears a case arising under legislation of that kind it may have jurisdiction to make determinations and to order remedies in respect of circumstances occurring outside Australia. However, its orders will only be enforceable within the territorial jurisdiction of the court.[58] Thus the extra-territorial scope of the legislation may increase the scope of the issues and evidence to be considered by the court, but will not increase the territorial scope of the remedies available from the court. Accordingly, when legislation is being considered for its applicability to extra-jurisdictional activities, the practicalities of enforcing the legislation in these circumstances must also be considered.

Australian laws which have extra-territorial scope give rise to a greater potential for overlapping jurisdiction between the courts of Australia and courts outside Australia. There is also a potential mismatch between the claim that the Australian court can determine and the remedies the Australian court is able to order in relation to the claim.

Attempts to enforce laws which apply extraterritorially against non-residents and other entities outside the jurisdiction can create political tensions. For example, United States courts have asserted the right to extend the application of domestic American antitrust law[59] to the conduct of foreign individuals and corporations which are operating outside the United States but where the effect of their conduct is alleged to impact upon the United States.[60] The assertion of jurisdiction is based on the effect of acts performed abroad on United States trade (the 'effects doctrine')[61] Australia has opposed the extension by the US of territorial jurisdiction and has enacted legislation to 'block' its enforcement by United States courts.[62]

The extra-territorial application of laws of an individual state assumes a special poignancy when those laws purport to regulate activities taking place on the Internet. The problem can be illustrated by the example of an Australian ISP, merchant or user who places an advertisement on a Web site in Australia which can be accessed throughout the world. Can this simple act of placing information on the Internet make the party subject to the laws of every jurisdiction in which that information may be accessed? It seems likely that it can. Curiously, recent attempts to provide an answer to this question have invoked a media marketing principle commonly known as 'push versus pull'.[63] According to this theory, whilst most of the advertising media to date have been push oriented (television, radio, print, billboards), the Internet is a pull media, in that users actively seek out or request to view or download material. Information being pushed into a jurisdiction is said to be akin to pushing paper, an act is arguably taking place within the jurisdiction and so it is said the laws of the jurisdiction are more likely to be invoked. Conversely, where material is mounted on a foreign Web site without specifically being directed to any particular audience or jurisdiction, it can equally be argued that no act has been done in the jurisdiction which would have the consequence of invoking its laws. The relevance of the 'push-pull' theory has to be questioned, however, by the introduction of services such as Pointcast, which has led the

---

[58] In general terms, remedies ordered by an Australian court are only enforceable within Australia and its Territories. The courts and administrative agencies of other nations are similarly constrained.

[59] (US) Antitrust Act 1890, 26 Stat 209 (US) (the 'Sherman Act') and the (US) Antitrust Act 1914, 38 Stat 730 (US) (the 'Clayton Act')

[60] As is noted later in the paper, the Trade Practices Act (Cth) (TPA) also has various extra-territorial operations.

[61] Which was set out in *United States v Aluminium Co of America* 148 F 2d 416 (2d Circ 1945). There was some move away from the doctrine in *Timberlane Lumber Co v Bank of America NT & SA 549 F 2d 597 (9th Circ 1976)* where it was held that the effects on American trade should be weighed against the interests of other states, taking into account a number of factors. See *Halsbury's Laws of Australia*, Volume 14 [para 215 390] and further cases cited therein.

[62] See the amicus brief in *Conservation Council of Western Australia v Aluminium Co of America (Alcoa) 518 F Supp 270* (District Court of Pennsylvania). The Australian position is shared by other states, including the UK. Blocking statutes were passed in Australia in 1979 and have been consolidated in the (Cth) Foreign Proceedings (Excess of Jurisdiction) Act 1984. The (UK) Protection of Trading Interests Act 1980 provided a model for some provisions contained in Australian legislation. *Halsbury's Laws of Australia* Volume 14 Foreign Relations[para 215-390] briefly explains the operation of the legislation and provides some useful further references.

[63] See for example, Bartlett, P and Deeble, M (1996): 'When Push Comes to Pull' BTCE Communications Forum Paper, Melbourne.

introduction of more push oriented technology to the Internet or at least blurred the distinction between push and pull as it applies to the Internet.

In criminal cases, a state may exercise jurisdiction where there is a link or nexus between the exercise of an alleged criminal act and the state. As indicated previously, the most widely accepted basis for the exercise of jurisdiction is territoriality. Territorial jurisdiction is established where the alleged offence occurred within the territory of the state.[64] States may also exercise jurisdiction over their own citizens, wherever they are situated. Persons or companies who engage in activities, such as gambling services, which take place on the Internet and constitute a criminal offence in a state where they are accessed may be subject to prosecution in that state, even though the service was being provided from another jurisdiction.[65] However, whether States can enforce criminal laws against persons not their own citizens or entities outside their jurisdiction is another matter, and generally speaking will require the consent of the other State.

The Attorney General of the US State of Minnesota has issued a policy statement[66] which sets out the enforcement position of the Minnesota Attorney-General's Office in respect of activities taking place on the Internet. The Memorandum on Jurisdiction states that 'Persons outside of Minnesota who transmit information via the Internet *knowing* that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of State criminal and civil laws'.[67] In July 1995 lawsuits were accordingly instituted against a number of companies and individuals allegedly operating scams and illegal business activities on the Internet. Minnesota Courts have upheld the extra-territorial application of State consumer protection statutes to illegal gambling activities operating on the Internet, where the service was provided by persons in another State of the United States.[68] The requisite link is provided by knowledge that the information will be disseminated in Minnesota. Assuming that these laws will be enforceable in an international context, whether nexus based on proof that the person ought to have known that the information may be accessed or 'pulled down' by a user in Minnesota is adequate, remains a critical issue. This is because the person may not be entitled to rely on a defence that the activity was lawful in the jurisdiction in which the activity took place, or that they were unaware that it was an offence in Minnesota.

4.2 International Law and Treaties

Key Issues: *What international treaties, conventions, model laws, standards and protocols have a bearing in the area of Internet commerce? What difficulties arise for the development of international principles applying to consumer transactions taking place on the Internet and for Internet commerce generally?*

By international law we mean the system of law regulating the interrelationship of sovereign states and their rights and duties with regard to one another.[69] The usual sources of international law are conventions and treaties, international custom and general principles of law.[70]

---

[64] *Lotus Case (France v Turkey)* 1927 PCIJ ser A No. 10 (Judgment of 7 Sept). A State may also assert jurisdiction when the commission of the offence takes place outside the territory but the effects of the alleged criminal act are felt within its territory.

[65] The act of placing the gambling service online will presumably take place in another State.

[66] http://www.state.mn.us/ebranch/ag/memo.txt

[67] The memorandum sets out a number of criminal and civil cases which are analogous to situations in which Internet activities could be found to constitute acts sufficient to invoke the jurisdiction of the Minnesota courts.

[68] The ruling was made by a State Court judge in Minnesota v Granite Gate Resorts No. C 6-95-007227 (District Court of Ramsay, filed July 18 1995). A further case of interest is that of Georgia Tech Lorraine, the European platform of the Georgia Institute of Technology, which has been sued for failing to comply with French law requiring that goods and services be offered in French in addition to any other language in which they may be offered. See www.cyberlaw.com

[69] Martin, E A, *A Concise Dictionary of Law* 2nd Ed 1990.

There is no really comprehensive system of 'international law' as such, and certainly no laws exhaustively governing contractual or other relationships between parties, and it is through a web of international conventions and treaties that the larger part of international relationships are defined.

As a general rule, international trade treaties negotiated by Australia with other countries neither bind Australian or foreign traders nor create enforceable rights or duties in the absence of incorporation into domestic law.[71]

An effective means of regulating Internet commerce at an international level is through the adoption and implementation of international treaties or conventions. Assistance can also be provided by model laws, protocols and technical standards. Some existing treaties governing various aspects of international trade will apply to Internet commerce, provided they involve business or trade transactions. However, it is evident that electronic commerce is making many of these agreements irrelevant as they fail to keep pace with commercial realities.[72] There have also been some international endeavours to develop model laws to govern Internet commerce on a more global scale, to introduce consistency in laws between nations and to help promote commerce in the medium. One apparent shortfall in this area, which has arisen as a consequence of the dis-intermediation effect of the Internet, is the lack of international principles governing consumer transactions. In the past, importers and traders have largely shielded consumers during the purchase of overseas products.

4.2.1 International Sale of Goods

One international convention of particular significance in international trade is the United Nations Convention on Contracts for the International Sale of Goods.[73] However, it should be noted from the outset that the Convention does not apply to consumer sales and hence will be inapplicable to the larger part of Internet transactions. It does apply, however, to business transactions which come within the terms of the Convention.[74]

The Convention does not apply to sales of goods bought for personal, family or household use, unless the seller, at any time before or at the conclusion of the contract, neither knew nor ought to have known that the goods were bought for any such use.[75]

The Convention governs only the formation of the contract of sale and the rights and obligations of the seller and the buyer arising from such a contract. It will be deemed to apply unless expressly excluded and the parties to a contract may exclude the application of the Convention in whole or in part.

The Convention has been adopted by legislation in Australian States and Territories.[76]

---

[70] Ibid.

[71] Fischer, S and A Hurley (1995) Trade and Commerce - International Trade, in *Halsbury's Laws of Australia* Vol 27 Title 420.

[72] Willis, A, 1996, *Legal Issues in Electronic Commerce*, IPAA/IIR Conference, Rydges Lakeside, 30 May.

[73] Vienna, 11 April 1980.

[74] The Convention applies to contracts of sale of goods between parties whose places of business are in different states when the states are contracting states; or the rules of private international law lead to the application of the law of a contracting state.

[75] The Convention does not apply to sales by auction, on execution or otherwise by authority of law, of stocks, shares, investment securities, negotiable instruments or money, of ships, vessels, hovercraft, or aircraft, or of electricity.

[76] (ACT) Sale of Goods (Vienna Convention) Act 1987, (NT) Sale of Goods (Vienna Convention) Act 1987, (NSW) Sale of Goods (Vienna Convention) Act 1986, (QLD) Sale of Goods (Vienna Convention) Act 1986, (SA) Sale of Goods (Vienna Convention) Act 1986, (TAS) Sale of Goods (Vienna Convention) Act 1987, (VIC) Sale of Goods (Vienna Convention) Act 1987, (WA) Sale of Goods (Vienna Convention) Act 1986.

4.2.2 United Nations Model Law on Electronic Commerce (1996)

The Model Law developed by UNCITRAL,[77] which has yet to be implemented in Australia, has been developed to facilitate electronic commerce internationally, by suggesting a common way in which national laws can be modified to resolve certain well known issues. These are:

- the recognition of data messages as satisfying the 'in writing' requirements of some documents;
- the recognition of data messages as satisfying the signature requirements of some documents;
- the recognition of data messages as satisfying the evidentiary requirement of producing the original of a document to prove the contents of that document;
- the recognition of data messages in the context of contract formation as constituting a valid offer and acceptance; and
- the recognition of data messages as having legal effect in certain circumstances.

As with the Vienna Convention, however, the UNCITRAL Model Law does not apply to consumer transactions[78].

4.2.3 The United States Framework for Global Electronic Commerce

The policy position of the United States in electronic commerce rates a mention due to its significance in the Internet 'market'. Although without the weight of a Convention, the Clinton Administration has developed a draft policy for Global Electronic Commerce, through an interagency working group on Electronic Commerce[79]. It lays out the principles which should support policy development, articulates a number of policies, and outlines a 'road map' for discussions with US international trading partners to ensure the development of a free and open global electronic marketplace. The policy articulates a non-regulatory, market-oriented approach to electronic commerce policy development and supports in particular the development of a global uniform commercial legal framework that will facilitate commercial transactions.

4.2.4 The World Trade Organisation (WTO)

Amongst the many prospective international fora which could have potential impact in the field of electronic commerce is the WTO. The WTO was established in 1995 and oversees the General Agreement on Tariffs and Trade (GATT) and multilateral agreements which resulted from the Uruguay Round (1986-94). It provides both a code of rules and a forum for countries to address trade problems. Recent initiatives in the WTO include telecommunications liberalisation (for basic voice services) and international recognition of intellectual property rights. A field in which the WTO may provide a good forum for international initiatives, particularly if it involves trade liberalisation which is part of its basic charter, is global Internet commerce.[80] A major shift in thinking will evidently be required in order to deal with consumer, as opposed to trade, transactions.

4.2.5 Carriage of Goods and Other Issues in International Transactions

One area of law of potential significance in Internet commerce is the law relating to carriage of goods. However, this law is ill suited to apply to the general range of consumer transactions which take place over the Internet, unless they involve goods of a sizeable nature. They are unlikely to arise for items delivered by post,

---

[77] The United Nations Commission on International Trade Law (UNCITRAL) is an organisation based in Vienna which develops model laws and standard documents directed at facilitating international commercial transactions.

[78] Consumer transactions are specifically exempted from the application of the Model Law.

[79] *A Framework For Electronic Commerce,* 11 December 1996, *http://www.iitf.nist.gov/eleccomm/gol_comm.htm*

[80] Willis, A, 1996, *Legal Issues in Electronic Commerce*, IPAA/IIR Conference, Rydges Lakeside 30 May.

which will more than likely fall within the ambit of postal conventions. The law will apply in the main to business transactions over the Internet where they involve carriage of goods.

International transactions associated with the international sale of goods usually involve contracts of sale, carriage, insurance and finance. Sea carriage is essentially governed by the Carriage of Goods by Sea Act 1991 (Cth)[81] and the Amended Hague Rules 1979[82]. International carriage by air is principally governed by the Convention for the Unification of Certain Rules relating to International Carriage by Air (Warsaw Convention) 1929 and the (Cth) Civil Aviation (Carrier's Liability) Act 1959.[83]

4.3 Private International Law

Key Issues: *What are the steps involved in applying the law to a transaction with international dimensions? How do we decide which country's laws apply to a transaction with international dimensions? How will Australian courts resolve conflicts of laws issues arising from Internet transactions? What problems do the conflicts of laws create for enforcement of contracts taking place across international borders and the range of remedies available? What are the consequences for consumers and sellers of jurisdictional uncertainties? What are the available remedies for parties to an Internet transaction with international dimensions and what are the risks and prospects of enforcing them?*

Conflicts of Laws

Jurisdiction principles have led to the evolution of rules to deal with private transactions which take place across international borders. Disputes which arise in the context of Internet transactions taking place across international borders will bring into play the part of the national law of a country that establishes rules for dealing with cases involving a foreign element. The rules deal mainly with relations between private citizens and organisations. This area of law is referred to as 'private international law' or 'conflicts of laws'. Private international law is concerned with resolving the issues which arise because a matter has a connection, or claimed connection, with the legal system of more than one nation ('law area').

These rules will come into play when a transaction between parties in different law areas results in a dispute (eg, non-payment under a contract of sale) which requires resolution by a court. In such a case the court in which the proceedings have been brought (the 'forum') must decide whether it should extend its jurisdiction, law or institutions to the matter before it, or recognise and/or apply the jurisdiction, law or institutions of another law area.

In an international context, the private international legal systems of many countries are underdeveloped. They are inadequately evolved to provide proper dispute resolution procedures, as well as in substantive terms, to properly support the rights and remedies of parties engaged in activities which take place across international borders. Quite apart from these shortcomings, the laws have evolved slowly to accommodate paper based transactions, and physical distribution channels and contacts. Accordingly, there is no concept in the law which can identify what constitutes an adequate link between digital or electronic activities or entities and a particular jurisdiction.[84] Such principles will have to take into account the particular characteristics of the Internet as an 'electronic distribution chain' which make it different from the physical world, and the various parties connected with the system, including carriers, service providers, users and others.

---

[81] Which does not recognise electronic documentation. See below.

[82] Also known as the Visby Rules.

[83] Parties to an international contract of sale may also choose to incorporate customary terms of trade, which can have the effect of modifying or excluding the application of the Convention. With respect to sea carriage, customary terms of trade include the 'FOB' (free on board) contract and the 'CIF' (cost, insurance and freight) contract . Incoterms 1990, which are *s*tandardised rules for the interpretation of trade terms designed in cross-border sales and purchases of goods, may also be applied. They were developed and are promoted by the International Chamber of Commerce (ICC) and have been endorsed by the United Nations Commission on International Trade Law (UNCITRAL).

[84] Rose, A, 1997, *Electronic Commerce and the Law Free Zone*, ASC Conference on Electronic Commerce, Sydney, 4-5 February.

The Australian Law Reform Commission (ALRC) has undertaken a major study of legal risk in international transactions,[85] which arose out of concerns about the effectiveness of the legal remedies available when commercial transactions cross international borders. The Report focuses on civil remedies in international commerce available under Australian law and under multilateral and bilateral instruments or arrangements. The Commission found that cross border legal problems create two types of risks for Australian firms. The first is the risk of being involved in a dispute that involves the laws or courts of more than one country. These disputes are marked by high levels of cost, complexity and delay. The second risk is where the law fails to provide appropriate support for an Australian firm in its international commercial transactions. The ALRC also examined electronic commerce which it referred to as an emerging priority for cross-border legal initiatives. It recommended that the Attorney General's Department work in electronic commerce, which amongst other things, involves the establishment of an expert group to examine legal issues in the area, should be given a high priority.[86] However, to date, neither terms of reference nor members of the expert group have been settled.

The Report contains an extensive analysis of problems of jurisdiction and enforcement of civil remedies in disputes involving a cross border element in commercial transactions which is highly pertinent to Internet transactions, albeit broader in application. It is not proposed to reproduce the analysis of issues raised in that Report,[87] but the following discussion contains a summary of some of the most relevant issues in the context of Internet commerce.

Jurisdiction

The steps taken in a conflicts of laws case can be described in general terms as follows. In each case involving an international dimension the court may first have to consider the question of jurisdiction. The jurisdiction of the court will normally be confined to matters occurring within its law area or to persons having a defined connection with its law area.[88] The requisite connection between the subject matter and the forum or between the parties involved and the forum must be established before the court can hear the case. A court's jurisdiction in contract cases is established, amongst other things, if the contract is held to have been made in the jurisdiction.[89]

Legal proceedings are commenced in Australia by service of initiating process.[90] Service of initiating process outside the geographical jurisdiction of the court is only permitted in defined circumstances. The court will need to be satisfied at that stage that it has jurisdiction to hear the case raised by the initiating process. After service the defendant can do one of the following:

- choose not to come to Australia to defend the proceedings;
- enter a conditional appearance in the Australian court, submitting to the court solely for the purpose of challenging jurisdiction;
- appear in the Australian court to defend itself on both jurisdictional and substantive grounds; or
- initiate counter-proceedings in a foreign jurisdiction.

If the defendant does not come to Australia to defend the proceedings, any assets it has in Australia and its ability to visit or do business in Australia in the future will be jeopardised. The plaintiff will need to take action in the defendant's jurisdiction, either by commencing new proceedings or applying for recognition of its Australian judgment. Even if the Australian judgement is recognised, the foreign court may not grant the same remedies.

---

[85] Australian Law Reform Commission Legal Risk in International Transactions, ALRC 80 (1996) Commonwealth of Australia.

[86] ALRC 80 Ch 5.

[87] The Report should be consulted for its comprehensive analysis of key issues which will be directly applicable to Internet and electronic commerce.

[88] *Laurie v Carroll,* 1958, 98 CLR 310.

[89] As to what needs to established for a contract to be held to have been made in the jurisdiction, see below under choice of law in contract. Jurisdiction may also be established by other means.

[90] ALRC 80 Part II Chapter 6.

If the defendant challenges the jurisdiction of the Australian court, it can argue not only that the matter is beyond the power of the court but also that the court should, in its discretion, refuse to hear the matter on the ground that the Australian forum is clearly inappropriate.[91] Depending on the laws of its own jurisdiction, the defendant may also commence proceedings in its own jurisdiction seeking an order prohibiting the plaintiff from continuing proceedings in Australia[92] or a favourable declaration which would negative any rights over property sought by the plaintiff in the Australian forum.[93]

The complexity of jurisdictional issues have led to a great deal of cost and delay in international litigation. There is also potential for parallel proceedings in two or more countries, for incomplete or inadequate remedies out of any one court and for lengthy legal argument challenging jurisdiction. For any particular cross-border dispute there are likely to be overlaps or gaps between the jurisdiction of an Australian court and the jurisdiction of courts outside Australia. Conflicts of laws issues which arise in Internet commerce are likely to be far more complex than those which occur in the context of physical or paper trading. It will become commonplace for the manufacturer, customer, seller, and principal bank to be situated in different jurisdictions. When these types of cases have come before courts in the context of physical transactions, it has been a matter of very fine judgment as to which jurisdiction has the closest connection.[94]

The ALRC identified a natural tendency to try to solve problems of enforcement of legal remedies, and the difficulties faced by companies in adapting to laws of several jurisdictions, by extending the extra-territorial effect of Australian laws or court orders, or by creating a supra-national authority or regulatory regime to overcome the inefficiencies of separate national regulation.[95] However, the ALRC found this type of solution to be effective in only limited circumstances. It held the view that often it will be more effective, and will better suit Australian business interests, to maintain territorial limits and seek greater cooperation in applying local laws quickly and cheaply.[96]

Choice of Law

After any issue of jurisdiction has been resolved the court may need to consider the question of the applicable law. Usually this is framed as a choice between the application of the law of the forum or the law of another law area. In some cases, which could become more frequent in the context of Internet commerce, the conflict may arise between two foreign laws.[97] In such a case the court must make a choice between the two laws, this stage is referred to as the 'choice of law question'.[98]

Particular rules have been established in the 'choice of law' process which will apply to issues arising from a contract made across international borders. Identifying the applicable law will be important to establish the rights, obligations, enforceability and available remedies for the parties to the contract. It will establish, for example, whether provisions of legislation which purport to incorporate terms into certain types of contracts, such as the Sale of Goods legislation which has been enacted within all Australian jurisdictions, will be applicable.

Enforcement of Cross-border Civil Remedies

There are a number of consequences of a finding by an Australian court that it either does not have jurisdiction to hear a case or that the laws of another jurisdiction apply to a transaction. The aggrieved party may be left with the prospect of having to commence an action overseas which may not be warranted for the amount at

---

[91] forum non conveniens.

[92] This is referred to as an anti-suit injunction.

[93] The plaintiff can in turn counter this by seeking an anti anti-suit injunction in Australia.

[94] See for example some of the cases listed under Choice of Law in Contract, section 5-2 herein.

[95] ALRC 80 Overview.

[96] See the Overview of the Commission's Report, ALRC 80.

[97] See for example, *Tomkinson v First Pennsylvania Banking and Trust Co*, 1961, AC 1007 where the choice lay between Cuban and Pennsylvanian law.

[98] The law which is ultimately applied is referred to as the 'proper law'.

stake in the transaction. Otherwise, the aggrieved party may be subject to the uncertainties of outcome when the laws of another jurisdiction are deemed to apply in a case. Even then, an Australian court may not be able to deliver appropriate remedies due to jurisdictional constraints. Conversely, the judgment of an Australian court may not be enforceable in another country, where the defendant resides or carries on business.

Enforcement Outside Australia

The judgments of Australian courts cannot be unilaterally enforced outside Australia, which would otherwise breach the sovereignty of other countries. However, Australian law includes some mechanisms to assist in enforcement outside Australia and to encourage international cooperation in enforcement proceedings.[99]

One of the principal mechanisms for international cooperation in enforcement proceedings is reciprocal recognition of judgments. Under Australian law, foreign judgments will be recognised and enforced in Australia if they fall within the category of judgments recognised under the Foreign Judgments Act or if they otherwise qualify for recognition under the common law. The Foreign Judgments Act provides a framework for enforcement of foreign money judgments in Australia based on assurances that the foreign jurisdictions to which the Acts applies will substantially reciprocate in the enforcement of judgments of the Australian Supreme and Federal Courts. The Act is limited in its application to nominated countries.[100] Under the Act, a mandatory procedure is established for the relevant Australian court to register and enforce money judgments of foreign courts to which the Act is proclaimed to apply. Non-money judgments such as injunctions are within the scope of the Act but have not yet been prescribed in the regulations in relation to any of the reciprocating foreign jurisdictions. If the Act is not proclaimed to apply to a particular foreign jurisdiction then enforcement of the foreign money judgment in Australia is to be conducted at common law, requiring the judgment debtor to be served in or having submitted to the jurisdiction of the enforcing court in Australia.

In enforcement proceedings taken outside Australia, a party attempting to enforce an Australian right can only obtain relief in the form and manner which the forum in the foreign jurisdiction provides. The degree to which the foreign court will modify the remedy will depend on the mechanisms for enforcement available in the foreign jurisdiction and how closely the remedies from the two jurisdiction compare.

Australia has one other separate agreement regarding reciprocity of recognition and enforcement of judgments from a foreign jurisdiction with the UK.[101] The agreement contains an undertaking by the United Kingdom to enforce money judgments and arbitration awards (other than matters in respect of taxation and maintenance) of the Federal, Supreme and District Courts of Australia[102].

In the context of Internet commerce taking place internationally, there are two matters to be considered. The first is that judgments will only be enforceable against a few nominated foreign jurisdictions under the legislation, or under common law which requires the defendant to submit to the jurisdiction. The second relates to quantum of money judgments. The legislation only applies to higher courts. Judgments for sums of tens to hundreds of dollars will not be enforceable.

Foreign Evidence

Disputes with a cross-border element usually require evidence to be collected outside Australia. If a person outside Australia who has the evidence does not wish to give it, a court order will be needed to compel the person to do so. However, Australian courts can only compel evidence to be given within Australia and its territories. There are two mechanisms which address this difficulty: letters of request and certain mutual assistance powers.[103]

---

[99] See ALRC 80 Part II Chapter 6.

[100] California, USA, Germany, Switzerland, Cook Islands, Indonesia and Vietnam.

[101] Agreement between the government of Australia and the Government of the United Kingdom of Great Britain and Northern Ireland providing for the Reciprocal recognition and Enforcement of Judgments in Civil and Commercial Matters 1990.

[102] The agreement came into effect on 1 September 1994.

[103] See ALRC 80 Part II Chapter 6.

Section 7(1) of the Foreign Evidence Act empowers the courts to make certain orders relating to the giving of evidence by a person outside Australia. If it appears in the interests of justice to do so, the court may order:

- the examination of a person outside Australia before a judge, court officer, or other nominated person;
- the issue of a commission for the examination of a person outside Australia;
- the issue of a letter of request to the judicial authorities of a foreign country to take the evidence of a person or cause it to be taken.

The letter of request will be the most useful procedure if the person outside Australia does not wish to give evidence since it can lead to appropriate compelling orders from a court with jurisdiction over that person.

It appears that under the Foreign Evidence Act, letters of request cannot be issued for the purpose of obtaining only documentary evidence, unattached to a record of oral testimony. At the same time, Australian courts do have the power to order the production of documents alone in response to a letter of request from a foreign court. Concern has been expressed that if this interpretation of the Act is correct, it would prevent much evidence being obtained that is needed for commercial matters, particularly from corporations.[104] For the purposes of proving Internet transactions, the application of this legislation to evidence contained electronically will also need to be addressed.

Jurisdiction Clauses And Trading Partner Agreements

Parties engaged in Internet commerce may alleviate many of the above difficulties by entering into trading partner agreements if there is an established or ongoing business relationship between them, or include clauses in contracts which submit disputes to the jurisdiction of a particular country. These are discussed further in the next section.

[104] See ALRC 80 Part II Chapter 6 and references cited therein.

5. The Internet Transaction

Key Issues: *How do we establish the terms of an international contract made via the Internet, and what country's laws govern the contract? What problems arise for enforceability of the contract? What solutions have been developed?*

There are a number of issues which arise in identifying the nature of a contract with international dimensions. The first involves establishing the terms of a contract made via the Internet. The second issue relates to establishing the law which governs the terms of the contract under the principles of private international law. The third issue relates to enforcement and arises as a consequence of traditional laws requiring certain contracts to be in 'writing' or evidenced in writing. Electronically generated documents may not fall within the purview of these laws. Related to this is the law of signatures which arises as an issue not only in respect of some documents which depend on signatures for their enforceability but also because of new developments in the area of 'digital signatures'. Finally, traditional solutions to some of these problems, such as trading partner agreements and their limitations, are discussed.

5.1 The Electronic Contract

In the absence of legislation providing for the recognition of electronic contracts, the terms of an Internet contract will be established under general law of contract and the principles of private international law, in largely the same manner in which terms of a contract are established in the physical world. Generally speaking, the terms can be established by writing, orally, or implied from the conduct of parties. Other terms may be incorporated into contracts by legislation. Some contracts may not be enforceable by reason of legislation requiring certain contracts to be in writing or evidenced by a written note or memorandum, but this will not affect the existence of the contract. It merely means that the contract will not be enforceable by a court.[105]

However, some assistance in this area could be provided by a legislatively recognised 'electronic contract' which would include rules about, amongst other things, the time and place of offer and acceptance, what constitutes a valid electronic offer or acceptance, and presumptions about which law will apply to the contract.

5.2 Choice of Law in Contract

The proper law of a contract is the system of domestic law which defines the obligations assumed by the parties to the contract. There is no international law which exhaustively defines the obligations under a contract.[106]

The situation is clearest where the parties have chosen the law which will apply. The parties may expressly choose the body of law which will apply to all or part of their contract, but in the absence of any express choice or necessary implication from the contract an Australian court will look for the system of law with which the transaction has its closest and most real connection. The test is similar in the United Kingdom and most common law jurisdictions.

There are no specific presumptions to be applied in the search for the system of law with the closest and most real connection.[107] A list of factors is provided by *Halsbury's Laws of Australia*[108] as at times having been significant:

---

[105] Contracts requiring writing under the Statute of Frauds and other similar legislation are examined further below.

[106] However see *Deutsche Schachtbau-und Tiefbohrgesellschaft mbH v Shell international Petroleum Co Ltd,* 1990, 1 AC 295 at 316 per Sir John Donaldson MR, CA.

[107] *McLelland v Trustees Executors and Agency Co Ltd*, 1936, 55 CLR 483 at 493 per Dixon J.

- the place of contracting;[109] communication of acceptance determines the time and place at which the contract is formed, and cases deal with communications by fax, telex, mail and other means.[110] The general rule is that a contract is formed at the time and place that the acceptance is received, unless accepted by post, in which case the contract is formed at the time and place of postal of the acceptance. However, instantaneous communications do not fall within this rule, and it has been held that where an offer to sell goods is accepted by facsimile or telex or by telephone the contract is made at the place where the notification is received. Arguably, e-mail would fall into the latter category of instantaneous communications despite any time lag in delivery,[111]

- the place of performance of the contract;[112]

- the language and form of the contract;[113]

- the place of residence of the parties to the contract;[114]

- in relation to shipping contracts, the flag of the ship;[115]

- in a borrowing transaction, the residence of the lender;[116] and

- in the case of a letter of credit, the place where payment is to be made on behalf of the issuing bank against presentation of documents;[117]

- in the contract between banker and customer, the place where the accounts are kept;[118]

- where there is a choice between the law of a place which would uphold the contract and the law of a place which would invalidate it, the law of the place which will sustain the contract and its provisions.[119]

Normally, a court will presume that the parties intended to refer the entirety of their obligations to one system of law only. However, sometimes the court will find that a particular part of the contract is governed by a different law than that which governs the primary obligations under the contract.

Some Australian State and Federal legislation purports to apply mandatory rules to contracts entered into within the forum, or which are to be performed within the forum, or which would have been governed by the law of the forum but for any choice, notwithstanding any agreement as to the proper law.[120] Such a mandatory rule will not be applied to contracts which, objectively considered, are governed by the law of another jurisdiction unless they fix upon an event which occurred within the forum.[121]

---

[108] *Halsbury's Laws of Australia*, Volume 4 Title 85, para 85-1180

[109] *Mendelson-Zeller Co Inc v T&C Providores Pty Ltd,* 1981, 1 NSWLR 366. Compare *Amin Rasheed Shipping Corp v Kuwait Insurance Co,* 1984, AC 50 at 62 per Lord Diplock, HL.

[110] *Entores Ltd v Miles Far East Corporation*, 1955, 2 QB 327; *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelgesellschaft mbh*, 1983, 2AC 34.

[111] There are no decided cases on this point, but courts have traditionally been reluctant to extend the application of the postal acceptance rule to any further categories.

[112] Compare McLelland v Trustees Executors and Agency Co Ltd, 1936, 55 CLR 483 at 492 per Dixon J.

[113] Amin Rasheed Shipping Corp v Kuwait Insurance Co, 1984, AC 50.

[114] Chellaram v Chellaram, 1985, Ch 409 at 425 per Scott J.

[115] Coast Lines Ltd v Hudig & Veder Chartering NV, 1972, 2 QB 34.

[116] Tomkinson v First Pennsylvania Banking and Trust Co, 1961, AC 1007 at 1068 per Lord Denning, HL.

[117] Power Curber International Ltd v National Bank of Kuwait SAK, 1981, 3 AllER 607.

[118] Libyan Arab Foreign Bank v Bankers Trust Co, 1989, QB 728 at 746 per Staughton J.

[119] Per Fox J,(obiter) Permanent Trustees Co (Canberra) Ltd v Permanent Trustee Co of NSW Ltd, 1969, 14 FLR 246 at 254 (SC ACT).

[120] (Cth) Trade Practices Act 1974 s 67.

[121] *Gosper v Sawyer (1985) 160 CLR 548.*

The simplest means for parties to alleviate uncertainties of surrounding applicable law is to make an express agreement at the time of contracting about the law which will govern their contractual relationship. For business transactions, between parties which conduct business regularly, a trading partner agreement may be entered into. The same result can arguably be achieved in consumer transactions on the Internet by the appearance of terms of contract at the time of ordering by the Internet consumer. These terms should include terms about governing law and jurisdiction and, provided they are properly brought to the attention of the customer, will be enforceable by analogy to the ticket cases in contract law.[122]

[122] Pollard, S, 1996, *Electronic Payment Systems: the Legal Perspective*, Gilbert & Tobin, p6 http://www.gtlaw.com.au/gt/news/updates/elecpay.html

5.3 Enforceability

5.3.1 Evidence and Electronic Documents

Key Issues: *Which types of electronic documents can be used under Australian and international law? Which documents need to be evidenced in writing or require paper evidence? What are the problems of proving electronic documents and paperless transactions in courts in Australia and overseas. What impact do the various Evidence Acts around Australia have on proving electronic documents and contracts? What constitutes a valid signature, and which documents require it to be enforceable?*

Formalities and the Statute of Frauds

Although there is no general formal requirement of writing in the law of contract, some legislation makes it necessary for certain contracts to be evidenced by a written note or memorandum if they are to be enforceable by a Court. These contracts are derived from the requirements of England's Statute of Frauds 1677 (UK). In Australia, the members of this group of contracts have been eroded so that in most jurisdictions the only significant types of contract that must still comply with the modern derivatives of the Statute of Frauds, are contracts for the disposition of an interest in land and contracts of guarantee.[123] However, the position across Australia is not uniform. For example, it is still necessary for contracts for the sale of goods over a certain amount to be evidenced in writing if sued on in the NT, Tasmania and WA.

The statutes prescribing requirements that contracts satisfy formal requirements of writing fall into two categories: legislation derived from the *Statute of Frauds 1677* (UK) and consumer protection legislation. Examples of the latter include credit transactions, commercial sale of second-hand motor vehicles, door-to-door sales, lay-by sales, residential tenancy agreements and others. Non-compliance with the statutory requirements has different consequences depending on the legislation.

The various Interpretation Acts which have been enacted in Australian Federal, State and Territory jurisdictions,[124] together with caselaw, provide guidance to what constitutes 'writing' or 'written note or memorandum' for the purposes of a contract.[125] But taken together, electronic data does not seem to satisfy these requirements, unless a hard copy document is produced.[126] Thus there is still legislative insistence on paper transactions even though technology is moving to paperless transactions, such as contracts brought about by electronic data interchange (EDI).[127]

Electronic or EDI Contracts

It is possible for commercial entities to make contracts with each other through computers whereby the transaction is initiated by the computer. For example, a manufacturer may have an arrangement with a supplier of component parts under which, when stocks fall to a certain level, an order for more parts is automatically sent. The component manufacturer's computer processes the order and a contract is made.[128] This paperless

---

[123] Even contracts of guarantee need no longer be evidenced in writing in the ACT, NSW and SA.

[124] *Acts Interpretation Act 1901 (Cth),* s 25; *Interpretation Act 1967 (ACT), s 17; Interpretation Act 1987 (NSW), s 21(1); Interpretation Act 1978 (NT), s 26; Acts Interpretation Act 1954 (Qld) s 36; Acts Interpretation Act 1915 (SA), s4; Acts Interpretation Act 1931 (Tas), s 24; Interpretation of Legislation Act 1984 (Vic) s 38; Interpretation Act 1984 (WA), s 5.*

[125] The Evidence Acts also have an impact in this area. See further below.

[126] There is some scope to argue that a screen display may meet the requirements of some of the legislation by constituting a representation of words in visible form.

[127] An imaginative court could extend the idea of a note or memorandum to electronic data which, at least initially, constitute evidence of the paperless transaction.

[128] see Riordan, J (Ed), 1994, *The Laws of Australia*, The Law Book Company Ltd Vol 7 Contract, General Principles Title 7.2 Vitiating Factors.

transaction may be unenforceable because there is not sufficient note or memorandum.[129] In sale of goods cases, the problem is restricted to the Northern Territory, Tasmania, and Western Australia, the other jurisdictions having abolished the statutory requirements. However, in those three jurisdictions, the problem may be overcome by a subsequently generated hard copy of the order.

The usual method used to deal with potential legal problems that may arise in EDI transactions is by establishing a trading partner agreement, which can provide for a hard copy to be generated in the event of it being needed by either party or alternatively, can include a clause under which both parties agree not to rely on a *Statute of Frauds 1677 (UK*) defence.

The Evidence Acts

Certain types of electronic documents can be introduced into evidence in court under the Evidence Acts in Australian Federal, State and Territory jurisdictions. Any computer- produced material has the potential to be introduced into evidence, including all forms of computer output: screen displays, printout (both text and graphic), data stored in magnetic or optical forms on discs, diskettes, or CD-Rom, and audible output.[130] However, the approaches under the legislation vary in the situations and types of material that can be used. The legislation is also limited in that it does not govern proof of the fundamentals of contract formation where a paper or written document is required.[131] However, the legislation is useful for proving certain types and aspects of a commercial transaction between parties. Unfortunately, we can only speculate on its relevance to Internet commerce, especially where an international contract is being examined. Evidence held on open networks will be accessible in any event, but on its own, the legislation is unlikely to reach to computer produced evidence which is contained on closed foreign networks.

Three different approaches have been adopted to determine the admissibility of computer produced evidence in Australian legislation.[132] The 'computer specific' approach is specifically directed to the admissibility of computer produced evidence,[133] while the 'business records' approach sees computer produced evidence merely as one aspect of the general question of admissibility of business records.[134] Finally, some jurisdictions have adopted both approaches. The Commonwealth and New South Wales Evidence Acts 1995[135] represent the most general of the three approaches.

The Evidence Act 1995 (Cth) has been heralded as a model law for computer evidence and deserves a few brief comments. The Act may facilitate electronic commerce in the following three areas:

- It allows proof of the content of electronic records by a print-out of those records;[136]
- The exceptions to the hearsay rule have been widened, particularly in relation to business records. Section 71 makes telecommunications such as electronic mail exempt from the hearsay rule so far as they constitute evidence of the identity of the sender, the addressee, and the date and time the message was sent.[137]

---

[129] The problem arose in the United States where the Sale of Goods Statute of Frauds requirements have not been abolished. (Uniform Commercial Code (US), s 2-201).

[130] Brown, Dr R A, 1996, The Laws of Australia, The Law Book Company Ltd, Volume 16, Chapter 16.6 Computer Produced Evidence.

[131] This aspect was discussed earlier.

[132] See Dr R A Brown, 1996, *The Laws of Australia*, The Law Book Company Ltd, Volume 16, Chapter 16.6 Computer Produced Evidence.

[133] Evidence Act 1977 (Qld), s95; Evidence Act 1929 (SA), Pt IV; Evidence Act 1958 (Vic), s 55 B. The relevant provisions in Victoria and Queensland were copied from the Civil Evidence Act 1968 (UK).)

[134] Evidence (Business Records) Interim Arrangements Act 1984 (NT), ss 1 - 22; Evidence Act 1977 (Qld), s 93; Evidence Act 1929 (SA), s 45a; Evidence Act 1910 (Tas), Pt III Divn 2B; Evidence Act 1958 (Vic), s 55.

[135] Evidence Act 1995 (Cth); Evidence Act 1995 (NSW). Under s 4(1), the Evidence Act 1995 (Cth) applies to all proceedings in a federal court or an ACT court.

[136] This is an exception to the best evidence rule.

[137] See for example, Willis, A, above.

Internet contracts made by e-mail may fall within these provisions; and

- It applies a statutory presumption as to the correct operation of devices and machines, in the context of proof of machine produced evidence. This could be used in relation to authentication devices for electronic signatures and potentially to prove contracts which are initiated by computer.[138]

Signatures

Many documents still need to be signed to be valid. The legal significance of a signature does not lie in the actual form of the signature but in the information it conveys. A human signature represents that its maker understood and adopted what has been signed. As a matter of law, a signature need only be any mark placed at any point of a document which identifies its maker.[139] The function of a signature may vary depending on the instrument upon which it is used. For example, an analogy has often been drawn between a signature on a cheque and a PIN, which acts as an authorisation to make the payment ordered and to debit the account for the amount.[140]

The new digital signatures, which are described further below, appear to satisfy the legal criteria for valid signatures under the general law,[141] even without legislative recognition.[142] However, it is more likely that the legislature in Australia will establish a specific regime governing digital signatures but as yet there has been no facilitating legislation making this possible.

The Australian Government has announced that it is planning a similar framework to the Utah Digital Signature Act 1996 in which Australia Post will be appointed as the first Certification Authority.[143]

5.4 Trading Partner Agreements and Other Solutions

In business transactions where the parties have an established or ongoing relationship trading partner agreements have been used, which amongst other things can deal with:

- the law which will apply to the contract, as well as the jurisdiction where disputes can be heard;
- the requirements for paper records of transactions;
- requirements for signatures;
- record retention;
- allocation of responsibility for network security and other failures; and
- applicable standards and protocols.

However, these types of agreements may not be capable of accommodating the Internet trading environment of the future which may not necessarily encompass established links between parties. In addition, these types of agreements may not be appropriate for consumer transactions.

For consumer transactions to be properly facilitated, in Internet commerce a concept of the 'electronic contract' is required.[144] Some progress towards this end has been made by the UNCITRAL Model Law described

---

[138] Willis, A; *Legal Issues in Electronic Commerce*, IPAA/IIR Conference Rydges Lakeside 30 May 1996.

[139] Pollard, S, 1996, *Electronic Payment Systems, The Legal Perspective*, p 9 http://www.gtlaw.com.au/gt/news/updates/elecpay.html

[140] Tyree, A, *PINs and Signatures*, http://www.law.usyd.edu.au/~alant/inchoate.html p1.

[141] Except those types of contracts which require witnesses to be enforceable, but these could also be authenticated digitally.

[142] Ibid, p 9.

[143] This is discussed further below.

already, although this Model Law is inapplicable to consumer transactions. Terms may also be incorporated in Internet transactions by the appearance of terms and conditions at the time of contracting, ie. when the consumer enters his/her details onto an Internet order form. Arguably the same terms as those traditionally contained within trading partner agreements could be incorporated this way and providing they are sufficiently brought to the notice of the consumer, they should be enforceable by analogy to the ticket cases in contract law.

5.5 Payment Mechanisms

5.5.1 Internet Money

Key Issues: *What are the various payment mechanisms which may be applicable to Internet commerce? How is liability between the parties established for unauthorised transactions or security system failures? What features are required to ensure the satisfactory operation of payment systems in Internet commerce?*

The new Internet money, or the form of money using the Internet as the main transaction mode, builds on payments instruments such as credit cards and direct debit and credit and electronic versions of cash and cheques.[145] They are accordingly an adaptation of payment mechanisms already in use independently of Internet commerce.

There is a widely held view that the Internet will be used to make transactions of relatively small denomination only, at least by consumers. The real outcome will influence the types of payment mechanisms which are developed and ultimately used for transactions via the Internet. For example, credit cards are a relatively expensive payment method to administer and are therefore unlikely to be used for small denomination transactions. It is more likely that digital coins and Smart cards will cater for this subset of transactions.

A number of payment mechanisms are being developed or adapted from existing payment mechanisms to cater for Internet commerce, including credit cards, Smart cards, digital cheques and digital cash. Satisfactory payment systems are integral to the operation of Internet commerce, and amongst other things, must be cheap to cater for smaller transactions, must be secure, and should provide a degree of privacy.

The legal nature of some of the traditional payment mechanisms will be examined because Internet payment mechanisms are largely adaptations of them. However, new payment systems designed for the Internet raise issues specific to themselves. These include how to classify them conceptually as a legal instrument, and how they interact with the laws applicable to established payment mechanisms such as cheques, credit cards and money. The Internet also changes the risk scenario so that questions arise about allocation of liability between users and providers of new payment mechanisms for security system failure, including unauthorised use or fraud. Other unresolved issues which arise include how the various laws and codes, particularly those with consumer protection charters, which govern payment systems in Australia and other countries, will apply to Internet-based payment systems which exist in an international setting.

5.5.2 Credit Cards

Legal Nature of Transactions and the Rights of the Parties

The 'third party credit card' represents a complex commercial arrangement between the card issuer, the merchant and the customer who is issued with the card.

The credit card is not a legal instrument. Instead, the credit card system is based on three contractual relationships:

---

[144] Willis, A, *Legal Issues in Electronic Commerce*; IPAA/IIR Conference, Rydges Lakeside, 30 May 1996.

[145] Singh, Dr S, *The Use of Internet Money*, http://www.arraydev.com./commerce/JIBC/9604-5.htm

- *between the issuer and the cardholder*. This authorises the cardholder to use the card. Terms and conditions of use usually include that the cardholder notify the issuer as soon as possible if the card is lost or stolen.

- *between the issuer and the merchant*. This obliges the merchant to accept the card as payment and the issuer to reimburse the merchant. The merchant is usually obliged to obtain the cardholder's signature and to compare it to the signature on the card itself, and to obtain express authority from the issuer before accepting the card for payment in excess of some agreed amount. Providing the terms of the contract are complied with, the merchant can rely on the issuer's guarantee of payment.

- *between the cardholder and the merchant for the sale of goods or services*. On the basis of this contract, the merchant accepts the card as payment.

Unauthorised Transactions

The contract between the card issuer and the cardholder will usually make the cardholder liable for all unauthorised use of the card until such time as the cardholder notifies the issuer that the card has been lost or stolen, subject to a nominated ceiling on cardholder liability. However, the conditions of use currently place a very low ceiling on the liability.

The merchant will usually only be liable for failing to take the steps outlined above, or where there has been some negligence or fraud on the merchant's part.[146]

Otherwise the bank or card issuer will bear the larger part of the risk and liability for unauthorised transactions and failure of systems security.[147] This allocation of risk is linked with security processes and the scenario may change where transactions take place over open systems such as the Internet, where the potential for fraud is probably larger.

Jurisdictional Issues

Significant jurisdictional issues should not arise in relation to credit card transactions on the Internet because the relationships between the parties are based on three separate contracts. It is generally likely that the issuing bank or card issuer will be carrying on business in the place of residence of both the cardholder and the merchant, whether or not the latter two parties are in the same jurisdiction. The merchant need only seek payment from the bank or card issuer, which is guaranteed by the latter subject to certain conditions. Banks and card issuers act as intermediaries which absorb a large part of the risks associated with jurisdictional uncertainties.

The SET Protocol

Although most payments on the Internet are presently being made simply by consumers providing credit card numbers by consumers to merchants, such a payment mechanism is clearly recognised as being inadequate for realising the full commercial potential of the Internet because:

- credit card transactions are too expensive to accommodate small denomination amounts down to a fraction of a cent, or even to a dollar; and

- credit cards are considered as being too insecure, due to the present lack of accepted authentication procedures worldwide across the Internet.

As a response to these concerns, card issuers VISA and Mastercard have developed the Secured Electronic Transaction Protocol (SET) which is designed to make credit card transactions over open systems like the

---

[146] The issuer sometimes reserves the right to debit the merchant's account in cases of forgery of a signature, counterfeit of a card or if the card is contained in a list of stolen cards.

[147] Credit cards may come within the EFT Code if they are used with a PIN. The EFT Code contains rules about the allocation of liability between parties and is discussed further below.

Internet secure. At the time of writing, liability issues under the system have not been addressed.[148] Given the estimated potential profits for card issuers and banks which could flow from Internet commerce, and on the basis of the current allocation of liability in credit card regimes for non-Internet purchases, it seems likely that card issuers and banks will need to absorb a large portion of the risk in order to make the credit card system viable for Internet commerce. This will translate into an acceptance of a responsibility for the proper operation of secure systems and/or compliance with protocols which are developed to govern it. This responsibility can be shifted to insurers and other parties by contract.

The EFT Code

Direct debit and credit mechanisms such as ATM transactions are not yet widely available in open systems such as the Internet, due to unresolved security considerations. However, the Electronic Funds Transfer (EFT) Code[149] which has been adopted at a banking industry level, provides a useful contrast to laws which apply to credit cards, and provides guidance for possible future regulation of Internet payment systems. It is also likely that Smart Cards and other Internet payment systems will ultimately be subject to special regulation.

The EFT Code[150] applies to those transactions which are initiated by an individual through an electronic terminal by the combined use of an electronic funds transfer plastic card and a personal identification number. It therefore applies most notably to EFTPOS and ATM transactions, which are currently provided over 'closed' telecommunications systems. It could also apply to credit card transactions and smart card transactions if they are initiated with a PIN.[151]

The Code governs the relationship between users and ATM providers, and provides for the establishment of dispute resolution procedures.

The EFT Code contains provisions dealing with liability for unauthorised transactions.[152] An unauthorised transaction is one which is carried out without the knowledge and/or consent of the holder of an electronic funds transfer card. The cardholder is not liable for any losses:

- which are caused by the negligent or fraudulent conduct of employees of the issuer of an EFT card, those involved in networking arrangements or of merchants who are linked to the EFT system;
- if the unauthorised transaction is effected by means of a card which is forged, faulty, expired or cancelled;
- which occur before receipt of his or her card and PIN number; or
- for any unauthorised use which occurs after the cardholder has notified the card issuer that the card has been lost or stolen or that PIN security has been breached.

In all other cases the extent of the cardholder's liability depends upon the behaviour of the cardholder. The basic rule is that the cardholder is liable for a sum which must not exceed the lesser of $50, the balance of the cardholder's account (including any pre-arranged credit facility) or the actual loss at the time of notification of the loss or theft of the card.[153]

---

[148] The basic principles of the SET Protocol are examined further below.

[149] There is no specific legislation governing electronic funds transfer.

[150] See Tyree, A, 1995, Banking Law in Australia, 2nd Ed Butterworths.

[151] See Tyree, A, *Virtual Cash III*; p 3 http://www.law.usyd.edu.au/~alant/netpay3.html

[152] The EFT Code of Practice also contains Privacy provisions which are described further below.

[153] An exception to these rules arises when the cardholder has contributed to the loss. If the contribution is by way of voluntarily disclosing the PIN, by indicating the PIN on the card or by keeping a record of the PIN with any article carried with the card or likely to be stolen at the same time as the card without any reasonable attempt to disguise it, the cardholder may be liable for a sum which does not exceed the lesser of the actual loss at the time of notification, the maximum amount which the cardholder would have been entitled to access or the balance of the account (including any prearranged credit facility). If the cardholder contributes to the loss by unreasonably delaying notification of the misuse, loss or theft of the card or if the PIN security has been compromised, the cardholder may be liable for all losses which could have been

Liability in cases of system malfunction is held by the issuer of the card for any losses caused by a failure of an EFT system to complete an otherwise valid transaction.[154]

prevented had the cardholder acted reasonably. This liability is limited to the lesser of the maximum amount which the cardholder was entitled to access over the relevant period or the balance of the account (including any prearranged credit facility).

[154] Liability in relation to failure of secure systems is dealt with more generally under Security, section 7.1 herein.

5.5.3 Negotiable Instruments

Key Issues: *What are the essential features and formal requirements of negotiable instruments? Can negotiable instruments be negotiated across international borders? What is their applicability to Internet commerce?*

Characteristics Of Negotiable Instruments

Apart from Australian notes and coins, the only three payment instruments in use in Australia which are fully negotiable are bills of exchange, promissory notes and cheques.[155]

The essence of a negotiable instrument is that the debt which is represented by the instrument should be easily, cheaply and freely transferable[156] and that the person who is entitled to the instrument for the time being, the 'holder', should be able to obtain payment of it.[157]

The following have been put forward as essential features of negotiability:[158]

- *Method of transfer*. The first characteristic is that the transfer of the rights embodied in a negotiable instrument are transferred by delivery and, in some cases, endorsement.[159] The addition of the endorsement will usually make the endorser a surety for payment as well as transferring the right to the payment.

- *Transferee to sue in own name.* The person who is entitled to the instrument, called the holder, may sue in his or her own name. This is an important exception to the common law doctrine of privity of contract, for it is not necessary to sue the person from whom the holder took the instrument. The holder may recover from any party who is liable on the instrument.[160]

- *Transfer free of equities*. Finally, the holder who takes an instrument which is in proper form, who takes for value and without any notice of defects in the transferees title, may take 'free of equities', ie, it is possible in the ordinary course of transferring rights in a negotiable instrument to pass a better title to the transferee than is held by the transferor.

---

[155] Although these are not the only financial instruments which are negotiable.

[156] Negotiable instruments were originally developed for the purposes of extending credit and obtaining payment in international sales transactions. In the form of bills of exchange and promissory notes, they now play a significant role in the mobilisation of short term capital.

[157] In order to facilitate this easy transferability, the usual rules about the transfer of property do not apply to negotiable instruments. The fundamental position is that a bona fide purchaser for value with no notice of defect of title will get good title, even if the transferor has a defective title or, in some instances, no title at all.

[158] The complete meaning of the word 'negotiable' is not always clear. There is no correct usage, but three characteristics are essential.

[159] Endorsement signifies the writing on the instrument, usually on the back, of the name of the person who is transferor The process of transfer by endorsement and delivery is called 'negotiation'.

[160] >From this follows one of the most significant differences between debts and negotiable instruments. The assignee of a debt must sue for breach of contract if the debt is not paid. All of the usual defences may be raised by the defendant. By contrast, the holder of a bill of exchange, for example, must only plead that he or she is a holder and that the signature of the defendant is on the bill in a position which makes the defendant liable. The plaintiff is then entitled to summary judgment for the face value of the instrument unless the defendant can obtain the leave of the court to defend. This will not be granted lightly, for the rule is that negotiable instruments are to be treated as cash unless there are exceptional circumstances. As one court has said: '[the] rule of practice is thus, in effect, pay up on the bill of exchange first and pursue claims later': *Ceborah SNC v SIP (Industrial Products) Ltd,* 1976, 1 Lloyds Rep 271 at 276.

Particular rules apply as to whether a negotiable instrument can be negotiated in Australia.[161] Australian law determines whether an instrument can be negotiated in Australia.[162] A foreign instrument is negotiable in Australia if it falls within the definition of 'bill of exchange'[163] or 'promissory note'[164] and is negotiable under the law of the place of issue.[165] Cheques are governed by separate legislation.

Cheques

In Australia, cheque law is governed by Federal legislation; the *Cheques and Payments Orders Act* 1986. A cheque is a type of negotiable instrument drawn on a banker and payable on demand. Since a cheque is payable on demand it need not be presented to the drawee bank for acceptance. A cheque operates as a mandate or order to the drawee bank to pay and debit the account of its customer, the drawer.

A cheque must be in writing signed by the drawer. At present, the Cheques and Payments Orders Act does not recognise electronic cheques.

As with other types of negotiable instruments, particular rules apply to whether a foreign cheque can be negotiated in Australia. Provided the instrument is a cheque under the law of the place where it was issued[166] a foreign cheque will be negotiable in Australia whatever restriction may exist under the law of the place of issue[167].

Bills of Exchange

The Bills of Exchange Act 1909 (BEA) s 8(1) provides that:

> a bill of exchange is an unconditional order in writing, addressed by one person to another, signed by the person giving it, requiring the person to whom it is addressed to pay on demand, or at a fixed or determinable future time, a sum certain in money to or to the order of a specified person, or to bearer.

---

[161] At an international level, bills of exchange and promissory notes (not cheques) are governed by the 1988 (New York) UN Convention on international bills of exchange and international promissory notes, but Australia has not adopted the Convention.

[162] *Rosenhain v Commonwealth Bank of Australia,* 1922, 31 CLR 46

[163] Bills of Exchange Act 1909 (Cth) s 8.

[164] ibid s 89.

[165] *Guaranty Trust Co of New York v Hannay & Co* [1918] 1 KB 43 at 55-62 per Bailhache J.

[166] Cheques and Payment Orders Act 1986 s 117(3).

[167] ibid s 39(1).

This definition is very similar to a cheque but the bill need not be drawn on a banker, need not be payable on demand, and the money must be payable to or to the order of a specified person or to bearer. It is common for bills and notes to be drawn payable at some future time. The primary purpose is to provide a secure legal mechanism for an extended period of credit.

A bill of exchange must be in writing signed by the person giving it. The BEA does not currently recognise electronic bills of exchange.

Promissory Notes

The law relating to promissory notes is also governed by the BEA. While the definition of a bill of exchange requires at least two parties, the drawer and the drawee, the promissory note requires only one. The BEA s 89(1) states:

> A promissory note is an unconditional promise in writing made by one person to another, signed by the maker, engaging to pay, on demand or at a fixed or determinable future time, a sum certain in money, to or to the order of a specified person or to bearer.

A promissory note must be in writing signed by the person making it. The BEA does not currently recognise electronic promissory notes.

5.5.4 Emerging Payment Systems

Key Issues: *What are the emerging types of payment systems, such as Smart Cards, digital cash and digital cheques? How will they be applied to Internet commerce? Can they be accommodated by existing laws? What are the risks with each type of new payment system and who bears it? How would the general law of (say) cheques or money apply to a digital cheque or digital money? How do these new payment systems 'fit in' with current laws, ie. how do we identify each payment mechanism legally? What problems arise when the transaction assumes an international dimension?*

Smart Cards

A 'Smart Card'[168] is shaped like a conventional credit card but with an embedded computer chip that can receive, process, store and transmit information.[169] Amongst other things, the card can be used to store money, or a value of money, including digital coins; the Stored Value Card or SVC.[170] These types of cards have been referred to as "electronic purses". SVCs are designed to replace currency, which is currently used for 90 percent of consumer transactions, including groceries, bus fares, and small denomination items.

The magnetic stripe technology currently used on credit and debit plastic cards is suitable for high cost purchases and would be too expensive for smaller transactions because it requires a system to be continually 'on-line' for instruction, recording and messaging. On the other hand, SVCs do not require verification by signature or PIN, and can therefore be used to replace low denomination currency. SVCs can not only be designed to be disposable once the value of the card has been used, but also can be reloadable either through an ATM or via the Internet from or to a bank account.[171]

---

[168] Tyree, A, *Computer Money - Legal Considerations*, http://www.law.usyd.edu.au/~alaut/newcast/html

[169] Centre for Electronic Commerce, Report to Australian Commission for the Future, *Smart Cards and the Future of Your Money,* p2; http://acff.com.au/smartcard.html

[170] Examples of SVCs currently in use include the phonecard, photocopy cards and bus/tram/rail cards.

[171] Centre for Electronic Commerce, Australian Commission for the Future, *Smart Cards and the Future of Your Money,* p2; http://acff.com.au/smartcard.html

The legal nature of a smart card requires some clarification. As a facilitating device or data storage mechanism, Smart cards do not really warrant classification as a legal instrument as such. They are more likely to be governed by an EFT code type of regime.[172]

Digital Cash[173]

A 'digital coin' or digital cash consists of a message issued by a bank or other entity and encrypted[174] by its private key.[175] The message contains the serial number of the cash, the identity of the issuer and its Internet address, the amount of the cash and an expiry date. Because the message is encoded with the bank's secret key it may only be read by using the bank's public key. It cannot be altered without destroying its message content.

When a customer wishes to be issued with cash the customer sends a request to the bank. The request must be encoded with the customer's private key. The bank may then decode the message with the customer's public key and have confidence that the request is what it appears to be and that it originated with the customer.

The cash is 'issued' to a particular customer by encoding the cash with the customer's public key. This message is then sent to the customer who decodes it using his or her private key. Even if the message is intercepted it would be worthless since only the customer to whom the cash issued can read the message. The cash thus received are stored on the customer's private electronic memory system, be it a PC or a Smart Card.

A customer may send the cash to a merchant via the Internet. The cash would probably be encrypted with the merchant's public key to prevent interception. The merchant decodes its private key and then does two things with the received message. Firstly, the message is decoded using the bank's public key to verify it is cash for the appropriate amount of the payment. Secondly, the merchant must ascertain that the cash has not already been spent. This is done by asking the bank to verify that the serial number of the cash is still current. The bank then credits the merchant's account and cancels the serial number so that the cash may not be spent again.

The relatively recent development of the concept of digital coins or cash means that there is little or no legal guidance about who bears the risk for unauthorised or fraudulent interception or use of it. In the absence of legislative intervention or the development of codes of practice, the liability is likely to be established under contractual arrangements between the parties. However, this may not be adequate in a system which allows the free exchange of digital coins. In that case it will be necessary to determine the legal nature of a digital coin, because the relationships may not necessarily be determined by an express contract.[176] For the payment mechanism to be effective in Internet transactions which take place internationally, there must also be international standards and recognition.

Electronic Cheques

The digital cheque[177] is a message which contains all of the ordinary information appearing on a paper cheque and which is then 'signed digitally', that is, it is encoded by encrypting with the 'drawer's' secret key. It is then sent to the 'payee'. The 'payee' may further 'endorse' the instrument by encoding the already encoded message with his or her private key. A complete 'chain' of signatures may be built up so that none of the 'endorsers' may deny that it is their endorsement.

---

[172] Clarke, R, *Smart Move by the Smart Card Industry*, http://www.anu.edu.au/people/Roger.Clarke/DV.SMSC.html

[173] Tyree, A, Virtual Cash Payments on the Internet, p 3 *http://www/law.usyd.edu.au/~alaut/netpay.html*

[174] Encryption is discussed further below under security.

[175] Tyree, A L; *Virtual Cash; Payments on the Internet*; p 3; http://www.law.usyd.edu.au/~alant/netpay.html

[176] Tyree, A, *Virtual Cash?*

[177] Tyree, A, *Computer Money - Legal Considerations* http://www.law.usyd.edu.au/~alaut/newcastle.html See also other papers listed at Alan Tyree's Web site.

When the instrument is paid by the 'drawee' it is so marked and the resulting message is encoded with the bank's secret key thus providing proof of payment. In order to avoid duplication, each 'cheque' must have a unique serial number.

In the absence of recognition of digital cheques by the applicable legislation (see above) the liability of the various parties for unauthorised use or fraud is unclear. The question remains as to whether a digital cheque should be governed by laws relating to existing paper cheques or whether it should be treated as a new or distinct legal instrument or as a contract.

Regulation of New Payment Systems

Internet payment mechanisms including smart cards, digital coins, cheques and signatures are likely in the future to be governed by a variation of the EFT Code of Conduct. They may also be subject to legislation supported by international treaties. In addition, standards and protocols are being developed, which not only deal with security aspects of new payment systems but also have a bearing on liability issues in some circumstances.

5.5.5 Other Payment Mechanisms

Given the nascent development of payment mechanisms for use in Internet commerce, one can only speculate about potential new or existing payment mechanisms which could be applied. One example could be a form of letter of credit.

Letters of Credit[178]

Letters of credit are a conventional payment mechanism used in international trade and will be suitable for business, rather than consumer transactions. A contract for the sale of goods between two parties in different countries will usually be found to have a stipulation that payment of the price is to be by this method. Letters of Credit are one of the principal means used by traders to deal with jurisdictional uncertainties, effectively by passing the risk on to the bank which acts as a payment intermediary.

A letter of credit is a promise by a bank acting on behalf of the buyer of the goods, that it will honour the drafts, drawn by the seller for the price of the goods, provided that stipulations appearing on the face of the instrument are met, such as the handing over of the documents of title (eg the bill of lading, insurance policy and invoice) and other specified documents. On the application of the buyer, the letter of credit is issued by the bank to the seller.

Letters of credit are governed by general law and usually expressed to be subject to the Uniform Customs and Practice for Documentary Credits (1993 Revision) International Chamber of Commerce Brochure No 500 (UCP).

It is uncertain whether the general law could allow for recognition of electronic letters of credit. However, some moves towards recognition of electronic documents in international trade has been made in moves to provide for electronic bills of lading.[179] Whether these documents could be used via the Internet is unknown.

[178] Sutton, K, 1995, *Sales and Consumer Law* 4th Ed, LBC Information Services, Chapter 26.

[179] See Faber, D, 1996, Electronic Bills of Lading, *Lloyds Maritime and Commercial Law Quarterly*, 232.

6. Consumer Protection

Sale of goods, consumer protection, consumer credit and advertising laws in Australia are governed by a variety of Federal, State and Territory laws and industry codes aimed at protecting the consumer from unfair practices by merchants and advertisers, and to provide rights in respect of goods, services and credit provided to consumers. Internet commerce raises issues about the application of these laws to the medium and to the various parties operating in the medium. It also raises issues about the reach of these laws to parties outside Australia, as well as the reach of counterpart overseas laws to parties situated in Australia.

6.1 Advertising

Key Issues: *What are essential components of the various rules governing advertising in Australia, do they have extra-jurisdictional application and do they apply to the Internet? How will the Internet affect the way advertising laws are enforced in Australia?*

Advertising in Australia is governed by a number of Federal, State and Territory Acts and industry Codes. The Trade Practices Act 1974 (Cth) (TPA) applies to corporations and traders involved in international or interstate business activities, and covers all television advertising. At a State level, the Fair Trading Acts contain mirror provisions to those contained in the Trade Practices Act and operate alongside the Federal Act. The following overview relates to provisions contained in the Federal legislation but the considerations are similar in relation to State legislation.

Laws Governing Advertising in Australia[180]

Advertising is regulated under the TPA by provisions contained in Part V of the Act. The rules fall into two categories.

Firstly, section 52 prohibits conduct which is misleading or deceptive. In determining whether conduct is misleading or deceptive, the court will consider the particular audience the advertisement is aimed at, including its levels of sophistication and understanding. Section 52 has been given an extremely broad application by the Courts. There is no concept of 'contributory negligence' under section 52; it is an 'all or nothing' prohibition.

In the context of advertising, section 52 prohibits:

- advertisements which, either directly or indirectly or by implication, make claims of a factual nature which are demonstrably untrue;
- businesses from benefiting from a competitor's reputation by adopting similar advertising slogans, images or themes when this would mislead the public into believing the advertisers product was somehow connected with the competitor; and
- favourably comparing a product with a well know rival, by claiming scientific objectivity through test results and surveys, or by endorsements and testimonials from experts and celebrities, if claims are made or suggested which cannot be substantiated. Breach of this provision can result in civil penalties only.

Other provisions contained in Part V of the Act have more specific application and carry criminal as well as civil penalties. The prohibitions contained in these provisions can be summarised as follows:

- false representations in the supply or promotion of goods or services (s 53);
- false or misleading representations in the promotion of land transactions (s 53A);

---

[180] Goldring, M & McKeogh, 1993, *Consumer Protection Law* 4th Ed, Federation Press.

- misleading conduct in the promotion of employment opportunities (s 53B);
- failing to state the full cash price where a promotion includes a statement of an amount to be paid, such as a deposit (s 53C);
- conduct liable to mislead the public about the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity of goods (s 55);
- conduct liable to mislead the public about the nature, the characteristics, the suitability for their purpose or the quantity of services (s 55A);
- misleading statements about home operated businesses (s 59(1));
- misleading statements about investment activities (s 59(2));
- bait advertising (s 56);
- offering gifts or prizes with no intention of providing them (s 54);
- inertia selling (s 64);
- referral selling (s 57); and
- pyramid selling (s 61).

Defences

The Act contains a number of defences to breaches of Part V of the Act. Section 85(1) provides defences to prosecutions for criminal offences under Part V the Act.

Under s 85(1)(a) and (b) an advertiser will not be convicted of an offence if it can show that the contravention was the result of a reasonable mistake, or a reasonable reliance on information supplied by another person.

It is a defence under section 85(1)(c) to show that, despite exercising reasonable precautions and due diligence, a contravention arose because of the act or default of another person, an accident or some other cause beyond the control of the advertiser.

Section 85(3) provides a special defence for broadcasters and publishers to actions for breaching Part V including actions under s 52. The defence is available only to people 'whose business it is to publish or arrange for the publication of advertisements'. It applies if the advertisement has been received for publication in the ordinary course of business, and the publisher does not know or suspect that the publication would amount to a contravention of the Act. Although the defence is available to broadcasters, it is probably not available to advertising agencies, or by analogy to Internet content creators.

Most of these defences should, depending on the circumstances, be available to Internet service providers.[181] However, if the ISP assists in the design of the Web site which includes infringing material, the defences may not be open to them.

Self Regulation of Advertising

A system of advertising self-regulation has been developed by media organisations, advertisers and advertising agencies, consisting of a number of self-regulatory codes which are subject to authorisation by the Australian Competition and Consumer Commission (ACCC). The codes are designed to prevent misleading or offensive advertising, and to reflect community expectations and standards.

The system is administered by the Media Council, which represents nearly all proprietors of commercial media, and compliance with the codes is enforced by the accreditation of complying advertising agencies. The Media

[181] As to the liability of a person as a party to the contravention, see further below under consumer protection.

Council administers and enforces a general advertising code[182] and four more specific codes.[183] The Codes apply to all advertisements submitted for publication or broadcast by members and associates of the Media Council. Each arm of the media has a body to which advertisements are submitted for authorisation before they are broadcast or published.

Internet Advertising and Enforcement

There are currently no specific legislation or industry codes applicable to Internet advertising in Australia. The existing voluntary industry codes will govern bodies only if they presently fall within the jurisdiction of the Media Council, which is largely limited to the proprietors of commercial media. Advertising self regulation also relies on the submission by accredited advertising agencies of material for vetting by a representative body from each arm of the media. The same quality control cannot be enforced for Internet advertising unless a similar representative body can be brought into existence. Neither it seems will the voluntary industry Codes apply to extra-jurisdictional advertisers, unless they fall within the jurisdiction of the Media Council. This would probably require their voluntary submission.

However, Australian companies, Internet advertisers, content service providers and content creators, will always be subject to the Australian State and Federal legislation which applies to advertising. Whether any or all of these parties can avail themselves of defences within the legislation is another matter. However, Australian laws may not be able to control what material is accessed from outside its borders. The extent of the application of Australian laws to overseas Internet advertisers and other parties, is yet to be established.

Further issues arise in relation to enforcement. In the physical world, enforcement is possible because the identity of the maker of an advertisement or representation may be readily established. This is not the case with the Internet, where the identity of the party may not be known or traceable. The ease of creation and removal of Web sites also creates problems of proof.

The use of 'hyperlinks' creates a further subset of problems relating to liability under advertising laws. Controllers of hyperlinks on Web sites may be exposed to liability under advertising laws if they cannot bring themselves within the purview of defences outlined above. This is best illustrated by an example of a shopping mall Web site of a major retailer contains hyperlinks to sub-boutiques of various brand names. If the Web sites of sub-boutiques contain material which breaches advertising laws in Australia, can the major retailer or the retailer's ISP also be liable? What if the sub-boutique Web site has been hyperlinked from another jurisdiction where the material is not in breach of the laws, but breaches Australian law, or vice versa? In this situation, there will be a number of parties, including ISPs which are exposed to potential liability. Even without legislative intervention, the general law has not come close to solving any of these issues.

6.2 Sale of Goods and Consumer Protection Laws

Key Issues: *What are the essential features of the laws relating to sale of goods and consumer protection in Australia? What are the formal requirements of contracts coming within the terms of the laws? Can sale of goods contracts be made electronically? When are the laws likely to govern a transaction with international dimensions? When is the sale of goods legislation likely to govern an international transaction made over the Internet? In what circumstances will Australian consumer protection laws apply to Internet transactions with an international context?*

There is a three-tier system governing contracts for the supply of goods and services in Australia. These are:

- Uniform sale of goods legislation (SGA), of which the provisions may be contracted out;

---

[182] The advertising code of ethics, a general code which sets standards for all media advertising.

[183] The Therapeutic Goods Advertising Code, the Slimming Advertising Code, the Cigarette Advertising Code and the Alcoholic Beverages Advertising Code.

- Consumer protection provisions of the TPA, applicable to transactions involving the supply of goods or services by a corporation to a consumer; which cannot be contracted out and which take precedence over state legislation; and

- State legislation applicable to consumer transactions which do not fall within the ambit of the TPA. The State legislation either amends the SGA in respect of transactions within its ambit or implies conditions as to title and quality which differ from those contained in the SGA and which are similar to but not always identical to the corresponding provisions of the TPA. These provisions cannot normally be contracted out. There is also State legislation which governs particular types of transactions, such as credit transactions, commercial sale of second-hand motor vehicles, door-to-door sales, lay-by sales, residential tenancy agreements and others.

Sale of Goods Laws[184]

The law governing the sale of goods in Australia and New Zealand is based on the English Sale of Goods Act of 1893.[185] The States have enacted legislation substantially identical with the English Act. Consequently there is a high degree of uniformity between English law, New Zealand law and the laws of the Australian States, although some differences do exist. In addition, legislation which has a bearing on certain types of sales transactions has been passed in some jurisdictions.

Application of Sale of Goods Legislation

Except where the Sale of Goods Act expressly provides, the general principles of the law of contract will govern the sale of goods.

For the Sale of Goods Act to apply there must be a contract of sale,[186] the sale must be one of goods,[187] property must pass therein and there must be a money consideration.[188]

Of particular interest in sale of goods laws are certain terms which in the absence of a contrary intention, are deemed to be implied in every contract for the sale of goods. Thus, there are implied conditions of a right to sell the goods, that the goods correspond with the description, that they are of merchantable quality, that they will be reasonably fit for the purpose for which they are bought, and in the case of a sale by sample, that the bulk corresponds with the sample and with the description, that there will be a reasonable opportunity of examination. These provisions may be 'contracted out' or expressly excluded by the parties to a contract.

Formal Requirements of Sale of Goods Contracts

The requirement of writing for sale of goods contracts has been abolished in some jurisdictions. For example, the Victorian legislation, the Goods Act 1958, states in section 8 that 'a contract of sale may be made in writing or by word of mouth or partly in writing and partly by word of mouth or may be implied by the conduct of the parties'.

Although the legislation does not specifically provide for electronic documents, there is no need for the contract to be in writing, which may obviate evidentiary difficulties surrounding proof of electronic documents. It also

---

[184] *Halsbury's Laws of Australia,,* 1995, Vol 23, Title 375 Sale of Goods

[185] In the UK, Sale of Goods transactions are governed by the (UK) Sale of Goods Act 1979. As previously stated, because the laws of England and Australia are based on the same original Act relating to the sale of goods there is a great deal of uniformity between the laws. In the United States, sale of goods is governed by the Uniform Commercial Code, first promulgated in 1962, which has superseded the Uniform Sales Act in American jurisdictions. The Code still contains requirements that sale of goods contracts be in writing.

[186] A contract of sale is defined in section 5(1) as including an agreement to sell in the future as well as a sale.

[187] The term 'goods' is defined in section 5(1) as including all chattels personal other than things in action and money, and also industrial crops, and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale.

[188] The Sale of Goods Acts in Australia apply primarily to the sale of goods on land.

suggests the legislation may apply to transactions taking place over the Internet providing the transactions otherwise come within the terms of the legislation.[189]

Geographical Reach of Sale Of Goods Legislation

The sale of goods legislation will largely govern transactions which take place within the jurisdiction of each State. Some sale of goods legislation purports to have extra-territorial effect by linking at least part of the transaction to the State, for example, the Goods Act 1958 (Vic) states[190] that Part IV applies to certain sale and leases which are to be delivered or supplied in Victoria. This provision gives the legislation potential application to overseas merchants subject to jurisdictional constraints outlined in 4.1 and 4.3.

Liability Under Sale of Goods Legislation

Sale of goods legislation applies to a contract between defined parties, and it is unlikely that third parties not subject to the contract will be otherwise subject to the legislation. The legislation does not apply to credit providers.

Consumer Protection Laws[191]

The Trade Practices Act 1974 (Cth)

The Federal consumer protection provisions are contained in Part V of the TPA. There are four divisions together with the provisions contained in the new Part VA:

- Division 1 deals with misleading statements and unfair practices by a corporation in trade or commerce in connection with the supply of goods or services. This area was discussed above under advertising;
- Division 1A deals with product safety and product information;
- Division 2 implies certain terms in a contract for the supply of goods or services by a corporation to a consumer. These provisions are similar to the conditions and warranties relating to title, quiet possession, correspondence with description and with sample, merchantable quality and fitness for the particular purpose implied in the SGA. However, the seller is prevented from contracting out of the provisions under the TPA. The TPA also contains provisions which set out warranties to be implied into every contract by a corporation in the course of business for the supply of services. These are (i) that the services will be rendered with due care and skill and that any materials supplied in connection therewith will be reasonably fit for the purpose; and (ii) that where the particular purpose for which the services are required or the result sought is made known, the services and materials supplied will be reasonably fit for that purpose or are of such a nature and quality that they might reasonably be expected to achieve that result.
- Division 2A deals with the liability of manufacturers where no direct relationship applies between the supplier corporation and the consumer ('product liability'). It creates in certain circumstances a statutory liability on the part of the manufacturer (or importer) of goods to the ultimate purchaser or 'end user' of the goods for loss through defects. The Division does not apply to services. There must be no direct contractual relationship between manufacturer and 'end user' or consumer for the Division to apply. Otherwise, Div 2 of Part V will apply.
- Part VA of the TPA places strict liability on the part of a corporate manufacturer who supplies defective goods. It allows a person who is injured or who suffers loss or damage through a defective product to obtain compensation from the manufacturer without the need to establish negligence on the latter's part or the existence of a contractual relationship. An importer of goods will be deemed to be a manufacturer if the actual manufacturer has no place of business in Australia, and the same is true of a corporation which holds itself out as the manufacturer through branding or otherwise.

---

[189] Small denomination transactions may not come within the terms of the legislation if they fall below a threshold value prescribed in some of the Acts.

[190] In section 117.

[191] *Halsbury's Laws of Australia,* Butterworths Australia, Vol 5, The Annotated Trade Practices Act 17th Ed, 1996, LBC Ltd (RV Miller).

Liability For Contraventions

Although the TPA applies primarily to corporations, it has some applications to the conduct of individuals. In particular, a number of sections of the TPA apply to conduct by non-corporates in trade or commerce between Australia and places outside Australia[192] and to conduct involving the use of 'postal, telegraphic, telephonic and like services'.[193] The latter provision relies on the words of placitum (v) of the Commonwealth Constitution which have formed the basis of federal regulation of broadcasting and telecommunications in Australia. Accordingly it is strongly arguable that Internet commercial transactions which involve an Australian end are within the scope of the TPA.

It will also apply to persons involved in the contravention of the legislation by a Corporation. Section 75B of the Trade Practices Act (Cth) sets out the situations in which a person can be involved in the contravention of a provision of Parts IV, IVA and V sufficiently to render that person liable for the contravention.[194] The orders which a court may make against any person coming within the provision are set out in section 76(1).

Under section 75B, a reference to a person involved in a contravention is a reference to a person who:

- has aided, abetted, counselled or procured the contravention;
- has induced, whether by threats or promises or otherwise, the contravention;
- has been in any way, directly or indirectly, knowingly concerned in or party to, the contravention; or
- has conspired with others to effect the contravention.

A person is required to have knowledge of the essential facts of the offence to bring themselves within the description of a person involved in a contravention. The provision has potential application to ISPs, their representatives and other parties taking part in Internet commerce but the full implications of the provision can only be the subject of speculation.

Territorial Reach of The TPA

Section 5(1) of the TPA confers limited extra-territorial operation by applying the Act to conduct outside Australia. Territorial nexus is provided by the requirement that the party engaging in the conduct must be an Australian citizen, a person ordinarily resident in Australia, an Australian incorporated entity or a body corporate carrying on business in Australia. Operative effect can be given to s 5 if it is interpreted as applying to conduct engaged in outside Australia which may reduce competition or mislead consumers in Australia.[195] It may also apply to the conduct of Australian corporations or individuals which take place outside Australia.

When private proceedings are instituted under the Act for damages under s 82 or remedial orders under s 87 and the conduct in question is engaged in outside Australia, the applicant is required to obtain the consent of the Attorney-General before the extra-territorial conduct complained of can be relied on at a hearing. The Attorney-General must give consent unless he or she considers that the conduct is required or specifically authorised by the law of the country where the conduct is engaged in or that it is not in the national interest to give consent.

In the context of Internet commerce, the TPA will apply, on the basis of section 5, to conduct which takes place on the Internet by Australian citizens, persons ordinarily resident in Australia, Australian corporations and corporations carrying out business in Australia. It will apply if the conduct is engaged in within or outside Australia. It is not known whether ISPs or merchants operating Web sites from outside Australia could come within these terms, and problems relating to enforceability may nonetheless arise. However, on the basis of section 51 (v) of the Constitution it is likely that the TPA will apply in many situations where there is an Australian end to the transaction.

---

[192] see TPA s6 (2)(c) and (h).

[193] see TPA s6(3)(a).

[194] Thus this provision will also apply to the advertising provisions outlined above.

[195] *Wells v John R Lewis (International) Pty Ltd*, 1975, 25 FLR 194 at 208.

State Consumer Protection Laws

Legislation dealing with the supply of goods and services to consumers has been enacted by States and Territories and operates alongside the TPA and SGA provisions. These provisions are similar but not always identical to the corresponding TPA provisions. In contrast to the TPA, the provisions of State legislation are not limited to corporations. They apply to 'persons' generally.

Legislation in some States and Territories also imposes liability on manufacturers for defective goods, which will apply alongside the TPA provisions and in situations beyond the reach of the Federal legislation.

Territorial Reach Of State Consumer Protection Laws

Most of the State legislation purports to have extra-territorial application. The Queensland statute is expressed to apply to every person who does an act or makes an omission in Queensland that constitutes a contravention of the legislation. It is further provided that where acts or omissions occur that would constitute a contravention of the legislation if they all occurred in Queensland, and any of the acts or omissions occurs in Queensland, the person who does the act or makes the omission is to be taken to have committed the contravention.

In Tasmania, it is provided that the legislation applies to and in relation to transactions that take place, conduct that occurs, and representations that are made within the State whether wholly or partly.

In the Victorian legislation it is provided that, except where otherwise expressly stated, the legislation applies to and in respect of an acquisition or supply of goods or services, or a proposed acquisition or supply, if:

a) the supplier or the customer signs a document in Victoria relating to the transaction; or

b) the goods or services are to be delivered or supplied in Victoria.

It is further provided that the 'Act extends to the engaging in conduct outside Victoria by bodies corporate incorporated or carrying on business within Victoria or by persons ordinarily resident within Victoria.

There are similar provisions in the Western Australian statute, except that it also refers to the disposal of interests in land. Enforceability of these laws are, however, subject to the same problems as other legislation.

Consumer Protection Laws and Internet Transactions

At a local level, problems of enforcement of consumer protection laws in respect of distance selling and Internet transactions appears to be being dealt with, at least initially, by proposals for industry Codes of Conduct. However, these are not likely to apply to international transactions where the seller is not based in Australia or party to the Code.

On 17 January 1997 the Ministerial Council on Consumer Affairs (MCCA) released a draft Distance Selling Code of Practice and discussion paper for public comment. The draft Code is designed to establish minimum standards of behaviour for distance sellers. 'Distance selling', where consumers buy goods and services without visiting a trading premises or meeting the seller, includes mail order, telemarketing, 'infomercials' and television as well as Internet advertisements.

It is proposed to implement the Code as a voluntary industry code aiming to:

- ensure that rights of privacy (and disclosure) are protected;
- improve the market for consumers and sellers;
- discourage fraudulent and unacceptable conduct;
- ensure that fair trading practices are followed; and
- ensure that there are adequate redress mechanisms applying to distance selling.

Other Legislation

As previously mentioned, there is other legislation at State level which governs specific types of consumer transactions, such as consumer credit and door-to-door sales, and which may have a bearing in the area of

Internet commerce. It is not proposed to review all the legislation in detail but it ought to be mentioned that legislation such as the door to door sales legislation in some States may catch certain Internet transactions.

6.3 Consumer Credit[196]

Key Issues: *What are the essential features of consumer credit laws? What are the formal requirements of credit contracts, and can they be formed electronically? Does the Consumer Credit Code apply to liability for unauthorised transactions? What is the territorial reach of Australian consumer credit legislation? When will these laws apply to Internet transactions involving an international dimension?*

A uniform scheme of consumer credit laws[197] for the regulation of consumer credit has been enacted in all Australian States and Territories.[198]

The Code applies to all credit provided for a personal, domestic or household purpose, regardless of the amount to be provided. It applies to all types of contracts, including closed-end accounts, credit cards and bank overdrafts, and its provisions cannot be contracted out. The Codes may also apply to credit contracts which are linked to sales transactions.

The legislation sets out the requirements for credit contracts, including pre-contractual disclosures, the fact that credit contracts must be in writing and that they must contain certain key material designed to ensure that 'truth in lending' is given effect to. The overriding objective of 'truth in lending' is for disclosure of prescribed information and key disclosures are set out in Cl 15 of the Code, dealing with issues such as the annual percentage rate of rates, the amount and number of repayments, the calculation and total amount of interest charges, credit fees and charges, default rates, enforcement expenses, commissions, insurance financed by the contract and other information.

Application of the Code

Under s 6, the Code is stated to apply to the provision of credit (and to the credit contract and related matters) if when the credit contract is entered into or (in the case of pre-contractual obligations) is proposed to be entered into:

a) the debtor is a natural person ordinarily resident in the jurisdiction or a strata corporation formed in the jurisdiction;

b) the credit is provided or intended to be provided wholly or predominantly for personal, domestic or household purposes; and

c) a charge is or may be made for providing the credit; and

d) the credit provider provides the credit in the course of a business of providing credit or as part of or incidentally to any other business of the credit provider[199].

The Code is presumed to apply to a credit contract unless the contrary is shown[200].

---

[196] Elizabeth Lanyon et al. (eds), 1994, *Australian Consumer Credit Law Guide*, Butterworths Australia

[197] The template legislation, the Consumer Credit (Queensland) Act, 1994, received Royal Assent on 14 September 1994, but was not proclaimed to commence until 1 November 1996. The Consumer Credit Code is contained in the Appendix to that Act.

[198] In the United States, consumer credit is governed by the Consumer Credit Protection Act of 1968. This legislation is similar to the Australian legislation in that it is based on certain required disclosures.

[199] For the purposes of the Code, credit is provided if under a contract (a) payment of a debt owed by one person (the debtor) to another (the credit provider) is deferred; or (b) one person (the debtor) incurs a deferred debt to another (the credit provider): s4.

The Code also apples to certain mortgages and guarantees which secure obligations under a credit contract,[201] to goods leases with options to purchase which are regarded as sales by instalment,[202] to consumer leases,[203] related sales contracts[204] and related insurance contracts[205]. In the case of related sales contracts, liability is imposed in certain circumstances on the credit provider for the actions of the supplier of goods and services[206].

Section 7 sets out the provision of credit to which the Code does not apply. It does not apply to:

- short term credit for a total period not exceeding 62 days (s 7(1));
- credit without prior agreement between the credit provider and the debtor. For example, when a cheque account becomes overdrawn and there is no agreed overdraft facility (s 7(2));
- credit for which only a fixed or periodic account charge is payable which does not vary according to the amount of credit provided. (s 7(3)). However, the Code applies if the charge exceeds the maximum charge prescribed by the regulations, currently set at $200 for the first 12 months and $125 for each subsequent 12 month period;
- joint credit and debit facilities, where the contract or any amount payable or other matter arising out of it relates only to the debit facility (s 7(4));
- bill facilities (7(5))
- insurance premiums by instalments (s 7(6));
- pawnbrokers (s 7 (7));
- trustees of estates (7 (8));
- employee loans (s 7(9));
- specific classes of credit exclude by the regulations.

The Regulations set out additional exempt credit under the Code. The Code does not apply to the provision of credit under a contract (other than a continuing credit contract) if:

a) the amount of credit does not at any time exceed $200; and

b) there is no insurance financed under the contract; and

c) there is no mortgage or guarantee taken by the credit provider; and

d) the annual percentage rate for the contract does not exceed the maximum annual percentage rate (if any) for the contract if it were a contract to which the Code applies.

Continuing Credit Contracts

Unlike the previous regime of Credit Acts, both credit card contracts and overdraft facilities are included within the definition of 'continuing credit contract' which in Schedule 1 of the Code is defined to mean:

> 'A credit contract under which:
>
> a) multiple advances of credit are contemplated; and

---

[200] s 11.

[201] ss8,9.

[202] s 10.

[203] Part 10.

[204] Part 7. Related sales contracts are linked to credit contracts which fare established to finance them.

[205] Which includes insurance over mortgaged property and consumer credit insurance.

[206] See Part 7 of the Code and the following for a detailed discussion: Elizabeth Lanyon et al. (eds), 1994, *Australian Consumer Credit Law Guide*, Butterworths Australia.

b) the amount of available credit ordinarily increases as the amount of credit is reduced...'

It is likely that with the development of computer and communications technology, the flexibility provided by continuing credit contracts will become even more attractive to credit providers because of the simplicity of payment mechanisms which can be developed for them.

Consequences of non-compliance with the Code

Consequences of non-compliance with the Code include the following:

- fines and civil penalties;
- compensation to any person suffering loss;
- contracts rendered unenforceable or void;
- jeopardy to ability to continue business in jurisdictions which introduce licensing or registration regimes; and
- personal liability of directors, officers and advisers.

Enforcement Issues

The States and Territories are dealing with the following matters separately, which under the 1993 inter-governmental agreement are not required to be uniform:

a) regulation of credit providers, be it positive, in the form of licensing as applies in NSW, Victoria, ACT, and WA, or negative, in the form of automatic registration of credit providers subject to deregistration, as applies in Queensland;

b) the establishment, jurisdiction and functions of the Government Consumer Agency; and

c) designation of the court or tribunal having jurisdiction to entertain matters arising out of the Code.

Formal Requirements Of Credit Contracts

Section 13 permits the regulations to authorise other means of forming a credit contract that do not involve a written document. Presumably this provision is intended to allow for the electronic formation of contracts, despite the current law requirement for contracts to be in writing.

Liability For Unauthorised Transactions

Matters relating to liability for unauthorised use of the credit contract for example by reason of loss or theft of the 'card' or other means of access to the account are not covered by the Code itself. These matters are covered by contractual arrangement, common law and Codes of Practice.[207]

Territorial Reach Of Australian Consumer Credit Legislation

The Code applies[208] to the provision of credit (and to the credit contract and related matters) if when the credit contract is entered into the debtor is a natural person ordinarily resident in the jurisdiction or a strata corporation formed in the jurisdiction. The Code also has a continuing or extended jurisdiction in certain situations. These are (a) that if the Code applies to the provision of credit or the contract it will apply in relation to all transactions or acts under the contract whether or not they take place in this jurisdiction; and (b) the Code will continue to apply even though the debtor ceases to be ordinarily resident in the jurisdiction.

There are also provisions dealing with the situation where there are more than one debtor in different jurisdictions. If not all the debtors under a credit contract ordinarily reside, or are strata corporations formed in the jurisdiction, the Code applies only of the credit is first provided under the contract in the jurisdiction. Although these provisions seem to contemplate interstate rather than international credit contracts they arguably give the Act international application.

---

[207] Such as the EFT Code of Practice, where it applies. The Code of Banking Practice does not contain provisions of this type.

[208] Section 6 sets out the general jurisdiction of the Code.

Credit Transactions and the Internet

It is foreseeable that some credit arrangements may be entered into in the context of Internet transactions by consumers which may fall within the purview of the Code, if the debtor is or has been ordinarily resident in an Australian State. The Code seems implicitly to be based on the view that established entities in the business of providing credit to consumers in Australia are in the main also incorporated or carrying on business in Australia. One concern may be that entities which conduct business on the Internet, either based from Australia or overseas, may offer credit in a manner which could bring its activities within the terms of the Code.[209] Conversely, Australian credit providers may need to comply with similar laws which have been enacted in other jurisdictions, such as the United States. The extra-territorial application of the Code remains to be established.

[209] These entities may also require an Australian banking licence.

7. Security and Privacy

Security and privacy considerations go to the heart of issues about the viability of the Internet as a commercial medium. Both of these are part of the broader question of trust of the medium. In order to achieve the full potential of electronic commerce, and more broadly, the Global Information Infrastructure, it is fundamentally important that the users of information technology have trust in the security of information and telecommunications systems, and the confidentiality and integrity of data on those systems. Accordingly, it is necessary to examine the current state of security measures being implemented at a local and international level.

7.1 Security

Key Issues: *What form of protection is offered for new payment mechanisms What/who governs the use of encryption and security technologies? What encryption measures can be taken legally in Australia? Can encryption technologies be used legally for transferring data to other countries or in terms of export control of encryption technologies? Should the government legislate to provide a secure framework for Internet commerce? Legislation could include laws covering the use of digital signatures, the requirements and liabilities of certificate authorities. Should legislation be developed on an international basis? How would this be facilitated and through what mechanisms?*

Numerous payment mechanisms are currently available to meet consumer preferences. These include cash, cheques, credit and debit cards, prepaid cards, bank notes, physical tokens, travellers cheques and others. Many of these payment mechanisms have already begun to adapt in response to the conduct of business over networks, although the use of electronic commerce is, to date, limited.

A key impediment has been the absence of a secure system for conducting commercial transactions. Without secure payment tools both customers and merchants are reluctant to trade using the Internet.

Different payment schemes have been designed or are being used on the Internet. Each of these mechanisms has a different set of attributes that make them more or less desirable for different types of electronic commerce transactions. To be accepted by users, payment systems must contain certain controls that allow transactions to be verified and authenticated. The system must also be reliable, private and protected. Major requirements for both merchants and consumers include:[210]

- **Authentication** - users should be assured that their orders and/or payments cannot be easily forged or altered, and if they are altered, evidence of this tampering will be immediately apparent;
- **Non-refutability** - users should be able to verify that exchanges have taken place between the intended parties. This verification could be provided by a receipt and/or proof-of-payment mechanism. Receipt and payment information must be non-refutable, despite any complications that may result from delivery of services over long periods of time, interruptions in service, or differences in billing and collection procedures by different service providers; and
- **Protection** - the users should be assured that they cannot be easily duped, swindled or falsely implicated in a fraudulent transaction. They should be protected against eavesdroppers, impostures and counterfeiters. This protection should apply throughout the whole transaction process by which a good is purchased and delivered.

[210] Clarke, R. 1996, *Issues in Technology-Based Consumer Transactions*, September, http://www.anu.edu.au/people/Roger.Clarke/SOS/SOCAP96.html

Specific customer requirements include:[211]

- unauthorised entities should not have any access to transactions;
- credit card information can be optionally hidden from the merchant to prevent attacks on a merchant's server;
- optional receipts signed by the merchant; and
- prevention of unauthorised transactions including transaction replays by a hacker, modified transactions or fake transactions.

Specific merchant requirements include:[212]

- efficient and automated operation of payment authorisation and capture;
- authentication;
- guaranteed non-repudiation of customers' orders
- proof of customer approval of transactions.

There are still many risks involved in the transmission of data. These include:[213]

- non-receipt of a message by the intended recipient;
- access by an unintended person or organisation;
- deliberate or accidental change to or corruption of the contents while in transit; and
- receipt of a false message.

7.1.1 Security of Payment Mechanisms

Based on an examination of the different payment systems that are currently being offered, it appears that there are four main schemes available:

- electronic cash;
- stored value cards;
- centralised systems of provisional accounts whereby a third party manages transactions on behalf of subscribing consumers and merchants; and
- credit card payments.

Each of these payment mechanisms purport to have some mechanism built-in or being developed to protect the security of transactions performed.

a) Electronic Cash

Systems such as Digicash[214] and Netcash allow the customer to deposit cash into a bank account and use this cash to purchase items via the Internet. Encryption techniques are used to establish secure 'electronic purses' on a user's work station to hold 'digital dollars'. Cash is transferred from a bank account onto the user's hard

---

[211] Elgamal, T. 1995, *Commerce on the Internet: Credit Card Applications Over the Internet*, Netscape Communications Corporation, July, http://home.netscape.com/newsref/std.credit.html

[212] *ibid.*

[213] *ibid*.

[214] Digicash, 1996, *Digicash home page*, http://www.digicash.com

drive, encoded into 64 bit numbers. The customer can then transfer the cash to a merchant on the Internet provided that the merchant accepts this form of payment. The cash is then returned to the bank in exchange for real money.[215]

Electronic cash is often seen as more attractive because it is untraceable. The bank does not link the numbers to a particular person which makes it impossible to link or trace payments and purchases, ie. anonymity is preserved.

Another advantage of electronic cash is its ability to facilitate small purchases. Credit cards are not conducive to buying small items when the fees could cost the merchant more than the price of the item purchased.

The main disadvantage of such a system is that digital dollars are uninsured. If the user's hard drive was to crash or hackers decode the numbers of the electronic cash there would be no way to retrieve the money as the bank does not link the money to a particular person. These payment systems are also often limited to dollar payments and are therefore not conducive to international exchanges.

Questions of who should regulate electronic cash remain. Should there be restrictions on who can issue electronic cash? Should issuing organisations be licensed and/or regulated? Are international agreements and regulations required? Without sufficient controls and safeguards, a wide variety of unofficial currencies could be created and circulated.[216]

Another significant security concern, predominantly for consumers rather than merchants is that these new 'banks' such as Digicash are operating outside the official regulated payment system. Similar organisations located within Australia such as QuickLink, a consortium of private companies, and Transcard, also a private organisation are also exempt from banking regulations. There may be no legal avenue for consumers to reclaim their deposits in some circumstances, such as insolvency of the entity.

b) Stored Value Cards

Similar to electronic cash, stored value cards (SVCs) will enable value to be transferred, not onto a users hard drive, but onto a card that may have a computer chip which can receive, process, store and transmit information. SVCs can be designed to be disposable, with the card thrown away once the value has been depleted, or reloadable either through an ATM terminal or via the Internet from a bank account.[217]

SVCs are currently being designed and trialed. There have been predictions that they will replace currency that is currently used for approximately 90 percent of our purchases.[218]

The main advantage of SVCs is the ability to use them as quickly and easily as cash. Unlike cash, however, it is expected that the cards will enable lost money to be refunded, provided they are linked to a particular person.

c) Payment Clearing Systems

A number of companies are providing intermediary services or electronic clearing systems to facilitate commerce over the Internet. Companies such as First Virtual[219] and CyberCash[220] act as trusted third parties for

---

[215] Helmer, R. 1996, *Romans Internetwork Payment System - DB*, http://olymp.wu-wien.ac.at/usr/h90/h9053078/encrypt/artikel.html

[216] Cross Industry Working Team (XIWT), 1996*, Electronic Cash, Tokens and Payments in the National Information Infrastructure*, June, http://www.cnri.reston.va.us:3000/XIWT/documents/dig_cash_doc/TOC.html

[217] Centre for Electronic Commerce, 1996*, Smart Cards and the Future of Your Money*, Report to Australian Commission for the Future, http://acff.com.au/smartcard.html

[218] *ibid*.

[219] First Virtual's founding members, 1996, *The Lessons of First Virutal's First Year*, http://www.FV.com/pubdocs/fv-austin.txt

[220] Crocker, S. et al, 1996, *CyberCash: Payments Systems for the Internet*, August, http;//info.isoc.org/HMP/PAPER/8/abst.html

both merchants and consumers. They manage the accounts and provide a gateway to one or more financial instruments for payment.[221]

The advantages of such a system is that the intermediary provides clearing, settlement and authorisation of transactions. Yet, there is a requirement that both customers and merchants must have accounts with such an intermediary service in order to utilise the service.[222]

d) Credit Cards

Credit card systems will operate much the same way as they currently do, and for this reason are highly conducive to performing commercial transactions over the Internet. In addition, there is already a very large base of users of credit cards.[223]

The use of credit cards eliminate the need for intermediaries other than the financial institution. Consumers use a Web based form to fill out their order information and provide their credit card number directly to the merchant who then executes that transaction with the financial institution.

Unlike the system of using intermediaries, as outlined above, there would be no need for merchants or users to open new accounts. This is specifically advantageous for merchants, who, under the intermediary systems currently operating, would have to pay a commission to the intermediary company for every transaction processed.[224]

Another advantage is that credit card transactions link the customer's name to the account. This means that customers will not be able to maintain the anonymity of a cash transaction. Also, unlike cash, the money is retained in the account until it is 'spent', eliminating the risk of loss.

The efficiency of credit-card payment systems is well proven. Therefore, when extended to Internet commerce, this method of payment should be particularly useful for international transactions. However, using a credit card becomes impractical for payments below a certain amount, under which the proportion of administrative costs becomes excessive.[225]

Credit card payment systems require the transit of the customer's credit card number via the Internet, which could lead to fraud problems, but automatic encryption techniques are being developed. In addition, protocols are being established, such as the SET protocol (discussed below) to facilitate the use of these techniques.

---

[221] Pays, P. & Comarmond, F. 1996, *An Intermediation and Payment System Technology*, Presented at the Fifth International World Wide Web Conference, May 6-10, France. http://www5.conf.inria.fr/fich_html/papers/P27/overview.html

[222] *ibid*.

[223] Elgamal, T. 1996, *op cit*,.

[224] *On-line Payment Systems are only waiting for merchants and buyers,* http://www.dafsa.fr/commerceline/Version-anglaise/pay2.html

[225] European Commission, 1996, *Online Commerce and the Payment Issue*, April. http://www2.echo.lu/GST/Ecash.html

7.1.2 Developments to Protect Security

Technological Developments

To some extent the race to provide these features and develop the means of secure electronic exchange is a race of technology - developing encryption techniques. Most of the payment schemes operating are using some form of cryptography to ensure both the security and privacy of commercial transactions.

Cryptography is the science of converting messages or data into a different form, such that no-one can read them without having access to a 'key'. There are two distinct classes of cryptography - symmetric (private) and asymmetric (public). Encryption is the use of cryptography techniques.[226]

Symmetrical or private key encryption involves the use of a single 'secret' key which both the message sender and the message recipient must have. It is used by the sender to encrypt the message, and the recipient to decrypt it.[227] Private key encryption is poorly suited to open systems like the Internet where sellers and buyers want to be able to do business with each other without having any prior relationship, as would be necessary if private keys were to be exchanged as a preliminary to single key encryption transactions.[228]

Asymmetrical or public key encryption is the use of different keys to encrypt and decrypt messages respectively. It is considered the most appropriate tool with which to build payment systems. It makes it possible to 'sign' a document so that the recipient can be assured that the source of the message is authentic, as well as to 'seal' a document so that no-one except for the recipient can open or change it. The system uses two different 'keys' for the same message, one of which is made available to the public generally and the other kept private. To ensure privacy the sender of a message uses the recipient's public key to encrypt their message, which is then inaccessible to anyone lacking the corresponding private key - which only the recipient has. An online merchant, for example, would make its public key available to shoppers. The merchant's private key would be used to decrypt messages encrypted by its public key.[229]

Public key encryption facilitates privacy and makes secure payment possible on open network architectures. It also makes it possible to add an electronic signature to a document. An electronic signature is, simply, a document encrypted with a persons private key. If the signature, decrypted with the signer's public key matches the document then it must have been 'signed' by that person. The document can not be altered without invalidating the signature.

The system, however, requires an infrastructure for key management. There must be places from which public keys can be obtained and associated with the person or entity with whom one wants to do business with. This essentially adds an additional layer of security such that merchants and vendors must provide details of themselves to an independent verification institution. These institutions are known as 'certificate/certification authorities' or 'trusted third parties'.[230]

Based on encryption, a number of companies are developing methods for encrypting messages that are sent over the Internet. Protocols are being established to facilitate:

- secure message mechanisms - standards used to ensure the privacy of part or all of the message sent over the Internet.

---

[226] Clarke, R. 1996, *Data Transmission Security*, May, http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy

[227] Sedallian, V. 1996, *Cryptography: What is at Stake?* April, http://www.argia.fr/lij/english/ArticleAvril1.html

[228] Ibid.

[229] Perritt, H. 1995*, Guidelines for Commercial Key Escrow, Including Transnational Protections - Draft*, June, http://www.law.vill.edu/chron/articles/forsea.thm

[230] XIWT, 1996, *op cit*,.

- secure electronic transactions - protocols for recording payments to be made through a third-party. These protocols cover the forms of the transmitted message, rather than the methods used to ensure the privacy of the message; and

What follows are a few examples of each.

Secure Message Mechanisms

- ***Netscape SSL -*** Netscape Communications have developed their own 'Secure Sockets Layer' (SSL) encryption standard. The goal of the SSL protocol is to provide privacy and reliability between two communicating platforms. The SSL protocol provides connection security that has three basic properties: the connection is private, can be authenticated and is reliable.[231]

- ***Secure HyperText Transfer Protocol (SHTTP)*** - Developed by the (US) Internet Engineering Task Force, this standard is an extension of HTTP providing independently applicable security services for transaction confidentiality, authenticity/integrity and non-reputability of origin.[232]

Secure Electronic Transaction Protocols

- ***Internet Keyed Payment Protocols (iKP) -*** IBM has developed the iKP protocol, using strong cryptography, to allow customers to order goods, services or information over the Internet while relying on existing secure financial networks to implement the necessary payments. Designed to work with credit cards, the protocol will support other payment instruments in due time.[233]

- ***Secure Electronic Transactions (SET) -*** Visa and Mastercard, with support from IBM, Microsoft and Netscape have formed an alliance with a mandate to develop a common security standard for Internet transactions. The protocol will allow consumers, merchants and credit card companies to verify identities and approve account information over the Internet.[234]

  The SET protocol uses cryptography to provide confidentiality of information, ensure payment integrity and authenticate both merchants and cardholders. It defines a mechanism to verify that a cardholder is a legitimate user of a valid payment card account number.

  Once a cardholder approves an order and chooses to use a payment card, the SET protocol provides the mechanisms for the cardholder to securely transmit payment instructions as well as for the merchant to obtain authorisation and receive payment for the order.

  Authentication is further strengthened by the use of certificates. Certificates will be issued to cardholder's upon approval of the cardholder's issuing financial institution. The certificate, managed by a third party (certificate authority) is transmitted to merchants with purchase requests and encrypted payment instructions. Upon receipt of the cardholder's certificate merchants can be assured that the account number has been validated by the card issuing financial institution.[235]

  A SET pilot project is scheduled to begin in early 1997 involving three merchants and 500 - 1000 consumers in Denmark.[236]

- ***Joint Electronic Payments Initiative (JEPI) -*** In an effort to avoid a myriad of incompatible standards and protocols, the World Wide Web Consortium and CommerceNet have proposed an Internet payment protocol

---

[231] Netscape, 1996, *SSL Version 3.0*, http://www.netscape.com/newsref/std/SSL.html

[232] Helmer, R. 1996, *op cit*,.

[233] Janson, P, 1996*, Internet Keyed Payment Protocols (iKP),* Zurich Information Technology Solutions Department Manager, http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP_overview.html

[234] Evans, C. 1995, *Secure Payment on the Internet*, October, http://www.qrg.com/secpaysys.html

[235] Mastercard and Visa, 1996, *Secure Electronic Transaction (SET) Specification Book 1: Business Description*, February, http://www.mastercard.com/set/set.htm

[236] Mastercard, 1996, *Mastercard Home Page*, http://www.mastercard.com/

known as the Joint Electronic Payments Initiative (JEPI). The JEPI standard is aimed at providing a single, unified protocol for everyone including web server, browser and payment vendors to incorporate their own products to ensure interoperability between different systems.[237]

JEPI will allow different payment instruments and protocols to exchange information. It is designed to be a negotiation method between browsers and servers and will act as an umbrella over standards such as SET and others.[238]

The development of encryption, and associated standards and protocols to protect emerging payment systems on the Internet is being complemented by further technological developments. A major problem with the use of credit cards has been that transactions are not processed in real time. Although the information is presented to the vendor in a secure process, it still needed to be processed manually. While this is acceptable for some vendors who deal in tangible goods, where delivery can be delayed until confirmation, it has presented a problem for merchant offering intangibles for immediate delivery.

Companies such as Switchtech and Verisign, both US based, are developing systems that verify credit card transactions in real time. Transaction authorisations are immediately sent to customers upon validation of the card information.

[237] World Wide Web Consortium (W3C), 1996, *W3C Home Page*, http://www.w3c.org

[238] *ibid*.

Regulatory Measures

While many security concerns will be addressed by these emerging technologies, standards and protocols, legislative measures may also be necessary. The most outstanding issues to be addressed include:

- the extent to which these encryption technologies can be used;
- the use of digital signatures; and
- the introduction and regulation of certificate authorities.

Use of Encryption

Australia is dealing with the issue of encryption through the use of standards. Although it can be strongly argued that the Federal Parliament has adequate power to regulate the Internet under the communications power of Section 51 of the Constitution,[239] the Australian government has claimed that there is no blanket constitutional power and that there would be problems in reaching agreement with State and Territory governments on such legislation.

It is presently being left up to groups such as Standards Australia to specify the standards for encryption.[240]

The United States is more advanced in developing policies to support encryption. Any American is free to use any encryption system domestically, although the administration is currently developing legislation to facilitate commercial key recovery, under which the keys for encryption products would be stored with trusted entities, which would provide the keys needed to decrypt encrypted information encountered during a law enforcement investigation. The legislation is expected to include providing penalties for improper release of keys and protecting key recovery agencies against liability when they properly release a key.[241]

Cryptography experts from OECD countries are drafting a proposal for OECD Cryptography Policy Guidelines. The Guidelines identify the issues which countries should take into consideration in formulating cryptography policies at the national and international level. The Guidelines will be non-binding recommendations to Member Governments, meaning that they will not be part of international law nor will they endorse any specific cryptography system.[242]

A working draft for the December 1996 meeting of the Ad-hoc Meeting of Experts on Cryptography Policy asserts free choice in cryptography techniques.[243] According to a press release the discussion has focussed on the rights of users to choose cryptographic methods, the freedom of the market to develop them, interoperability, consequences for the protection of personal data, lawful access to encrypted data and reducing the barriers to international trade.[244]

The draft states that in developing a cryptography policy, a state must carefully weigh the risks of fraud, additional expense of any supporting infrastructure, and other costs against perceived benefits. The present

---

[239] Placitum (V) - Powers of the Parliament in Section 51 of the Constitution states that the Parliament shall have the power to make laws for the peace, order, and good government of the Commonwealth with regard to postal, telegraphic, telephonic, and other like services. It is argued that the Internet could be classified under this definition.

[240] Orlowski, S. 1996. *Security of Government Information Infrastructure*, http://www.anu.edu.au/people/Roger.Clarke/II/Orlowski.html

[241] US Government, 1996, *Administration Statement on Commercial Encryption Policy*, July, http://www.epic.org/crypto/key-escrow/wh_cke_796.html

[242] Ad Hoc Group of Experts on Cryptography Policy Guidelines, 1996*, OECD Draft Guidelines for Cryptography Policy*, September, http://www.oecd.org/

[243] OECD, 1996, *OECD Expert Group Finalises Cryptography Guidelines*, News Release, 23 December 1996, http://www.oecd.org/news_and_events/release/hw96119a.htm

[244] Koops, B. 1997. *Crypto Law Survey*, http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm

wording of the Guidelines does not indicate that governments will be pushed to develop key-management systems; they allow governments to implement such systems, but prevent making such a system mandatory.[245]

Use of Digital Signatures

Digital signatures are used to provide user authentication, integrity and non-repudiation security services.[246] Electronic signatures are created through the use of encryption. A digital signature takes a different form to a handwritten signature on a paper document so that it not only provides evidence which identifies the sender, but can also ensure that the contents of an electronic message have not been altered.[247]

Changes to the law will be necessary if electronic signatures are to have the same legal validity as written signatures, allowing the signing of contracts online.

The European Union has launched a call for tender for a 'Study on the Legal Aspects of Digital Signatures' which, it is assumed, will provide a basis for developing rules and regulations, as well as (de facto) practices concerning digital signatures in the Member States. It is recognised that there is a need both to establish irrefutably the origin of, and the delivery of, such information and, particularly, that the information has been signed and stored in an unforgeable way.[248]

In the United States at least ten states are developing or have already implemented digital signature legislation. Many of the frameworks for such legislation are drawing on the legislation developed in Utah, and enacted into law in 1995.[249]

The Utah Digital Signatures Act (The Act) provides digital signatures with legal status as valid signatures and addresses a variety of issues relating to the place of electronic documents in contract and evidence law. A time stamped digital signature is considered prima facie evidence that the signature took effect as of the time and date indicated.

Dealing with the issue of who is responsible if a digital signature is used to perform an illegal or unauthorised transaction the *Act* makes two policy choices concerning liability allocation. First, consumers who undertake commercial transactions over the Internet under the *Act* subject themselves to far greater risk of extensive liability. Consumers are held to a negligence standard in guarding their private encryption key. If a criminal obtains a consumer's private key and commits fraud, the consumer if financially responsible for that fraud unless they can prove they had exercised reasonable care in guarding the private key. If they cannot prove this, the consumer will bear all the losses resulting from the fraud.[250]

Secondly, the *Act* limits the potential liability of one actor in the infrastructure - the certification authority (CA) to a fixed amount. This amount may be less than the actual damages a certification authority can cause.[251]

Such a policy decision, it is argued, was designed to create certainty for an entrepreneur contemplating a certification authority business and to foster the development of a certification authority industry. But it may have unintended consequences. Because the CA would not have to bear the full costs of losses resulting from the security breach, they may not have the incentive to take adequate precautions to protect against that occurrence.

In 1995 the American Bar Association developed a set of guidelines, primarily based on the Utah legislation, for the introduction of digital signatures on a national level. These guidelines are general, abstract statements of

---

[245] ibid.

[246] Standards Australia, 1996, *Strategies for the implementation of a Public Key Authentication Framework (PKAF) in* Australia, SAA Miscellaneous Publication 75 - 1996, p.21.

[247] Digicash, 1996, *Digital Signatures and Smart Cards*, Presentation delivered at the 3rd International Smart Card Conference, Amsterdam, March, http://digicash.support.nl/publish/digsig/

[248] Information Society Project Office (ISPO), 1996, *Study of the Legal Aspects of Digital* Signatures, http://www.ispo.cec.be/

[249] Biddle, B. 1996, *Digital Signature Legislation*, Privacy Rights Clearing House, Centre for Public Interest Law, February, http://pwa.acusd.edu/~prc

[250] *ibid*.

[251] *ibid*.

principle, intended to serve as long-term, unifying foundations for digital signature law across varying legal settings. They may serve as a common basis for more precise rules in various legal settings.[252]

The Guidelines seek to establish a secure, computer-based signature equivalent, which will:[253]

- minimise the incidence of electronic forgeries;
- enable and foster the reliable authentication of documents in computer form;
- facilitate commerce by means of computerised communications; and
- give legal effect to the general import of the technical standards for authentication of computerised messages.

Australia is currently attempting to provide a framework for the use of digital signatures through Standards Australia. Standards Australia has developed a Public Key Authentication Framework (PKAF) which will provide a scheme where a digital signature will be linked to a particular person by electronic certification processes. The transaction however can only be trusted if the total framework for supporting issue and maintenance of the keys is also trusted. A support system is essential for the PKAF to work.[254]

The framework, however, recognises the need for appropriate legislation to confer legal status on digital signatures created and used under the scheme. There is also a need to define the liability of users when using the scheme.[255]

It is also recognised that any use of digital signatures must be supported internationally. Although US initiatives are being matched by other countries such as Germany there are as yet no accepted international laws or standards to deal with electronic signatures. The Attorney General's Department expects that Commonwealth legislation on digital signatures will be introduced by the end of 1997.[256]

In Australia, the Department of Communication and the Arts (DoCA) APEC Telecommunications Working Group are pursuing the promotion of similar frameworks to PKAF in APEC economies to assist in introducing an international framework.[257]

On the global scale, UNCITRAL has proposed legal guidelines to expand the recognition of digital signatures as valid signatures. UNCITRAL has recommended that governments "review legal requirements of a hand-written signature or other paper-based method of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication".[258]

Certification Authorities (CAs)

It is argued, however, that no amount of cryptography or digital signatures alone will reliably authenticate or identify two strangers who have no alternative means of communication.[259] To assure proper linkage of a

---

[252] American Bar Association, 1995, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce*, October, Information Security Committee: Electronic Commerce and Information Technology Dividison, Science and Technology Section of the ABA. http://www.law.vill.edu/vis/student_home/courses/computer-law/abaguide

[253] ibid

[254] Australian Customs, 1997*, Electronic Commerce Discussion Paper 1: Security Aspects*, Draft paper for discussion.

[255] Standards Australia, 1996, op cit.

[256] ibid.

[257] ibid.

[258] Official Records of the General Assembly, 40th Session, Supp. No. 17 (A/40/17), P 360, 1985, as quoted in Raysman, R & Brown, P, 1995, Electronic Signatures, *New York Law Journal*, October.

[259] Froomkin, M. 1996, *The Essential Role of Trusted Third Parties in Electronic Commerce*, October. http://www.law.miami.edu/~froomkin/articles/trusted1.htm

digital signature with the owner of a distinguished name third parties are being established. These third parties are referred to as Certification Authorities (CA).

A CA is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact about the subject of the certificate.[260]

The PKAF, established by Standards Australia provides the scheme which outlines the functions and operating environment of the CAs.[261] It envisages CAs performing multiple functions, including:

- generation of pairs of private and public keys;
- escrow of private keys;
- storage of public keys; and
- authentication and certification of public keys

and outlines the requirements for creation, management and distribution of authenticated keys.[262]

CAs will need to certify the bindings of certified digital signatures to a user's identity, create certificates and generate Certificate Revocation Lists (CRLs). CRLs will be used to inform users of situations where a private key is known to be or suspected to have been compromised. This will allow users to identify and reject possibly fraudulent transactions.

To assure users that certificates they create can be trusted, CAs within the PKAF must function correctly, implement the specified security policy and preserve the binding between the user and the user's digital signature.[263] The PKAF also includes operational procedures for the trusted operation and interoperation of certification authorities within and external to its framework.[264]

The European Union is also preparing a proposal on the establishment of a Europe-wide network of Trusted Third Party Services. The network would be established for providing certification services by private trusted third parties (TTPs). Although primarily meant for establishing an infrastructure for the use of public key encryption, the proposal will also address the legal interception problem: law enforcement authorities could apply to access keys, provided they have a court order or warrant.

As electronic commerce grows it will become increasingly important to define the rights and duties of CAs or TTPs. Some states in the US have attempted to define the rules applicable to these entities in digital signature legislation. Both the Utah *Act* and the Guidelines produced by the ABA are, in large part, devoted to establishing the interrelated legal duties of certification authorities, subscribers and recipients of digital signatures. However, basic concepts, such as whether a CAs provision of a certificate is a sale of a good or a service still need to be determined.[265] Rules concerning the liability of a CA for negligent misrepresentation in a certificate are also necessary.

7.1.3 Liability for Failure of Secure Systems

Internet payment mechanisms including smart cards, digital coins, cheques and associated digital signatures are likely in the future to be governed by a variation of the EFT Code of Conduct which amongst other things, imposes liability for failure of the secure system on the card issuer. A degree of liability may also be imposed by legislation which is enacted as a consequence of international treaties.

---

[260] ibid.

[261] Standards Australia, 1996, op cit.

[262] Escrow is an arrangement whereby something is placed on deposit with a trusted party but may be accessed by third parties under certain conditions, ie. in the interests of national security or crime.

[263] Standards Australia, 1996, op cit.

[264] ibid.

[265] Froomkin, M, 1996, *The Essential Role of Trusted Third Parties in Electronic Commerce*, October, http://www.law.miami.edu/~froomkin/articles/trusted1.htm

Once a duty of care is found to exist, then liability for failure of secure systems will be dependent upon whether the standard of care has or has not been met. The standard of care, which would consist of minimum security standards for networks, will be established by a combination of caselaw, industry practice and standards, and potentially by legislation.[266] Australia has no current legislation of this nature.

Some caselaw in the United States deals specifically with standards of network security. For example it has been held[267] that a customer has the right to expect a reasonable level of network security taking into account the vendor's special knowledge, skills and ability. In that case, a computer network security specialist was found to be subject to the higher standard of care of a professional rather than an ordinary person. However, it appears that cases conflict on this point[268]. In another case[269] it has been held that a security system vendor's use of industry standard security technology could be evidence of reasonableness, but will not always relieve the vendor of liability because industry practice or standards may not be reasonable or adequate.

Industry standards which will have a bearing in this area include the Australia/New Zealand standards on Information Security Management,[270] the OECD Guidelines for the Security of Information Systems 1992,[271]and others.[272]

Standards Australia provides a outline of what it considers to be the extent of liability to which a CA should be exposed to in electronic transactions. These are as follows: [273]

- A CA has no liability associated with the loss by the user of the private keys;
- A CA has no liability associated with user generated keys unless they were generated fully in accordance with the guidelines of the PKAF;
- A CA has no liability associated with the compromise of the private keys it produces, unless it can be proved that the keys were compromised at the CA, or that documented policies and procedures were not followed during the key generation process resulting in a private key that is more susceptible to compromise or actual revelation of the private key;
- A CA has no liability for the compromise of the key distribution process;
- A CA has no liability associated with forged signatures, unless the forgery resulted from the policies and procedures of the PKAF not being followed, or could be shown to permit forgery;
- A CA has liability associated with the wrongful binding of an individual's identity with an associated digital signature, unless it can be proved that the documented policies and procedures for identification and authentication were followed. This liability shall extend to circumstances where a CA knew or suspected, or should have known or suspected that the binding might be wrongful;
- A CA has liability for not revoking certificates according to its revocation policy;
- A CA has liability for revoking a certificate for a reason not specified in its revocation policy; and
- A CA has liability if a certificate in the database is wrongfully changed or deleted.

---

[266] The legislature could also impose strict liability. In the United States government agencies are required under the Computer Security Act to establish computer security policies commensurate with the risk and magnitude of the harm resulting from the loss.

[267] *Diversified Graphics v Groves* 868 F.2d (8th Circuit 1989*).*

[268] *Re Hospital Computer Systems Ltd* 788 F. Supp. 1351 (D. NJ 1992).

[269] *T J Hooper* 60 F. 2d 737 (2d. Circuit).

[270] Document DR 95305.

[271] Upon which the Australian security standards are based.

[272] The Uniform Commercial Code Article 4A, the UNCITRAL EDI Uniform Rules of Conduct, the American Bar Association Model EDI Agreement, the United Nations Draft Model Law of Legal Aspects of Electronic Data Interchange and Related Means of Communication.

[273] Standards Australia, 1996, op cit.

It is recognised that any policy outlining liability of a CA must distinguish between direct liability and indirect and consequential damages. The liability policy must reflect limitations to liability which may be specified in government regulations and international agreements.[274]

Liability for risk of failure of secure networks can be allocated or shifted by means of contracts between merchants, ISPs, network security services vendors, insurers and customers.

7.2 Privacy

Key Issues: *Which laws/codes apply in international transactions given the absence of international legislation or regulation? What requirements will have to be met in terms of 'adequate' data protection in order to deal with the European Union?*

To a certain extent the issues of privacy and security go hand-in-hand. Commerce on the Internet will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information.

Security measures, specifically the use of encryption, in addition to protecting the authenticity and integrity of data communications, are also protecting privacy over networks.

Yet while these security measures can protect the actual message, they do little to protect or hide the trail created as transactions are conducted. Information sent over the Internet may pass through dozens of different computer systems. Each of these systems may be managed by different system operators, and each may be capable of recording the transaction. Most electronic forms of commerce leave records by definition. This includes the amount being spent, the date, time and location of transaction, the identities of the parties and the nature of the goods being purchased.

Some of the emerging payment mechanisms are designed to maximise privacy. DigiCash and NetCash have been designed to allow consumers to make payments with substantial anonymity. Such systems, however, are really only conducive to small transactions, given their limited protections in terms of liability. It is unlikely that large transactions would be undertaken using such systems.

Other payment systems leave the same 'trail' over the Internet as they do at points of sale. This means that detailed information about the transaction is available to merchants, financial institutions and credit card companies.

The introduction of personal information tracking mechanisms by web browsers have increased concern for the privacy of online communications. Known as 'cookies', these tracking mechanisms are able to both store and retrieve information on the client side of the connection.[275]

In simple terms, a 'cookie' is a program that a web server can send across the Internet and deposit on a users hard drive. It lets sites 'tag' a visitor with a unique identification so they can be identified every time they visit that same site in the future, depending on the life span of the cookie. The cookies collect a certain amount of information (up to 255 characters in length) and may include details such as the site entered from, the type of information requested and information about the system being used, the type of computer, ISP etc. By utilising cookies commercial web sites have also been able to construct online shopping sites which 'remember' products that have been bought by individuals.

Arguably, cookies are beneficial for both merchants and online consumers. Not only do they provide a marketing opportunity for site managers, but they are a device that will deliver to users the benefit of a site's knowing who they are and what they are like.

---

[274] *ibid*.

[275] Netscape Corporation, 1996, *Client State HTTP Cookies,* http://cgi.netscape.com/newsref/ std/cookie_spec.htm

Yet these tracking mechanisms raise numerous concerns about privacy and security, primarily because they are deposited on a users hard drive without disclosure or consent. Questions of how the use of cookies by web site operators can be covered by privacy legislation needs to be addressed. Regulators may need to legislate to prohibit web site operators from reading a site visitor's cookie file.

7.2.1 Current Privacy Protection

How this information is protected is an obvious concern, both for merchants and consumers. In Australia, there is little protection afforded to privacy in an online setting. There are three possible solutions to the protection of data.

a) Legislation

Federal Privacy Act

There is no general legal right to privacy in Australia, although there are various protections in statute and common law. The most significant of these statutes is the *Privacy Act* of 1988. The *Act* lays down strict privacy safeguards which Federal Government departments and agencies must observe in collecting, storing and using personal information.

The eleven Information Privacy Principles (IPP's) outlined in the Privacy Act are based on established international principles. They can be summarised as requiring:

- openness (through notification of individuals when collecting data);
- data quality (accuracy, relevance, completeness etc);
- access and correction rights for individuals; and
- use and disclosure limitations.[276]

In 1990 the *Act* was amended to include the credit reference industry but the credit aspects of the *Act* potentially extend to most persons who or bodies which provide credit. This was the first application of the Act to the private sector and as such is potentially important to Internet commercial transactions. The law aims to protect information relating to the credit-worthiness of individuals and to ensure that the use of this information is restricted to assessing applications for credit lodged with a credit provider. Credit reporting agencies will generally only be able to give access to personal credit information about individuals to businesses which are credit providers. Credit providers will themselves generally not be permitted to disclose consumer credit information except in circumstances described in the legislation.[277]

It also requires that credit reporting agencies only hold on your file permitted information which is up to date, complete, accurate and not misleading. The law also requires that credit providers and credit reporting agencies take reasonable steps to protect your personal information against unauthorised use and disclosure. Other obligations deal with access and amendment rights of consumers.[278]

A further amendment in 1991, the *Data Matching Programme (Assistance and Tax) Act* was introduced to regulate certain data matching activities by government departments. The Privacy Commissioner is specifically authorised to regulate the matching of personal data and especially the use of the tax file number as a data matching reference point.

---

[276] Austel, 1991, *Inquiry into the Privacy Implications of Telecommunications Services*, Discussion Paper, November.

[277] Privacy Commissioner, 1996, *About Australia's Privacy Laws: Credit Reporting*, Privacy Commissioner Human Rights Australia, http://www.austlii.edu.au/hreoc/privacy/abcred.htm

[278] ibid.

The latest amendment, however, is still only applicable to government agencies and departments. With the exception of the credit reference industry and other persons who or bodies which provide credit, there are no regulations covering how private companies can collect or use data.

In September 1996 the Attorney General's Department released a Discussion Paper[279] outlining a possible co-regulatory approach to further extending privacy protection. Standards for data protection would be set down in IPPs encompassing all the internationally recognised tenets of privacy protection. These would be complemented by Codes of Practice, to be developed in relation to specific information, activities, organisations, industries or professions. Codes would be tailored to meet the needs of a particular part of the private sector, and would be able to elaborate on the IPPs.[280]

The paper gives a detailed outline of what the Codes of Practice should contain, the procedure for issuing the codes, and ways of amending or revoking them. Under the proposed regime, the Federal Court would be able to order individuals and organisations to pay compensation, refrain from acts which would constitute an interference with privacy, and take the appropriate measures to avoid an interference with privacy.[281]

In addition to the above, a number of States in Australia are exploring the need to enact State Privacy Laws.

Telecommunications Act 1991

Although the *Act* imposes regulations on the carrier's handling and storage of personal information, the regulations imposed do not cover the activities of carriers or service providers when acting as a commercial entity.[282]

b) Self Regulation

Codes of Conduct may need to be developed by individual organisations to provide a guarantee to business partners and consumers to protect the privacy of the data they handle.

An example of such a code is the Electronic Funds Transfer Code of Conduct. This code establishes four privacy principles for the guidance of issuers of electronic funds transfer (EFT) cards. Customers' records must be treated in the strictest confidence and electronic terminal access to details of a customer's account is restricted to employees and agents of the institution which maintains the account, the customer and any person authorised by the customer.[283]

New online payment systems which do generate information about transactions may be subject to the restrictions which currently apply under the EFT code. Otherwise, payment entities could develop their own codes, enforceable through contract rules.

c) Technological Protection

As already outlined in the preceding discussion, there are several technologies available that could be used to enhance privacy online. Most obvious is the use of encryption to protect contents of messages being seen by unauthorised persons.

Other mechanisms emerging include anonymous re-mailers. Because it is relatively easy to determine the e-mail address and name of those posting messages, the practice of using re-mailers which strip all the identifying

---

[279] Attorney General's Department, 1996, *Privacy Protection in the Private Sector: Discussion Paper*, September.

[280] ibid.

[281] ibid.

[282] *Telecommunications Act*, 1991

[283] *Electronic Funds Transfer Code of Conduct* cl 10.1 (i), 10.1 (ii)

information off the e-mail and forward it to the appropriate address are becoming more common.[284] It is questionable, however, how these would work in the case of contracts that are being negotiated online.

d) International Measures

The degree of anonymity and privacy afforded to communications and transactions is a critical question with the ability of organisations to collect and collate large amounts of data on individuals and the possibility of the interception of private communications.

Yet, while national legislation and other regulatory structures such as codes of conduct may work to protect the privacy of communications within specific countries, the borderless nature of the Internet means that it will not be possible to rely on legislative or regulatory structures in the country where the user is located.

Further complicating the issue is the fact that consumers and businesses might not be aware of where the transactions are actually occurring. It is possible to conduct business with a US company which is actually run offshore without realising it. In such a case it is questionable where the transaction information is being collected/held and which privacy and protection laws apply.

Guidelines such as those drafted by international bodies such as the OECD[285] and the United Nations[286] attempt to set out an international approach to the protection of data. Both these sets of guidelines, however, are not legally binding.

The European approach to data protection may provide a possible model for an international approach to privacy. The European Union Council personal data protection Directive was formally adopted in July 1995.[287] It is argued to be the most important international development in data protection in the last decade.[288]

The Directive establishes a Europe-wide set of legal principles for privacy protection, to be enacted in all EU member states. The level of protection is essentially the same in both the public and private sectors, with no formal distinction being made between the two. It applies "to the processing of personal data wholly or partly by automatic means" and requires that data must be:[289]

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and used in a way compatible with those purposes;
- adequate, relevant and not excessive in relation to those purposes;
- accurate and, where necessary, kept up to date; and
- not kept in identified form for longer than necessary for those purposes.

The Directive also prohibits the transfer of personal data from EU countries to any countries which do not have 'adequate' data protection laws, and will therefore place significant international pressure for increased data protection on other countries, particularly in relation to the private sector. Where national legislation does not exist in the country receiving the data, there is provision for the flow of data to industry sectors or even

---

[284] Utility Consumers Action Network, 1996. *Privacy in Cyberspace: Rules of the Road for the Information Superhighway*, http://www.privacyrights.org/fs/fs18-cyb.html

[285] OECD, 1980*, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris.

[286] United Nations, 1989, *Guidelines for the Regulation of Computerised Personal Data Files*.

[287] European Council, *Directive on Protection of Individuals in Relation to Personal Data*, OJ 1995, L281/31.

[288] Greenleaf, G, 1996*, A Proposed Privacy Code for Asia-Pacific Cyberlaw*, School of Law, University of NSW. http://www.usc.edu/dept/annenberg/vol2/issue1/asiapac.html

[289] ibid.

individual organisations which do meet the criteria. This might stimulate both individual companies, or sectors as a whole to establish their own privacy protection codes in the absence of national legislation.[290]

No explicit equivalent restrictions exist on the import of personal data from a third country to an EU Member State. However, the importing of data may constitute collection and therefore processing, so that the importer must comply with national laws of the EU state into which the import takes place.

Australia, and other countries such as the United States will most likely have to adapt or improve their own privacy protection regimes in order to maintain international flows of data with the European Union.

[290] Orlwoski, S. 1996, *Privacy, Security and Law Enforcement*, Presented at a Conference at Charles Sturt University, November. http://www.anu.edu.au/people/Roger.Clarke/II/Orlwoski4.html

8. Proposals for Reform

The Study has revealed the following potential areas of reform:

- As a response to the immediate legal uncertainties arising from the development of electronic commerce and to provide some international standardisation of laws, the UNCITRAL Model Law has been developed to accommodate business transactions, but has not yet been implemented in Australia. The UNCITRAL Model Law governing electronic business transactions requires recognition by legislation in Australia and similar laws need to be enacted to provide for electronic consumer transactions.

- A number of existing international treaties and conventions govern various aspects of international trade and some of them will have a bearing on Internet commerce, particularly where it involves business transactions. However, there is an apparent lack of international principles governing consumer transactions. Appropriate conventions governing consumer sale of goods and consumer protection issues need be established at an International level. The World Trade Organisation is one of the international fora which could have potential impact in the field of electronic commerce, including Internet and online commerce.

- The Australian Law Reform Commission has identified electronic commerce as an emerging priority and recommended that the Federal Attorney-General's Department work on electronic commerce be given a high priority. However, to date neither terms of reference nor members of the expert group have been settled. There is every reason for Australia to take the initiative in law reform in this area and accordingly the Federal Attorney General's work in the area of electronic commerce needs to be fast-tracked.

- Although Internet advertising in Australia will fall within the ambit of the fair trading legislation there is currently no specific legislation or industry codes applicable to Internet advertising in Australia. In this context, the draft Distance Selling Code of Practice released in January this year by the Ministerial Council on Consumer Affairs is a step in the right direction. An industry level advertising code needs to be developed to cater for Internet advertising.

- There is no real reason to believe that many current laws cannot cope with new payment systems and electronic documents. However, minor changes in the law are necessary to legally define new payment systems, and in particular to deal with allocation of liability between parties for system failure or fraud. Legislative change is also required to provide for broader application or recognition of electronic documents.

- The main impediment to development of online commerce has been the absence of a secure system for conducting commercial transactions. While many security concerns will be addressed by emerging technologies, standards, protocols and legislative measures may also be necessary. Australia is dealing with the issue of encryption through the use of standards but legislation may be required at a Federal level to provide a secure framework for electronic commerce. There is strong support for the view that the Federal Parliament has the power under the Australian Constitution to enact such legislation.

- Privacy protection in Australia is somewhat ad hoc and despite recent initiatives by the Federal Attorney-General's Department to further extend privacy protection and various State initiatives, there is little protection afforded to privacy in an online setting. Legislation may be required at Federal and/or State level to provide adequate privacy protection in an online setting.