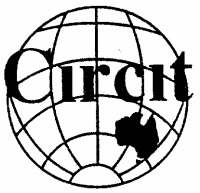

Centre for International Research on Communication and Information Technologies

Literature Review

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

Table of Contents

Overview

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 in December 1996 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 study was undertaken in the following three phases:

Phase 1 - Literature Review

Phase 2 - Statement of Issues

Phase 3 - Analysis of issues

This report contains the output of the first phase which provided a valuable starting point for proceeding further. The last two phases were published together and are available separately from the Literature Review.

The Literature Review is considered to have identified the majority of material sources relevant to the brief. The material is arranged under broad subject headings that properly identify the cover the field of laws and other developments pertaining to the issues under investigation. In addition to Australian laws, a review was also made of those laws of special relevance of the US, UK and EC. This approach enables a better means of comparison of developments in the international arena.

Despite various recent and current investigations by other organisations and bodies into discrete areas relevant to the general study topic, no formative text or collection of material was unearthed that encapsulated all issues raised by the original brief. For this reason, Phases 2 and 3 were then completed, enabling CIRCIT to crystallise its own views and ideas about the significant issues identified.

1. General Material

1.1 Australian Material

1.1.1 Government Reviews

Broadband Services Expert Group *Communications Futures,* Final Report, 1995

The Broadband Services Expert Group was established by the Commonwealth Government on 8 December 1993 with the task of examining the technical, economic and commercial preconditions for widespread delivery of broadband services to homes, businesses and schools in Australia.

Discusses challenges for Australia in building new communications services for the future, based on broadband services, including some reference to the legal and regulatory environment.

NISC, 1996 *Legal Issues Paper from the National Information Services Council,* Agenda papers from the first meeting of the Council, 10 August 1995

The paper discusses the legal issues that the community and business confront in expanding information services and networks to create an information superhighway, the adequacy of the present law in dealing with these changes, and suggests, where appropriate, specific areas that need reform, review or adaptation to overcome actual and potential legal gridlocks on the highway.

1.1.2 Research/Academic Reports

Australian Law Reform Commission, *Legal Risk in International Transaction*, 1996

Focuses on the legal problems faced by Australian business in international commerce. It is a feasibility report assessing the scope for law reform in this area. The report focuses on civil remedies in international commerce and their implications for reform.

Briefly surveys the international treaties and law reform initiatives in which Australia is or has been involved and gives some preliminary comments on the value of that international work to Australian firms.

Summarises the range of international legal techniques and options that are currently used to reduce cross border legal risk into five categories: international agreements, model laws/statements of principles, standard terms and conditions, explanatory guides and industry practice/familiarity.

Discusses the issue of electronic commerce and argues that the on-line economy cannot be achieved without Australia creating a world class electronic payment system for consumer transactions as well as business-to-business transactions. The ability to charge customers interactively over trusted networks is an essential prerequisite for a viable consumer on-line services industry.

Outlines the various law reform initiatives that are dealing with electronic commerce. The issue will be addressed partly through local law making and through the work of international bodies such as UNCITRAL. In the Commission's view the review of legal implications of electronic commerce should be given high priority. The legal issues considered should include federal laws, uniformity of State and Territory laws and relevant international legal and non-legal options.

http://online.anu.edu.au/alrc/report80/ALRC80.html

Bartlett, P and Deeble, M *When Push Comes to Pull, The Legal Implications of Publishing on the Internet,* Paper delivered at the Communications Research Forum 1996, Melbourne, Bureau of Transport and Communications Economics, Canberra.

Paper deals largely with publishing issues such as defamation and copyright, but also looks at recent developments in the law relating to liability of Internet service providers (ISPs) for material which appears on the Internet. Of particular interest are developments in the US where at least one ISP has been held liable as a publisher of defamatory material posted by its users. *Stratton Oakmont Inc v Prodigy Services Co* 1995 WL 323710NY Sup May 24 1995.

Buckeridge, R and Cutler, T; *The Online Economy: Maximising Australia's Opportunities From Networked Commerce* Cutler & Company Pty Ltd Melbourne October 1995

Report examines the preconditions for the development of a successful online services industry in Australia. The aim is to assist those making investment decisions and those involved in making government policy.

Tucker, G. ***Implications of the Use of Digital Cash for Banking Law, Privacy and Security, and Law Enforcement*****, Presented at Colloquium at National Computer Board, Singapore, 1996**

Discusses the impact of electronic payment systems on Australian banking law and raises a number of questions, including how to determine when value is passed, who will be responsible when electronic payments are forged. Raises the issue of the potential conflict of laws when electronic transactions cross national, state or territory boundaries and becomes subject to different legal regimes. These issues would normally be dealt with by the terms of any contractual provision of the relevant conflict of trade laws.

Outlines specific privacy issues including the collection and storage of electronic payments data and the pooling or matching of this data; the ability to conduct surveillance on the payments habits of individuals as they go about their daily lives.

Four major implications for law enforcement are identified, namely:

- movement of illegal funds;
- traceability of fund movements;
- counterfeiting; and
- regulation of the systems.

Observes that underlying the concerns of law enforcement is the desire to be able to trace the flow of funds. This is only possible to a limited extent in the current cash system as even legislative measures do not require reports of cash transactions below $A10,000.

It is of concern that one response may be to attempt to make all transactions/transfers traceable. This represents a significant shift from the current environment and one which may not be acceptable. The paper argues that perhaps one response is to monitor the incoming payment systems closely, including their potential uses, and their penetration into the marketplace.

http://www.ncb.gov.sg/nii/96scan5/gt2.html#p1

Rose, A, *Electronic Commerce and the Law Free Zone - The Limitations of the Law*, **Speech to the Australian Securities Commission Conference on Electronic Commerce, Sydney 4-5 February 1997.**

Paper discusses the challenges relating to regulation of electronic commerce in an international context and against the backdrop of technological and commercial developments. Looks at how the current law copes with electronic commerce and some solutions to problems.

Willis, A, *Legal Issues in Electronic Commerce,* **Paper presented at the IPAA/IIR Conference, Rydges Lakeside 30 May 1996.**

Paper briefly examines a number of areas of law which become relevant in electronic commerce including contracts, Trade Marks and domain names, Trade Practices Act, Fair Trading Acts and Misrepresentations, Negligence, Banking and Currency Transfer Laws, Customs Duties, Excises and taxes, GATT, Copyright, Privacy and confidentiality, evidentiary issues, computer crime legislation, and other miscellaneous laws, such as the Archives Act.

1.2 International Material

1.2.1 Government Reports

Financial Issues Working Group of the European Commission, *Electronic Money in the United States: Current Status, Prospects and Major Issues,* 1996

Based on a fact finding mission to assess the current status of various initiatives aiming to facilitate financial transactions for electronic commerce.

Presents main findings of the mission, including the status of various standardisation initiatives and electronic money innovations.

Discusses various approaches to security-related issues of privacy, message integrity, authentication and interoperability. The Secure Electronic Transaction (SET) protocol and the Joint Electronic Payment Initiative (JEPI) are examined, as well as other initiatives aiming to promote standardisation and interoperability in Internet banking.

1.2.2 Research/Academic Reports

Bowen, B. Digital Signatures: Are They Less Certain Than You Think, *Sunworld Online*, May 1996

Discusses the impact of digital signature technology on the growth of Internet based communication and commerce. Yet, argues that from a legal perspective electronic documents violate some of the core characteristics defining a legally binding document.

Outlines the four legal presumptions that make widespread reliance on digital signatures problematic; these being:

- the legal definition of a signature;
- legal documents have to be in writing;
- documents have to be original; and
- various rules of evidence vary from state to state.

The three states, including Utah, that have enacted digital signature statutes are discussed. California passed a limited, vague bill in 1995 stating that the State of California will accept digital signatures, but says little regarding private transactions. Virginia and Georgia have introduced statutes loosely modelled on Utah; and Florida and Arizona are currently working on similar legislation.

Argues that the Utah statute is not very flexible. It is overly specific regarding how signatures must be administered and should have permitted more decisions to be made administratively.

Under the Utah law, there is also the issue of consumer liability for the certificate authorities. There are at least three classes of persons to whom a certificate authority may be liable: a client, a third party that is harmed, and the party impersonated by a client.

Concludes that even if a majority of states do enact similar legislation it may not settle the issues. Most transactions in the US are interstate, so if two states have different rules difficulties will arise. Until there is some sort of national uniformity problems will remain.

http://www.sun.com/sunworldonline/swol-05-1996/swol-05-lawnet.html

Cornwall Stodart, 1996 The Internet: Legal Pitfalls for Uses and Providers, *Client Information Bulletin*, Cornwall Stodart, December

Outlines some of the legal issues that could arise for users of the Internet, and more specifically, Internet Service Providers. Includes the common law issues of privacy, copyright, defamation and statutory regulation.

Discusses the issues of misleading and deceptive conduct on the Internet pursuant to the *Trade Practices Act*. The two aspects of this issue covered are:

- an author of material that is deemed to be misleading or deceptive may be liable under the TPA if it is published on the Internet, just as if the material were published in any other way. An ISP might also be liable for allowing the misleading material to be put on the Internet via its service;
- misleading or deceptive use of a domain name might also breach the TPA.

Also discusses the issue of liability of businesses or companies for the actions of employees.

Crede, A. 'Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet', *Journal of Computer Mediated Communications (JCMC)*, Vol 1, Issue 3

Examines the current initiatives being taken in establishing electronic payment systems for the Internet.

The paper suggests that while approximately 85-90 percent of business payments of monetary value will be processed electronically, less than 10 percent of these will be handled in this way, due to four related factors:

- proprietary closed networks were developed by banks to handle large and increasingly internationally based payment systems;
- large value payments are increasingly associated with foreign exchange and global securities transactions, thereby divorced from underlying world trade;
- large value payment systems are not cost-effective for small value payments; and
- paper-based, non-automated payment systems remain an accepted business practice for varying institutional reasons.

The paper suggests that the creation of an Internet electronic payment system will provide opportunities for the creation of completely new sets of global and national trading relationships. The Internet offers the possibility of an 'open systems' payment and settlement which operates in parallel to existing more traditional bank-based networks, and which is particularly suited to meet the currently unsatisfied requirements for processing low value payments electronically. However, the institutional framework to exploit these opportunities does not yet exist. Regulatory and policy issues will need to be addressed in order that full advantage can be taken of the new types of commerce which could emerge.

The paper examines the role of payment systems in the economy and their role in respect to global trade and investment. It also reviews the various existing payment systems and concludes that a cost effective and efficient electronic means for small value payments has yet to be established on a universal global basis, in particular for cross-border payments.

Current developments in the expansion of the Internet as well as other broadly based on-line services and the efforts which have been made to create an environment for electronic commerce. Policy and regulatory issues are also examined briefly.

The development of payment clearing systems is discussed in terms of how companies are attempting to overcome the security issues involved in handling payments on the Internet.

Commercial issues raised in the paper include the implications that Internet payments will have for Anglo-Saxon contract law. The law attaches great importance to the existence of an offer and acceptance, as evidence that the parties to an asserted contract have in fact agreed.

http://shum.huji.ac.il/kc,c/vol1/issue3/crede.html

Cross Industry Working Team, 1995, *Electronic Commerce in the NII*, Reston, VA: Corporation for National Research Initiatives, 1995.

A White Paper produced by the Cross Industry Working Team, this document discusses critical technical issues that, if properly addressed, can guide the evolution of electronic commerce. It recognises that numerous social, legal and regulatory issues must also be addressed if the potential of electronic commerce is to be realised. Many of these are complex and must be dealt with for electronic commerce to realise its potential. These include finding acceptable methods for authentication and protection of information, accommodating the special needs of law enforcement and international transactions, and creating the requisite means, technological and otherwise, of settling disputes.

The paper is divided into five sections. It describes the advantages of electronic versus paper-based commerce and discusses several shortcomings of present electronic commerce systems. It goes on to describe the kinds of progress that will need to be made to overcome these deficiencies and create an electronic commerce infrastructure.

Three scenarios are presented to demonstrate the future electronic commerce infrastructure. The actual requirements of electronic commerce to facilitate such transactions are discussed including (a) the framework that must be in place; (b) the activities and functions that must be supported; and (c) the building blocks required to support these activities and functions.

These include requirements such as:

- maximum flexibility for innovation;
- information-intensive products;
- new revenue collection methods;
- legacy systems; and
- transaction devices.

The paper concludes that many existing business practices will be transformed as electronic commerce is developed and deployed. The National Information Infrastructure will enable new degrees of freedom in the relationship of buyers and sellers and will challenge well-established business practices and laws.

The electronic contract will link cash flows to the exchange of products, goods, and/or services rendered. It will spell out the conditions under which the cash exchanges are to be made and include the payment instructions. This may reduce the number of human actions needed to effect transactions, and make possible time reductions in the contracting process, changing traditional chains and practices of authority and responsibility.

A key requirement for electronic commerce is the need for confidentiality and security, since this area is a particularly attractive target for crime. Thus, a significant investment of time, attention and resources must be committed to the control and prevention of such serious threats as deception, fraud, embezzlement and money laundering. The tools and countermeasures available include encryption, passwords, biometrics, digital signatures, message authentication codes, tamper-proofing and dating. The problems and solutions for electronic commerce are not conceptually different than those for traditional commerce environments.

The paper concludes that a major issue raised by electronic commerce is its interaction with the nonelectronic world. Clearly, links between the electronic commerce world and our ordinary world must be built. The infrastructure must link older existing ways of conducting commerce with the newer electronic mechanisms. Parties in electronic commerce must be able to move seamlessly and transparently across both commerce systems. For many purposes, payment received electronically must be convertible to real paper cash, and paper cash should be easily convertible to digital form. Similarly, participants in an efficient economy must have the flexibility to do their business in the ways that satisfy their individual needs and desires.

http://www.cnri.reston.va.us:3000/XIWT/documents/ECommPaper.html#Introduction

Drake, W. ed. *The New Information Infrastructure: Strategies for US Policy*, Twentieth Century Fund Press, New York, 1995

Many of the research papers examining the US National Information Infrastructure (NII) and the related topics of electronic commerce, content regulation etc claim that the fragmented and diverse policy making procedures of the US will impact on the 'information superhighway'.

The publication examines current policy developments in the US regarding telecommunications and the NII. The fragmented American telecommunications policymaking apparatus, which divides authority over the issues among a wide variety of institutions is surveyed. It is argued that this longstanding pattern of (dis)organisation is increasingly antiquated and inadequate to the task of formulating comprehensive and coherent national strategies for the NII.

It is argued that the federal government must move quickly to rationalise the lines of authority. The shifts in technology and the market brought on by the emergence of the global information economy are recognised, but not complemented by changes in the policy process. It is concluded that there is a clear and compelling need for substantial reform.

Froomkin, M. 'Flood Control on the Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases', ***Journal of Law and Commerce*****, 1996**

Argues that the introduction of electronic commerce will bring with it unprecedented opportunities for the profiling of individual habits. Most consumers may find that their only practicable defence against profiling and data mining is to transact anonymously; as a result, the legal status of anonymous communication will become increasingly important.

Discusses the legal status of anonymous speech and anonymous digital cash. Also describes several of the most popular varieties of digital cash, including Mondex and DigiCash, and compares their differing implications for the user's personal privacy.

http://www.ssrn.com/Cyberlaw/lawpaper.html

Hart, K. US touts duty-free Internet, ***Communications Week International*****, Issue 175, 25 November 1996.**

Discusses the US proposal to declare the Internet a global duty-free zone for all electronic goods and services. The policy, designed to pre-empt any attempts to impose customs duties or other new Net taxes, will apply to all electronic items and services purchased across the Internet in the US and abroad. Under the proposal, only goods and services bought and delivered electronically would be exempt from tariffs and taxes. Material items such as modem purchased electronically will not be included.

The article claims that the proposal is likely to face resistance from local state governments and other countries that fear electronic commerce over the Internet will erode their current revenue base. However, free trade enthusiasts have called the move a "giant leap towards the creation of a stable, predictable market for global electronic commerce".

Foreshadows the development of a white paper on this issue and others including policy guidelines in areas such as data privacy, electronic payment, intellectual property rights and technical standards.

Hughes, G (Ed) ***Essays on Computer Law*****, Longman Cheshire, 1990**

This is a legal text which examines the broad range of laws which have a bearing in the area of computer technology.

Although mainly dealing with software and intellectual property issues, it contains some discussion of issues relating to electronic documents, privacy, security, and other matters.

Information Infrastructure Task Force (IITF), 1994, ***Electronic Commerce and the NII: Draft for Public Comment*****, IITF.**

Discusses the benefits of and the public interest in promoting electronic commerce. Claims that an advanced NII which supports electronic commerce applications will help US companies increase productivity by enabling rapid business transactions, data and information exchanges, and organisational changes. Through the ability to handle tremendous volumes of transactions and the ability to amass, analyse and control large quantities of specialised data, organisations will be able to improve efficiency and accuracy, and reduce costs, while providing faster, more reliable, and more convenient services.

The paper provides examples of how companies in several industries have experienced the benefits and realised the need to use electronic commerce. Also discusses the various federal government initiatives in the US that are further facilitating the uptake of electronic commerce. These include the work of the National Institute of Standards and Technology (NIST) which assists the private sector with the development of the technical underpinnings for interoperability, and works to coordinate and facilitate the standards process. NIST has also established an Electronic Commerce Integration Facility (ECIF) which:

- serves as a technology transfer centre to assist government and industry in the deployment of electronic commerce applications;
- demonstrates, through prototypes and pilots, generic open systems implementations of electronic commerce; and
- contributes to the development and testing of electronic commerce applications and infrastructure services.

There are a also a number of private sector activities that are developing and implementing electronic commerce applications for the NII. These include CommerceNet and the Enterprise Integration Network (EINet), both of which are discussed in the article.

The issues that the paper raises as needing resolution before electronic commerce becomes widely used are:

- security issues. There are clear requirements for authentication of the source of a transaction, verification of the integrity of the transaction, prevention of the disclosure of the transaction to unauthorised users, and verification of the receipt of the transaction by the intended trading partner.
- interoperation issues. Electronic commerce application will require the interoperation of communications, data management, and security services

The paper examines what role government should take to ensure the widespread use of electronic commerce. It poses the questions of what incentives can be provided so that workers will share in the benefits of electronic commerce? How can government and industry establish realistic business cases and success stories to encourage potential users and providers of electronic commerce hardware, software and services? And, how can government and industry ensure that electronic commerce will be viewed positively?

http://iitfcat.nist.gov:94/doc/Electronic_Commerce.html

Interactive Services Association, *Logging on the Cyberspace Tax Policy,* White Paper, 1996.

Prepared to initiate discussions with the nation's tax policymakers about state and local transaction tax issues affecting the Internet and online services industry.

Makes a number of recommendations, arguing that state tax rules should be uniform, fair, certain and administratively simple. They should not discriminate against electronic commerce of Internet-based transactions, and they should not hinder economic growth. The development of tax rules applicable to the Industry should be pursued with deliberation to ensure the achievement of these goals. Specifically it is the position of the ISA White Paper Task Force that, if the states adopt a tax system applicable to the Industry, that the system should call for the following:

- adoption of uniform definitions among the states;
- establishment of a single rate, within each state, of any applicable tax;
- recognition of the fact that the only type of tax that can be applied effectively to purchases made over the Internet or proprietary subscriber networks will be a tax on the purchaser with respect to the purchase transaction itself; and
- attribution, to the extent possible, of any applicable tax to the state into which the states are billed.

Concludes that the growth of the Internet should not be impeded either by expansive interpretation of existing tax laws or the imposition of new taxes on the industry.

http://www.isa.net/about/releases/taxwhpap.html

Johnson, D. & Post, D. *And How Shall the Net Be Governed: A Meditation on the Relative Virtues of Decentralised, Emergent Law,* 1995

Outlines four basic competing models for the governance of the Internet:

- existing territorial sovereigns can seek to extend their jurisdiction, and to amend their laws as necessary, to attempt to govern all actions on the net that have substantial impacts on their citizenry;
- sovereigns can enter into multi-lateral international agreements to establish new and uniform rules specifically applicable to conduct on the Internet;
- a new international organisation can attempt to establish new rules and new means of enforcing those rules and of holding those who make the rules accountable to appropriate constituencies; and
- defacto rules may emerge.

Examines the potential of applying each of these models to the Internet. The non-geographic character of the Internet makes it difficult to apply current, territorially based rules to online activities. Yet, while this might be addressed by means of creating a uniform law of the Internet by treaty, this model of governance also has many problems. The treaty process is slow and it is not clear that agreement could be obtained from all nations. Even the possibility of creating a new international organisation whose mission was merely to establish and enforce basic rules for the Internet would be problematic. How could domination of such a body by a single group or nation be prevented?

The paper claims that workable, accepted rules to govern the new trade in ideas and services can largely be developed without any massive new legislative agenda or rulemaking. It concludes that the law of the Internet has emerged, and can continue to emerge, from the voluntary adherence of large numbers of network administrators to basic rules of law (and dispute resolution systems to adjudicate the inevitable inter-network disputes).

http://www.cli.org/emdraft.html

Katsch, M E: *Law in a Digital World*, New York OUP, 1995

Reviews several areas in which the growth of information technology is likely to change law as a social institution, with particular focus on how participants in legal processes will interact with new technology.

Knight, P and Fitzsimons, J: ***The Legal Environment of Computing*** **Addison Wesley, 1990**

This legal text reviews various areas of law which relate to computers and computer technology. It also contains some discussion of contractual, privacy and security issues.

McKnight, L. Solomon, R. et al. ***Information Security for Electronic Commerce on the Internet: The Need for a New Policy and New Research*****, Presented at MIT Workshop on Internet Economics, March 1995.**

Drawing on workshop discussions, the paper argues that an intensified dialogue among industry, academia, government and the public on information security and electronic commerce issues are clearly needed.

Information security is compromised if federal policies and corporate initiatives ignore user requirements and the basic principles of Internet economics. This in turn may limit market acceptance of new research, services, applications, and technologies. For example, unintended results from ill-formed federal laws may severely limit economic benefits gained from federally sponsored research that has created the Internet. Furthermore, proprietary systems resulting from enhanced security measures may lead to a lack of interoperability that further compromises prospects for society to realise the benefits. Argues that many of these problems can be avoided by an open policy making process that is informed by collaborative research and development activities.

Discusses current US information security policy, and legislative efforts regarding encryption technologies.

Maps current research activities in the US regarding information security and electronic commerce. But the full potential of such research will not be recognised if the government's actions continue to be heavily influenced by enforcement and intelligence agencies. Argues that the interests of many researchers, civil liberty groups and leaders in the information technology industry should be incorporated into the government decision making process.

http;//www.press.umich.edu:80/jep/works/McKniSecur.html

Muscovitch, Z. *Taxation of Internet Commerce*, International Law Students Association, 26 April, 1996

Analyses how commerce and banking will be affected by the Internet, with particular attention to the existing international frameworks for taxation.

While the emergence of commercial transactions over the Internet will require adaptations in international trade laws, the paper argues that an issue that must not be overlooked by governments is the issue of how to adapt regulatory frameworks to ensure electronic transactions can be taxed. Otherwise, governments will face a significant decrease in their tax revenues, as more commerce takes place over the Internet.

Discusses the effect of the Internet on particular aspects of taxation laws. Existing regulatory frameworks are likely to be incapable of adequately taxing electronic transactions, and must be adapted. Argues that the task for governments is to attempt to fit Internet transactions into existing rules of taxation and where this is impossible, attempt to adapt and amend the rules in order to catch Internet transactions.

Covers the applicability of existing reporting laws, including *the US Electronic Funds Transfer Act* which applies not only to banks but to any person who holds an account belonging to a consumer or who issues an access device and agrees with a consumer to provide electronic funds transfer.

Examines how cross-border shopping by consumers will be affected by Internet commerce. As the Internet evolves and becomes more accepted as a commercial trade route, companies on the Internet will have to abide by their own domestic sales tax law.

Considers the impact of Internet transactions on banking, money laundering, bank secrecy laws and the question of whether the downloading of software will generate sales income or royalty income. Computer software can be viewed as either goods, or as a service or intellectual property thereby creating a characterisation problem.

http://www2.magmacom.com/~dbell/tax.htm

Neuman, C. Medvinsky, G. *NetCheque, NetCash, and the Characteristics of Internet Payment Services*, Presented at MIT Workshop on Internet Economics, March 1995

Secure methods of payment are needed before we will see widespread commercial use of the Internet. Recently proposed and implemented payment methods follow one of three models: electronic current, credit-debit, and secure credit card transactions. These three payment models are outlined.

NetCheque and NetCash, two payment systems developed at the Information Sciences Institute of the University of Southern California are discussed here. The benefits and drawbacks of alternative approaches are covered, and how the different methods can be used together to provide financial infrastructure for the Internet is described.

Perritt, H. 'Cyberpayment Infrastructure', *Journal of Online Law*, 1996,

Discusses how public key encryption can be used to develop a reliable and secure system to handle payment for goods and services purchased over the Internet.

Any payment system must meet certain requirements: (i) merchants can depend on it to be paid; (ii) consumers have access to the means of payment through intermediaries like certificate authorities; (iii) intermediaries understand their responsibilities and risks; and (iv) existing financial institutions understand their responsibilities in the world of non-paper-based financial instruments. It argues that much of what is necessary can be accomplished within today's legal framework without the need for new laws.

Examines the variety of payment systems possible and the legal requirements to cover these. The basic requirements for the legal infrastructure include:

- merchants must be reasonably secure against forgery and reasonably confident that credit card charges and other payment tokens will be honoured upstream in the financial system;
- consumers must be able to obtain access to the means of presenting credit card authorisations and payment tokens in forms acceptable to merchants. This probably requires the existence of certificate authorities readily accessible to consumers;
- certificate authorities must understand their legal responsibilities so that they can insure against or otherwise provide for risk; and

- banks and other financial institutions must understand their responsibilities. This is most notable because banks have been conditioned by a commercial culture with relatively precise and detailed specifications for presentment, acceptance, and dishonour or more conventional financial institutions such as personal cheques.

It is argued that all of these requirements can be satisfied without the erection of major new legal institutions or the creation of significant new areas of substantive positive law. The credit card payment system accounts for billions of dollars each year, and it is almost entirely regulated by private contracts among the several major credit card systems: Visa, Mastercard, American Express, and Diner's Club.

The paper considers the legal framework in four major categories: banking regulation; duties and limitations of liability of new intermediaries such as certificate authorities; allocation of the risk of fraud, unauthorised access, and trafficking in stolen keys or forged tokens; and jurisdictional and enforcement issues arising from the international character of the information infrastructure.

A regulatory system similar to that applied to banking might seem suitable for new Internet payment systems. However, the paper argues, when it is considered that most payment systems encountered by ordinary consumers - aside from personal cheques - occur largely outside this framework such regulation is questionable. The example of American Express is provided in the paper. American Express is not subject to banking regulation, yet it is the hum of all the electronic commerce that flows though American Express travellers' cheques and credit card payments.

The role of new intermediaries is also examined. With the introduction of public key encryption, the security of payment systems is being ensured. Public key encryption permits anyone in the world to verify with almost complete certainty the authenticity of the signature and the fact that the message contents have not been altered. Such verification uses a public key corresponding to the private key used to sign the original message. Public keys are made available through special databases called certificate authorities (Cas) which vouch for the relationship between a particular public key and its purported owner. A CA is a kind of insurer of the authenticity of a payment token, but unless new laws to define the responsibilities and rights of CAs emerge, it is unlikely that an adequate number of them will emerge.

The paper claims that the Utah Digital Signature Act and the Draft Digital Signature Guidelines being produced by the American Bar Association are both attempting to address this issue. Both provide default rules and safe havens for CAs and make it clear what consumers and merchants can expect of them.

Jurisdictional issues are also briefly examined. The paper argues that in the short term, the best hope to regulate Internet commerce is the development and use of specialised international arbitration systems drawing from the largely successful experience in commercial international arbitration, and on the remarkably complete governance systems represented by bank cheque clearing and funds transfer systems. The consumer protection aspect of this proposal can be modelled on well established agreements under credit card subscriber contracts represented by American Express, Diner's club, the Visa and Mastercard systems, as well as others.

http://warthog.cc.wm.edu/law/publications/jol/perritt.html

Post, D. *Law and Borders - The Rise of Law in Cyberspace,* 1995

Begins from the premise that the rise of the global computer network is destroying the link between geographical location and (i) the power of local governments to assert control over online behaviour; (ii) the effects of online behaviour on individuals or things; (iii) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (iv) the ability of physical location to give notice of which sets of rules apply.

Argues that may of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by conceiving of 'Cyberspace' as a distinct place for purposes of legal analysis by recognising a legally significant border between 'Cyberspace' and the 'real world'. When approaching the issue this way, the paper argues that many opportunities to clarify and simplify the rules applicable to online transactions become available. The paper uses the examples of copyright, defamation, fraud and antitrust to illustrate this point.

http://www.cli.org/X0025_LBFIN.htm

Reagle, J. & Leida, B. *Electronic Commerce Protocols and Competitive Strategies: Credit Card Transactions over the Internet,* 1996

Discusses the development of standards and protocols by standards bodies and the major players interested in or involved in electronic commerce.

Standards are currently being developed by bodies such as the American National Standards Institute (ANSI), the International Telecommunications Union (ITU) and the International Standards Organisation (ISO). Companies are also forming consortiums to develop their own protocols. Examples of these include the W3C and CommerceNet.

Discussion is limited to those protocols that shall provide security towards extending traditional credit card payment systems to the Internet.

http://web.mit.edu/reagle/www/career/stuff/compete/toc.html

Ritter, J.B. *Global Law for Commercial Digital Products: Work in Progress at the United Nations and in United States Commercial Law,* 1996

Examines recent efforts at the United Nations and in the United States to define the legal structures for electronic commerce.

Efforts of the Working Party on Facilitation of International Trade Procedures of the United Nations Economic Commission for Europe (WP.4) are outlined, particularly the development of standards for the global use of Electronic Data Interchange (EDI). The resulting standards, known as UN/EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) have also been adopted by the International Standards Organisation.

Complementing the work on EDI are law reform efforts within both the US and the United Nations Commission on International Trade Law (UNCITRAL). Efforts are being made to ensure that legal structures can equally recognise paper-based or electronic messages. UNCITRAL has recently finalised a Model Law on EDI Transactions which, if adopted, will provide to nations a means of confirming by statute that the law will accommodate electronic commercial documents.

The paper also outlines the emergence of digital authentication procedures for electronic transmissions. Both in the United States and Europe the prevailing trend is toward the view that electronic digital products representing purchase orders, government reports and similar communications will not be sufficiently authentic without the certification of trusted third parties.

It concludes that the technologies of the Internet will never be fully sufficient to provide complete protection for digital products, despite the emergence of certification authorities. The capability to seek recourse against wrong-doers must exist through conventions and laws made at both the international and national levels.

Ritter, G. 1994, *Removing the Legal Barriers to Electronic Commerce*, Paper presented at the United Nations Summit on Trade Efficiency, October.

Argues that restructuring the legal frameworks to remove barriers and fully accommodate electronic commerce practices is essential in order to realise the full potential of trade facilitation. It is not simply a task of making a few changes in administrative rules; legal facilitation is the challenge of reforming the interconnected legal systems of the world to fully recognise and accommodate electronic commercial practices.

The legal structures that govern trade include commercial laws, such as those that govern sales, transport agreements, banking transactions and insurance. Administrative laws are also significant. These structures exist at each level of trade. They are also largely national in nature. The emerging regional structures of the EU and North America, including directives and provisions regarding many aspects of trade. As well, a large number of international conventions, treaties and conferences to which many nations have become signatories exist.

Against this collection of statutes, regulations and international instruments, the commercial and administrative players much define the elements of each aspect of the trade process. In many instances, the existing legal structure, including established commercial practices, require writings, signatures and paper documents for reasons that can no longer be justified in the emerging information age. In other instances, the changes produced by electronic commerce require new rules.

In the absence of giving full validity to electronic commerce under each legal contract and legal instrument, the potential of electronic commerce cannot be realised. Delivering the legal tools which provide a framework for the full legal validity of electronic commerce is an essential priority.

The paper discusses the work of the United Nations Commission on International Trade Law (UNCITRAL) with regard to Electronic Data Interchange (EDI). It argues that the work of the Working Party will assist in the adaptation of the legal structures which affect international trade to electronic commercial practices. The work includes:

- promoting the use of uniform or harmonised commercial interchange agreements and practices across trading sectors, through which the more formal legal structures can then find support;
- harmonising reforms to existing commercial laws and international instruments to remove existing barriers and introduce appropriate laws that recognise electronic commercial practices; and
- developing model administrative laws for national adoption.

It concludes that removing the legal barriers to electronic commerce will establish governments and administrative agencies as full partners with the commercial sector in advancing trade facilitation and achieving trade efficiency.

http://eclips.osc.edu/elcips/barriers-to-ecommerce.html

Rose, L; *Netlaw; Your Rights in the Online World;* Berkeley, Osborne McGraw-Hill (1995)

Discusses the following legal issues relevant to the Internet and on-line services:

- Freedom, Censorship and control of the Online System;
- Contracts and Commercial arrangements;
- Owning and Using Online Property;
- Dangers and responsibilities in the Online world;
- privacy
- Crime and the Online system;
- Searches and Seizures;
- Adult material and themes.

Rubin, H., Fraser, L., & Smith, M. 1996, US and International Law Aspects of the Internet: Fitting Square Pegs into Round Holes*, International Journal of Law and Information Technology*, Vol 3. No.2. 1996

Introduces the problems of aligning US and international law to the Internet, not because the Internet exists in a legal vacuum, but rather because a plethora of legal regimes that either cannot be adequately applied or enforced govern the Internet, and the Internet community increasingly is subject to vague and, frequently, contradictory requirements.

Argues that because the US legal system tends to favour no regulation, self-regulation or, if necessary, state regulation (with some significant exceptions) it is likely that the US system will produce limited and reluctant piecemeal legislation. Continental and other civil law systems, by contrast, tend to embrace comprehensive legislative solutions.

While not suggesting that one approach is better than the other, it is argued that only specifically targeted and comprehensive federal Internet legislation, preferably buttressed by multilateral conventions, can hope to resolve some of the legal problems posed by the Internet.

Discusses the 'smorgasbord' of federal laws which provide very specific and limited privacy protection in the US, claiming that the lack of privacy protection has prompted several trade disputes with the European Union. During the Uruguay Round of the GATT, the US rejected European proposals for comprehensive information flow restrictions.

The issue of contracts completed on the Internet is also examined. Discusses the questions of whether there is a contract between an online user and the service, and how service providers could be bound to particular terms

and conditions. A meaningful and comprehensive cybercontract regime would have to clarify which statements constitute enforceable promises and what constitutes an offer potentially binding the offerer.

Trade regulation issues are discussed, particularly with reference to US export controls. Jurisdictional issues are also raised. Different countries have different laws regarding intellectual property, property, libel, banking, securities and other areas that are affected by Internet transmission. The paper argues that the uniqueness of the Internet merits an international convention settling the jurisdictional basis of a country's ability to (i) prescribe means of Internet conduct; (ii) adjudicate Internet related disputes; (iii) enforce Internet regulations. The Internet's defiance of sovereignty and nationality makes each country equally vulnerable. Therefore, conduct and the effects of conduct might well constitute the most appropriate basis for an Internet jurisdiction convention.

Concludes that if no comprehensive or internationally coordinated approach to any facet of the Internet emerges, not all will be lost. Cyberlaw may ultimately mimic the development of public international law, and likely will be based on a combination of multilateral and bilateral agreements; and, just as public international law is created through custom and general principles common to the world's major legal systems, certain aspects of cyberlaw may develop through self regulation by the Internet community and osmosis with real law.

Timmers, P. ***Electronic Commerce - An Introduction***

This paper provides a brief introduction to electronic commerce. It discusses the nature of electronic commerce, considers its scope and impact and outlines several examples. It argues that electronic commerce is a means of enabling and supporting commerce on a global scale. It enables companies to be more efficient and flexible in their internal organisations, to work more closely to suppliers, and to be more responsive to the needs and expectations of their customers.

Some of the supplier opportunities and customer benefits are outlined in the paper. These include:

- improved competitiveness/ quality of service;
- mass customisation/personalised products and services;
- shorten or eradicate supply chains/rapid response to needs;
- substantial cost saving/substantial price reductions;
- novel business opportunities/new products and services.

The paper also gives a number of examples of electronic commerce in a wide range of industry sectors and a wide range of application areas.

It concludes that there are a number of issues that must be resolved at the global level - the actors with responsibility for resolving the issues and promoting electronic commerce must include multi-national bodies. Equally, there is a role for national governments in removing national barriers and ensuring fair competition, and for sector representatives in promoting awareness and best practice. Finally, there are obvious roles for technology suppliers, user companies, and individual consumers in enabling, adopting and exploiting electronic commerce.

The G7 initiative "A Global Marketplace for SMEs" is outlined. The initiative has the overall objective of facilitating increased competitiveness and participation in global trade for SMEs by exploiting the opportunities offered by the development of the global information society. Specific objectives are to:

- contribute to the development of a global electronic environment for the open and non-discriminatory exchange of information; and
- expand global electronic commerce in order to enable enterprises to carry out their business operations and management more effectively and more profitably.

The paper concludes that despite a number of open issues that are yet to be resolved, electronic commerce is already happening. It is essentially a 'bottom up' revolution. Companies are establishing a basic electronic presence on a global network and are gradually becoming more sophisticated in their use of the technologies.

http://www.cordis.lu.esprit/src/ecomint.htm

Walden, I. ***Trading in Cyberspace: The Legal Frontier,*** **Prepared for the EITC Conference, 26 November 1996.**

Provides a scenario of an individual consumer purchasing products over the Internet and paying for such goods through an online payment service provider. The scenario raises a number of legal issues that are subsequently dealt with in the paper.

Discusses the importance of defining which laws are applicable to a transaction and in which legal jurisdiction any dispute will be heard. Claims that jurisdiction or 'conflict of law' issues are not altered by the use of electronic commerce, they are the same for any long-distance contract, except to the extent to which the range and complexity of reconciling the potential jurisdictions can increase when using international networks, such as the Internet.

Examines the legal issues raised when establishing contractual relationships for the purchase of goods and services over the Internet, including the questions of what is a valid contract; who the contract been formed with (the supplier or electronic retailer); and what terms are applicable.

Wright, B; *The Law of Electronic Commerce, EDI, E-mail and Internet.* Little Brown & Co Dallas Texas, September 1995.

Discusses the legality of electronic contracts and other business transactions. Includes a discussion of the law of signatures, records, evidence, liability and privacy, electronic cash, Internet, digital signatures and recent court decisions.

Wright, B; *Alternatives for Electronic Signing*

The article considers the practical features of two alternative methods of signing electronic documents. These are smart card based public Key cryptography and PenOp, a pen computer technology that captures handwritten autographs.

http://infohaus.com/access/by-seller/Benjamin_Wright

Wright, B; *EDI Law*

The article examines the law of Electronic data interchange (EDI), a form of electronic messaging used by business and government to make purchases, payments, and other routine transactions. The article explains EDI technology, considers the requirement that EDI be signed, analyses the need for an EDI trading partner agreement, offers ideas on the recording of EDI (particularly for tax purposes), and highlights the issues addressed in an EDI service provider agreement.

http://infohaus.com/access/by-seller/Benjamin_Wright

Wright, B; *Legal Identity*

The extract discusses legal identity and signatures from a philosophical, cultural perspective.

http://infohaus.com/access/by-seller/Benjamin_Wright

Wright, B; *Model for EDI Tax Records*

The article discusses the Model Policy for Recording EDI Invoices, which is an approach to the creation and storage of invoices to comply with taxation regimes.

http://infohaus.com/access/by-seller/Benjamin_Wright

Wright, B; *The Verdict on Plaintext Signatures; They're Legal*

The article examines the general law requirements of signatures, and states that the law does not require a signature to be secure to be legally effective, which has positive consequences for email and electronic commerce generally.

http://infohaus.com/access/by-seller/Benjamin_Wright

Wright, B. *Eggs in Baskets: Distributing the Risk of Electronic Signatures*. 1996

Discusses the risks associated with the use of electronic signatures. The signing of a document is a social event, not a scientific one, and as a result the bonding of a document to an individual is never a perfectly reliable process. Even with the introduction of scientific measures, such as biometrics, the signing of a document involves risk.

The paper covers the different strategies of signing contracts or documents. These include the traditional paper and ink strategy, using public key cryptography, and the use of digital signatures.

The article addresses the alternative strategies for dealing with the risks associated with electronic signatures. Examines one strategy, which uses biometrics to spread the risks so that no particular feature of the signing process, such as a private key, is highly important.

The use of biometrics is examined, including the risks associated with using such a technology.

http://infohaus.com/access/by-seller/Benjamin_Wright

2. Jurisdictional Issues

2.1 Jurisdiction

Halsbury's Laws of Australia Volume 14 Title 215 *Foreign Relations* Christine M Chinkin

The title Foreign Relations sets out the general principles of public international law and its application by Australia, including sources of international law and treaties.

The concept of jurisdiction in international law refers to the competence of a state to prescribe and apply its laws and regulations with respect to natural and legal entities. 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 in that 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: *Lotus Case (France v Turkey) 1927 PCIJ ser A No10 (Judgment of 7 Sept)* Jurisdiction is both criminal and civil.

2.2 International Law and Treaties

Halsbury's Laws of Australia Vol 27 Title 420 *Trade and Commerce - International Trade* Simon Fisher and Anne Hurley (1995)

The title Trade and Commerce - International Trade deals with international trade and investment, including international agreements, financing and transactional aspects.

As a general rule, international trade treaties negotiated by Australia with other countries do not bind Australian traders or foreign traders or create enforceable rights or duties for Australian traders or foreign traders in the absence of incorporation into domestic law.

2.2.1 Trade Related Agreements to Which Australia is a Party-

Australia has been active in negotiating treaties and as at 31 December 1994, Australia had entered into (or 'inherited') 2289 treaties of which 1303 were bilateral and 986 were multilateral. Some significant treaties are as follows:

- **Marrakesh Agreement establishing the World Trade Organisation** (Marrakesh 15 April 1994). Aims to increase the participation of developing countries in international trade, to reduce tariffs, and other barriers to trade and to eliminate discriminatory treatment in international trade relations.
- **General Agreement on Tariffs and Trade 1947 and 1994**

  GATT 1947 was restructured and amended by the Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations. GATT 1947 as amended, rectified or modified now forms part of the General Agreement on Tariffs and Trade 1994 which is part of the Marrakesh Agreement establishing the World Trade Organisation 1994.
- **The General Agreement on Trade in Services 1994**. A multilateral agreement which aims to promote the growth and development of the world economy through the expansion and development of trade in services.
- **The Agreement on Trade Related Aspects of Intellectual Property Rights 1994**. Annexed to the Marrakesh Agreement. Recognises some key features of trade related aspects of intellectual property rights.
- **The Agreement on Subsidies and Countervailing Measures 1994**. Contained in the Marrakesh Agreement. Affects Australian Government assistance to Australian international traders in the form of subsidies.
- **Understanding on Rules and Procedures Governing the Settlement of Disputes 1994**. Annexed to the Marrakesh Agreement.

- **United Nations Convention on Contracts for the international sale of goods 1980.**
- **International Convention on the Settlement of Investment Disputes between States and Nationals of Other States** (ISCID Convention) 1965.
- **South Pacific Regional Trade and Economic Cooperation Agreement 1980** ('SPARTECA') was entered into between the governments of Australia, the Cook Islands, Fiji, Kiribatu, Nauru, NZ, Nive, PNG, Solomon Islands, Tonga, Tuvali and Western Samoa.
- **Australia New Zealand Closer Economic Relations Trade Agreement 1983** ('ANZCERTA'). Bilateral Trade Agreement between Australia and NZ created by treaty. Affects trade in goods and services between the two countries.
- **Australia-Japan Friendship and Cooperation Treaty 1976**. Embraces a wide range of human endeavour, with an emphasis on trade and economic matters.
- Bilateral Investment Treaties. Australia has negotiated many agreements with other States dealing with the reciprocal encouragement and protection of investment including China, Vietnam, Indonesia, Hong Kong.
- **Paris Convention for the Protection of Industrial Property 1883**

2.2.2 Trade Related Agreements to Which Australia is Not a Party-

- **Treaty of Amity and Cooperation in South-East Asia 1976** established the Association of South East Asian Nations ('ASEAN') for economic cooperation measures.
- **North American Free Trade Agreements 1992** ('NAFTA'). Establishes a free trade area in goods, services, and also deals with Intellectual Property.
- Agreements Establishing the **European Union**. The European Union is a supra-national union of 15 Western European nations. A number of treaties constitute the legal framework for the European Union, the principal of which are the Treaty of European Union 1992 ('the Maastricht Treaty') and the Treaty Establishing the European Community ('Treaty of Rome') 1957. The Treaty of Rome 1957 establishes a common market and an economic and monetary union.

2.2.3 International Law Reform

Australia has been an active participant in international legal initiatives, principally through its membership of the United Nations Conference on International Trade Law (UNCITRAL) and the Hague Conference on Private International Law. Australia also participates in the International Institute for the Unification of Private Law (Unidroit).

2.3 International Trade Transactions

United Nations Convention on Contracts for the International Sale of Goods Vienna, 11 April 1980

This convention applies only to business transactions which have a cross border element.

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.

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;

- 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.

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.

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:

(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

United Nations Commission on International Trade Law ('UNCITRAL'), Model Law on Electronic Commerce (1996)

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.

The Model Law, which has yet to be adopted, has been developed to facilitate electronic commerce, 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;

the recognition of data messages as having legal effect in certain circumstances.

2.3.1 The United States Framework for Global Electronic Commerce

The Clinton Administration has developed a draft policy for Global Electronic Commerce. through an interagency working group on Electronic Commerce. The Framework for Global Electronic Commerce is an important element in the Administrations agenda on trade and technology as it discusses the commercial implications of the Global Information Infrastructure (GII). 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.

2.3.2 Carriage of Goods and Other Issues in International Transactions

International trade transactions associated with the international sale of goods typically involve contracts of sale, carriage, insurance and finance. Sea carriage is essentially governed by the Carriage of Goods by Sea Act 1991 (Cth) and the Amended Hague Rules 1979 also known as the Visby Rules. 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.

2.4 Private International Law

Halsbury's Laws of Australia Vol 4 Title 85 *Conflicts of Laws* PE Nygh (1993)

The title Conflicts of Laws sets out the general principles of Australian private international law. The title explores the principles by which matters involving a conflict of laws between different legal systems are resolved and examines related questions involving the jurisdiction of courts and the application and enforceability of foreign laws and judgements of foreign courts.

Cross Border Civil Remedies, Report of the Australian Law Reform Commission, Commonwealth of Australia 1996.

Review of the civil remedies available under Australian law and under multilateral or bilateral instruments or arrangements to which Australia was or could be a party. The Commission was asked to report on the feasibility of the systematic development and reform of the law in relation to those remedies.

The Report contains a chapter dedicated to finance and electronic commerce, dealing with issues such as the central role of banks, financial markets, cross border banking issues, and finance law reform.

3. The Internet Transaction

3.1 The Underlying Contract

Contract Law in Australia, 3rd Edition (1996), Carter, JW; Harland, DJ; Butterworths, Australia.

This textbook outlines the general principles of contract law in Australia.

3.2 Evidentiary Issues

The Laws of Australia The Law Book Company Ltd Volume 16 Evidence Ch 16.6 *Computer Produced Evidence* Dr R A Brown (1996)

This title examines the rules of evidence as they relate to computer produced evidentiary material.

3.2.1 The Evidence Acts

As a general description, any computer produced material has the potential to be introduced into evidence, and such material naturally includes 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. Whether in any particular instance such material is capable of being admitted into evidence is dependent upon such legal factors peculiar to each jurisdiction.

Three fundamentally different approaches, the 'computer specific' approach, the 'business records' approach, and the Evidence Acts 1995 approach have been adopted to determine the admissibility of computer produced evidence in Australian legislation. The legislation is diverse. The computer specific approach employs legislative provisions that are specifically directed to the admissibility of computer produced evidence, (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).) while the business records approach sees computer produced evidence merely as one aspect of the general question of admissibility of business records (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.). Some jurisdictions have adopted both approaches simultaneously. The approach contained in the Commonwealth and New South Wales Evidence Acts 1995 (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.) is the most general of the three approaches, applying a statutory presumption as to the correct operation of devices and machines.

3.2.2 Legislation

Evidence Act 1977 (Qld), Evidence Act 1929 (SA),Evidence Act 1958 (Vic),. Evidence (Business Records) Interim Arrangements Act 1984 (NT), Evidence Act 1977 (Qld), Evidence Act 1929 (SA), Evidence Act 1910 (Tas), Evidence Act 1958 (Vic), Evidence Act 1995 (Cth); Evidence Act 1995 (NSW), Civil Evidence Act 1968 (UK).

3.3 Contractual Issues

The Laws of Australia The Law Book Company Ltd Vol 7 *Contract - General Principles* Title 7.2 Vitiating Factors John A Riordan (Ed) (1994)

The title examines the rules relating to formal requirements of contracts.

3.3.1 Formalities and the Statute of Frauds

Although there is no general formal requirement of writing in the law of contract, legislation makes it necessary for certain contracts to be evidenced by a written note or memorandum if they are to be enforceable by action.

These contracts constitute a heterogeneous group deriving from the requirements of England's Statute of Frauds 1677 (UK). In Australia, this group of contracts has been whittled away so that in most jurisdictions the only types of contract of any importance 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. Even contracts of guarantee need no longer be evidenced in writing in the ACT, NSW and SA. The position is not uniform. For example, it is still necessary for contracts regarding the sale of goods over a certain amount to be evidenced in writing if sued on in the NT, Tas and WA.

The statutes prescribing formal requirements may be divided into two categories: legislation derived from the Statute of Frauds 1677 (UK) and consumer protection legislation. Modern statutes aimed at consumer protection provide that certain types of contracts must be in writing. Examples 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.

3.3.2 Legislation

Statute of Frauds 1677 (UK), (US) Uniform Commercial Code.

3.4 Payment Mechanisms

3.4.1 Texts

Banking Law in Australia 2nd Edition Butterworths 1995 Alan L Tyree

This text deals with the law relating to banking and finance in Australia, including consumer banking, credit cards and consumer credit, electronic banking, negotiable instruments, cheques and international banking.

Halsbury's Laws of Australia Volume 2 ***Banking and Finance*** 1995 Alan L Tyree

The title deals with the law relating to banking and finance in Australia, including consumer banking, credit cards and consumer credit, electronic banking, negotiable instruments, cheques and international banking.

3.5 Legislation

Bills of Exchange Act 1909, Cheques and Payments Orders Act 1986

3.6 Codes and Standards

The Australian Banking Industry Ombudsman

Under the Terms of Reference, the Ombudsman is required and authorised to consider disputes relating to the provision within Australia of banking services by any member bank to any individual.

Code of Banking Practice

The purpose of the Code is to describe standards of good practice and service, to promote disclosure of information which is relevant and useful to customers, to promote informed and effective relationships between banks and customers and to require banks to have procedures for the resolution of disputes between banks and customers. A 'customer' under the Code is an individual who acquires a 'banking service' which is wholly and exclusively for his or her private or domestic use s 1.1.

Electronic Funds Transfer Code of Conduct

The Electronic Funds Transfer Code of Conduct 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, or which are intended to be so initiated. It governs the relationship between users and providers.

3.7 Articles

Alan L Tyree, 'Information Technology and World Trade', ***Journal of Banking and Finance Law and Practice.***

Explores the problems which accompany vastly increased communications facilities. Identifies challenges in areas as diverse as copyright, administrative law, commercial law, and the control of financial corporations.

Alan L Tyree, 'PINS and Signatures', ***Journal of Banking and Finance Law and Practice.***

Looks at the law relating to PINS and signatures. Bankers often compare the PIN to a signature on a cheque, but the law treats the two quite separately. It may be that the legal treatment of the PIN is more suitable to modern conditions.

Alan L Tyree, 'Virtual Cash: Payments over the Internet', ***Journal of Banking and Finance Law and Practice.***

Discusses payment mechanisms over the Internet, including digital cash and cheques, cryptography and some issues relating to them.

Alan L Tyree, 'Virtual Cash II', ***Journal of Banking and Finance Law and Practice***

Part II of the above paper discusses digital coins, anonymous transactions and the legal nature of digital cash.

Alan L Tyree, 'Virtual Cash III', ***Journal of Banking and Finance Law and Practice***

Part III of the above papers looks at further issues in digital cash, including payment systems confidence, money laundering and tax avoidance, consumer protection.

Alan L Tyree, ***Computer Money*****, Paper presented to the First Australian Computer Money Day Conference, University of Newcastle, 28 March 1996.**

Discusses payments systems confidence, replacement of currency, privacy, money laundering and tax avoidance, consumer protection, and special problems with digital coins.

Alan L Tyree, 'Smart Cards: some issues', Journal of Banking and Finance Law and Practice.

Discusses issues relating to smart cards including the fact that they are not governed by the EFT Code of conduct.

Alan L Tyree, ***Legal Problems of Electronic Clearing and Settlement,*** **Paper Presented to the Australian Banking Law Association Conference, Surfers Paradise, 31 May 1996**.

Discusses aspects of legal problems of electronic clearing and settlement, including cheque truncation in Australia, validity of netting arrangements and other matters.

Clarke, Roger, ***Financial EDI in Australia***.

Explains the various conventional and electronic payment methods; overviews of the financial institutions that provide payment services and of Australian payment clearing systems; description of financial EDI; security aspects of financial EDI; reviews of the financial EDI services available in Australia, and of the capabilities of relevant software packages; report on a survey of EDI usage in Australia.

Clarke, Roger, ***Chip-Based Payment Schemes: Stored Value Cards and Beyond***.

Smart Card applications in the financial services arena have reached maturity. Contains detailed descriptions of five pilot based schemes: Quicklink, a Banksys-based scheme in pilot in Newcastle, NSW; CiT/Transcard, a Mifare-based pilot in operation in Western Sydney, NSW; the Mastercard Cash world pilot in Canberra, ACT; the Visa Cash worldpilot on the Gold Coast, Qld; the Mondex trial in Swindon, UK, and committed for Australia; a detailed description of Mikron's Mifare contactless card technology, which is bringing about a merger of the stored value card (SVC) and automated fare collection (AFC) markets; an in-depth, longitudinal study over an 8 year period of smart cards in Switzerland, including a detailed evaluation of the 3-year pilot SVC scheme in Biel/Bienne, and an assessment of the commercial and strategic factors.

Pollard, Simon, Gilbert & Tobin, ***Electronic Payment Systems: The Legal Perspective.***

Paper is directed to the questions which arise in the context of on-line commerce, including the legal paradigm of electronic payments, and the risks of introducing electronic payments systems, and how to shift them.

Pollard, Simon, Gilbert & Tobin, ***The Medium is the Message: The New On-Line Software Distribution Paradigm*****. Paper presented to the AIIA Forum for Information Technology Exporters held at Austrade Conference Centre 24 July 1996.**

Paper discusses the Australian perspective on on-line software distribution. Laws peculiar to Australia affect the process. The Internet represents a whole new paradigm for marketing, sale and distribution of software and will redraw channel strategies, business models and software makers' relationships with their customers and end-users forever.

Singh, Supriya: The Use of Internet Money, ***Journal of Internet Banking and Commerce*****, 1996**

Discusses the new forms of Internet money and the mix of new and traditional forms of money with focus on the user.

http://www.arraydev.com./commerce/JIBC/current.htm

Crede, A*: Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet***, Electronic Commerce and Banking,**

With the rapid expansion of the Internet, there are a number of initiatives underway for the creation of a secure, cost-effective payment system which will be able to support growing commercial activities on the network. The paper examines current progress in establishing payment systems. The paper argues that completely new institutional and legal structures could be required.

http://www.usc.edu/dept/annenberg/vol1/issue3/crede

ASC Background Information Paper, *Electronic Commerce in the Financial Services Industry,* ASC, Sydney, 6 May 1996.

The paper provides background information on the ASC's Electronic Commerce project. The project was initiated in 1995 in response to discussions with industry participants about the likely impact on the financial services industry and the operation of Australian capital markets of developments in electronic commerce.

4. Consumer Protection

Goldring, J; Maher, LW; McKeogh, J: Consumer Protection Law 4th Edition The Federation Press (1993)

Examines the Australian laws relating to consumer protection. Specifically examines the law relating to:

- contractual remedies against seller or supplier;
- manufacturers liability;
- prescription of standards;
- occupational licensing;
- general proscription of deceptive practices and controls in advertising;
- specific controls on deceptive practices;
- consumer credit;
- consumer remedies.

Sutton, K; Sales and Consumer Law, 4th Edition, LBC Information Services (1995).

Examines consumer protection law in Australia. The protection provisions of the Trade Practices Act 1974 and corresponding provisions of the Sale of Goods Act are analysed in detail, and the consumer legislation of the Australian States has been incorporated where relevant. Additional outline of the Uniform consumer credit code, liability of the manufacturer, effects of 'Romalpa' clauses, anticipatory breach and the right to damages.

4.1 Sale of Goods

4.1.1 Texts

Halsbury's Laws of Australia Butterworths Australia Volume 23 Title 375 *Sale of Goods* JW Carter (1995)

The title Sale of Goods sets out the general principles of Australian sale of goods laws. The title examines the source of sale of goods law, including the uniform sale of goods legislation, other legislation regulating or affecting sale of goods transactions and where applicable, common law principles. The title also examines the scope and application of international sales legislation.

The Laws of Australia The Law Book Company Limited Australia Looseleaf Service Title 8 *Contracts Specific* Subtitle 8.4 Sale of Goods Kenneth Sutton

The title examines the general principles of Australian sale of goods law and international sale legislation.

4.1.2 Legislation

The principal legislation regulating sale of goods transactions consists of uniform legislation in force in all Australian States and the principal Territories.

(NSW) Sale of Goods Act 1923, (QLD) Sale of Goods Act 1896 ,SA) Sale of Goods Act 1895, (TAS) Sale of Goods Act 1896, (VIC) Goods Act 1958, (WA) Sale of Goods Act 1895, (ACT) Sale of Goods Act 1954, (NT) Sale of Goods Act 1972. See also (UK) Sale of Goods Act 1979, (US) Uniform Commercial Code

4.2 Consumer Protection

4.2.1 Texts

Halsbury's Laws of Australia Butterworths, Australia Volume 5 *Consumer Protection*

The title discusses the various provisions within State and Commonwealth consumer protection and fair trading legislation.

The Annotated Trade Practices Act 17th Edition RV Miller (1996) LBC Ltd

The legal text provides an annotated guide to the Trade Practices Act 1974 (Cth).

4.3 Legislation

4.3.1 Trade Practices Act 1974 (Cth)

The consumer protection provisions of the Trade Practices Act 1974 (Cth) extend to conduct engaged in outside Australia by bodies corporate incorporated or carrying on business within Australia, or by Australian citizens or persons ordinarily resident within Australia. s 5(1). This provision is not limited to engaging in conduct that may be detrimental to Australian consumers: *Wells v John R Lewis (Int) Pty Ltd (1975) 25 FLR 194.*

The relevant provisions are contained in Parts IV and V of the Act. See for example section 55 of the (Cth) Trade Practices Act 1974, which provides that a person must not, in trade or commerce, engage in conduct that is liable to mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity of any goods. In contrast to other provisions of the Act, s 55 is not limited to conduct that is engaged in by a corporation. The reason for this is that it gives effect to the Paris Convention for the Protection of Industrial Property 1883, to which Australia is a party, and relies for its validity on the external affairs power.

It is expressly stated in section 75(1) of the Act that Pt V is not intended to exclude or limit the concurrent operation of any law of a State or Territory.

4.3.2 State Fair Trading Legislation

The State consumer protection legislation mirrors its federal counterpart:

(NT) Consumer Affairs and Fair Trading Act 1990, (QLD) Fair Trading Act 1989, (SA) Fair Trading Act 1987, (TAS)Fair Trading Act 1990, (VIC) Fair Trading Act 1985, (WA) Fair Trading Act 1987, (ACT) Fair Trading Act 1992, (NSW) Fair Trading Act 1987. See also US Antitrust Act 1914

4.3.3 Standards and Codes

The Advertising Code Of Ethics, a general code which sets standards for all media advertising) and four more specific codes (***The Therapeutic Goods Advertising Code, The Slimming Advertising Code, The Cigarette Advertising Code The Alcoholic Beverages Advertising Code***).

Ministerial Council of Consumer Affairs - Draft Distance Selling 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 and 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.

4.4 Consumer Credit Law

Australian Consumer Credit Law Guide Butterworths Australia (1994) Looseleaf Service Elizabeth Lanyon and others (eds)

Australian Consumer Credit Law focuses on the uniform Consumer Credit Code, enacted in Queensland on 2 September 1994 and adopted, directly or indirectly, by all Australian jurisdictions to commence on 1 November 1996.

4.5 Legislation

4.5.1 Consumer Credit Codes of Each Australian State and Territory

Each State has counterpart uniform legislation. Section 6 sets out the general jurisdiction of the Code. The Code applies 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.

5. Security/Encryption

5.1 International

5.1.1 OECD Guidelines for Security of Information Systems

State that the objective of security is the protection of the intercepts of those relying on information systems from harm resulting from failures of availability, confidentiality and integrity.

5.1.2 OECD Draft Guidelines for Cryptography Policy

The guidelines for cryptography policy are aimed primarily at governments. They are intended to strengthen the security of data in the GII; raise awareness of the need for interoperable cryptographic methods in global and national networks; assist decision-makers in developing and implementing coherent national and international policies; foster confidence in information technology systems and networks; and promote international cooperation between governments and standards organisations to achieve coordinated use of cryptographic methods.

Overall the guidelines promote freedom of choice in the use of cryptography technologies. Users should have a right to choose any cryptographic method to protect data and cryptographic methods should be freely developed in response to the needs and demands of individuals, businesses and governments.

Other policy guidelines state that:

- technical standards, criteria and protocols for the interoperability of cryptographic methods should be developed and promulgated at the national and international level;
- the rights of individuals to privacy and to the protection and confidentiality of their data, including their transactional data, should be taken into account in development, implementation and policy-making regarding cryptographic methods and the infrastructures on which they depend;
- cryptographic methods should also allow for timely lawful access to plaintext of encrypted data or, if appropriate, to cryptographic keys, so that public safety, national security and other interests can be protected;
- the liability of individuals and entities who hold or access cryptographic keys, whether established by contract or legislation should be carefully stated; and
- having regard to the clear and urgent need for international cooperation in all aspects of cryptographic policy, governments should work together to harmonise policies to the greatest extent possible.

One of the main purposes of the guidelines is to inform national governments on domestic policy-making which has international implications. It is noted that individual countries have the right to national policies, and these guidelines will not affect the sovereign rights of national governments, in respect of public safety, law enforcement and national security.

http://www.oecd.org

5.1.3 International Telecommunications Union X500 Standards

Drafted in 1988, the standards laid the technological foundation for authenticating computer based information

5.2 United States

5.2.1 Digital Signature Guidelines - Draft released by the American Bar Association

Drafted by the Information Security Committee of the Electronic Commerce Division of the American Bar Association, the Digital Signature Guidelines seek to establish a secure system which will 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.

The guidelines and the technical standards outlined in the draft mainly attempt to establish the interrelated legal duties of certification authorities, subscribers, and recipients of digital signatures. The roles of a certification authority, subscriber, and recipient are for the most part based on extensions to or elaborations of traditional legal doctrines, especially doctrines relating to contracts and intentional or negligent misrepresentations of fact. The relationship between a certification authority and subscriber is primarily contractual - a subscriber and certification authority will agree to initiate the subscriber's digital signature capability in exchange for a fee or other consideration. The duties of a certification authority to a third party relying on a certificate are rooted mainly in legal prescriptions against fraud and negligent misrepresentation, as are in large measure the duties of a subscriber to a person who relies on a digital signature.

http://www.law.vill.edu/vis/student_home/courses/computer-law.abaguide

5.2.2 Utah Digital Signature Act 1996

The Utah Digital Signature legislation began operation in 1996. Under the Act, a Certification Authority is established where users (corporates as well as individual consumer users) can register and obtain a digital signature pair. The user has an obligation to take reasonable care to retain control of their private key and the allocation of potential liability between the user and the Certification Authority is established by reference to a 'recommended reliance limit' specified in data contained within the certificate which is the key pair (and thus able to be made known to persons who receive messages signed with the private key). The Utah Act gives full legal status to digital signatures for any purpose where the law requires a signature.

5.2.3 Internet Architecture Board

Adopted standards for privacy-enhancing electronic mail in 1993

5.2.4 National Institute of Standards

Adopted Federal Information Processing Standard in 1994

5.2.5 American Bankers Association

Developing a set of digital signature standards for adoption by the American National Standards Institute.

5.2.6 American Society of Testing and Materials Subcommittee on Electronic Authentication of Health Information

Drafted digital authentication guidelines

5.2.7 US Federal Computer Fraud and Abuse Act 1988

Both these regulate against fraud, unauthorised access and trafficking in private keys and payment tokens. In the former, provisions explicitly criminalise trafficking in computer passwords which probably includes private keys and payment tokens. On the other hand, these criminal statutes do not establish default rules for allocating the loss resulting from the conduct they criminalise.

5.3 Europe

5.3.1 German Digital Signature Law

Drafted in November 1996, the Digital Signature Law is expected to be approved by the German Cabinet early 1997 and to be enacted into law shortly thereafter. The purpose of the law is to create general conditions for digital signatures under which they may be deemed secure and forgeries of digital signatures or falsifications of signed data may be reliably ascertained. Outlines the requirements and obligations of 'certifiers', and the licensing procedures for certifiers.

5.4 Articles

OECD Committee for Information, Computer and Communications Policy ***Payment for Goods and Services on the Information Superhighway: Reproduction Rights and Remuneration in the Electronic Marketplace*****, 1996**

Discusses the trade in reproduction rights for intellectual property works and the remuneration element in such trade.

Provides background information on the converging intellectual property industries and the ways in which rights are bought and sold and concludes with references to current experimentation into methods of payment.

The paper selects and proposes a number of matters which must be addressed and for which the right conditions must be put in place:

- the widest possible international agreement on the legal rights of all parties;
- a free market for the negotiation of rights, for establishing the market value of electronic rights and for establishing operating costs, profit margins and customer prices;
- effective laws and efficient technical procedures to govern cash-less transactions and electronic commerce; and
- strong consumer protection.

One of the challenges for payment on the information superhighway is to discover how available technology can allow casual network users to find information and services and pay for them in a single transaction. An important characteristic of the Internet community is the propensity of users to browse almost at random through the different services. This type of electronic supermarket shopping, making impulse purchases, or buying things at short notice, needs more flexible payment methods. Some form of network which links users, banks, credit card companies, clearing houses and suppliers is feasible.

First Virtual Holdings Inc. ***The Perils and Pitfalls of Practical CyberCommerce: The Lessons of First Virtual's First Year*****, January 1996.**

Discusses the development of the payment system First Virtual Holdings introduced to facilitate Internet commerce. The fully operational Internet payment system was introduced in 1994.

The system does not rely on encryption or any other form of cryptography. Instead, safety is ensured by enforcing a dichotomy between non-sensitive information and sensitive information and by a buyer feedback mechanism built atop existing protocols.

The paper briefly describes the First Virtual system, and discusses the role of intermediaries. It suggests that the use of an intermediary between the customer, the merchant and the financial institution will increasingly be seen as a necessary feature as the nature of Internet commerce becomes clearer.

A number of scenarios are given in the paper in order to present the case for using intermediaries in the payment process. It argues that it seems unlikely that Internet commerce can flourish without such intermediaries.

An outline of cryptography is provided, but it is argued that while this can be effective for safeguarding information passed over the Internet, the system will always be 'breakable'. First Virtual claims that its experience with running completely non-cryptographic payment system has been highly positive, but suggests that its system will not remain non-cryptographic forever. It does, however argue that their experience suggests that cryptography is not the single tool in the pursuit of security.

The paper concludes that while encryption can provide a modicum or additional security on the Internet, it is far more important to consider what is being encrypted, and not to encrypt anything that is better kept off the Internet in the first place.

http://www.law,vill,edu/vis/student_home/courses/computer-law/1stvir.htm

Kokuryo, J & Takeda, Y. 1995, *The Role of Platform Businesses in Electronic Commerce,* Presented at the Workshop on Economics of Information Society, 14-15 December 1995, Istanbul

Discusses the role of intermediaries, referred to as platform businesses, in electronic commerce. Argues that intermediaries will play important roles because electronic markets are likely to create trade partners that are far apart and have never traded with each other before. The intermediaries supply necessary elements of trade such as "trust" to convert potential matches between buyers and sellers into 'real deals'.

The research suggests increased opportunities for formerly unknown trade partners to transact actually increases the need for intermediaries. Computer networks by themselves lack some important functions that are necessary in realising open commercial transactions. Trust is just one example. Platform businesses provide functions that are essential in trade such as:

- provision of partner search function;
- creation of trust among trading partners;
- evaluation of economic value;
- provision of standardised interface; and
- integration of functions.

Platform businesses enable firms to utilise the emerging open computer network as a means of commercial activities.

The paper discusses the various functions of platform businesses outlined above. It argues that trust is perhaps one of the most critical elements in trade, and is particularly relevant in the attempt to utilise open computer networks for trade.

Trust among trading partners is relevant to the realisation of transactions in three areas. i.e., (a) the quality of the products, (b) the punctuality of delivery as well as the quality of after-sale service and other services, and (c) the credibility in fulfilling the financial obligations. When any of these factors does not exist, it is argued that the market mechanism is likely to fail.

The paper concludes that platform businesses play the facilitator's role in trade. Their existence and prosperity enable traders to make full use of the emergent business opportunities afforded by the new breed of computer networks.

Froomkin, M. 1996*, The Essential Role of Trusted Third Parties in Electronic Commerce*, Oregon.

Begins from the premise that while cryptography and encryption techniques can contribute greatly to the transactional security, this is only one element of securing electronic commerce. Many cryptographic protocols for secure electronic transactions require at least one trusted third party to the transaction, such as a bank or certification authority (CA). These partly cryptographic, partly social, protocols require new entities, or new

relationships with existing entities, but the duties and liabilities of those entities are uncertain. Until such uncertainties are resolved, the paper argues that they risk inhibiting the spread of electronic commerce and causing unnecessary litigation.

The article aims to describe what CAs do, explain why they are important to electronic commerce, and suggest that they are likely to provoke some interesting legal problems. It argues that clarification of the duties and liabilities of CAs will serve the interests of all parties to an electronic transaction in which a certificate plays a role.

Basic cryptographic techniques are described, including public key cryptography and digital signatures. Outlines the various types of digital certificates that can be offered by certification authorities and discusses the application of these techniques to the Internet. Also presents an introductory discussion of the liability of a CA that issues an erroneous certificate.

Given the dearth of applicable legislation, the complete absence of case law and the very small number of functioning CAs in the United States, the paper argues that the duties and potential liabilities imposed on CAs are unclear.

The paper discusses a number of scenarios that would bring the question of liability to the fore. It argues that the case of legislation begins with the observation that the legal climate for CAs is uncertain and that uncertainty increases costs and discourages transactions. In the case of CAs it threatens to produce overpowerful incentives for CAs to underproduce certificates and/or disclaim all liability for certificates, which threatens to limit their utility. It is also likely to lead to considerable litigation until all the relevant rules are identified.

Yet, implementing legislation requires a policy choice as to what the appropriate level of liability should be. The Utah Digital Signature Legislation provides one model. Under this, a CA that complies with relatively onerous requirements is granted a safe harbour from consequential damages and most liability in excess of a reliance limit stated in the certificate, even if the CA itself is guilty of a negligent misstatement. Yet is unclear whether such a framework will work, given that no CAs have qualified to offer such a service to date.

It is concluded that the general lack of regulatory and legal standardisation may prove to be a large impediment to the development of reliable electronic commerce. A national or even possibly international standard for accurately signalling what a certificate promises, and the extent to which a certificate can reasonably engender reliance, may be needed. Such a standard is unlikely to emerge until the relevant legal rules that already exist are identified; and the development of standards is also likely to be retarded by the great diversity of legal regimes in different jurisdictions that may be involved in a single transaction. Whether it would be best to produce the legal standardisation through legislation, the judicial process or market mechanisms is debatable. However, until some standardisation is achieved, users of digital signatures will find it difficult to determine what degree of commercial reliance to place on a representation in a certificate. In addition to national standards, at least minimal international norms for certificate recognition and CA regulation will become increasingly necessary as electronic commerce becomes more global.

http://www.law.miami.edu/~froomkin/articles/trusted1.htm

6. Privacy

6.1 International

6.1.1 1966 International Covenant on Civil and Political Rights

Article 17 of this Covenant directly applies to the issue of data protection:

- No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
- Everyone has the right to the protection of law against such interference or attacks.

6.1.2 United Nations Guidelines for the Regulation of Computerised Personal Data Files

44th Session of the United Nations adopted the Guidelines in 1989.

6.1.3 United Nations Guidelines Concerning Computerised Personal Data Files

Produced in 1990 by the UN Economic and Social Council, the guidelines set forth the UN position on data protection.

6.1.4 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Adopted in 1980, the guidelines were developed to harmonise the varying national data privacy laws of the OECD member states. Specify that personal data should only be collected by lawful and fair means, should not be disclosed or used for purposes other than that which it was collected for, and should be protected by the holder against risks such as loss or unauthorised access, destruction, use, modification or disclosure.

6.2 United States

6.2.1 Constitution of the United States

Although a right to privacy is not set forth in the Bill of Rights, the Federal Court has found sources for a right to privacy in the First, Third, Forth, Fifth, Ninth and 14th Amendments. In a landmark case, "Katz v. United States" the Federal Court recognised the privacy interest that protected an individual against electronic surveillance, but cautioned that the Fourth Amendment cannot be translated into a general constitutional right to privacy. The Fifth Amendment protection against self-incrimination involves a right to privacy against unreasonable surveillance by the government or compulsory disclosure to the government.

6.2.2 Privacy Act 1974

Enacted to provide legal protection for, and safeguards on the use of personally identifiable information maintained in federal government record systems. The Act established a framework of rights for individuals whose personal information is recorded and responsibilities of federal agencies that collect and maintain such information. The Privacy Act embodies principles of fair information practices.

6.2.3 Cable Act 1984

Precludes cable operators or third parties from monitoring the viewing habits of cable subscribers. Under the subscriber provisions of the Act, cable operators are required to inform their subscribers at the time of entering a contractual arrangement of their data collection and disclosure practices and subscriber rights to inspect such data.

6.2.4 1992 Cable Act

Extended the protection of the 1984 Cable Act to new services that may be provided over cable facilities, such as personal communications services. It also requires cable operators to take actions necessary to prevent unauthorised access to personal information by persons other than the subscriber or cable operator.

6.2.5 Computer Security Act of 1987

Established a federal government computer security program by assigning responsibility for developing government-wide computer system security standards and guidelines to the National Bureau of Standards (now the National Institute of Standards and Technology (NIST)). Requires that federal agencies identify computer systems containing sensitive information and develop security plans.

6.2.6 Proposed Legislation - Consumer Internet Privacy Protection Act of 1997

Introduced in the 105th Congress, the Consumer Internet Privacy Protection Act seeks to establish privacy safeguards for Internet users. If enacted it would create enforceable privacy rights for users of online services. The new bill requires that an interactive computer service obtain consent from a subscriber before disclosing personally identifiable information to a third party. The subscriber may also obtain the identity of third parties that obtain personal information.

Under the bill the Federal Trade Commission (FTC) is given the authority to examine and investigate providers and to issue cease and desist orders for violation. The bill also allows individuals to seek civil relief in court for violations of the Act.

6.3 European Union

6.3.1 Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data

Adopted in 1981 following OECD Guidelines but unlike the OECD guidelines they are legally binding on any member state that ratifies the Convention. The convention required the ratification by all member states of the Council of Europe. To permit ratification, each member state had to adopt its own national data protection law. The Convention is significant in that it calls for data protection legislation to cover the private sector in addition to government organs.

6.3.2 European Data Protection Directive

Formally adopted by the Council of Ministers in October 1995, the Directive provides for the protection of individuals with regard to the processing of personal data and on the free movement of such data. Member states are obliged to implement the provisions of the Directive within a three year period.

The Directive applies whenever personal data is processed wholly or partly by automatic means and also to certain forms of manual systems.

The processing of personal data will only be legitimate in specified situations. The first of these is where the data subject has unambiguously given his consent. The Directive provides that a data subject is to be given rights to object tot he processing of personal data at least in the situations where the justification for processing lies in the performance of a task carried out in the public interest or is undertaken for the purposes of the legitimate interests of the controller or of third parties to whom the data is disclosed.

The Directive also contains significant provisions regarding the control of Transborder data flows. It prohibits the flow of data to countries that have not provided an adequate level of data protection. The adequacy of a third country's data protection regime must be assessed in light of all the circumstances surrounding the transfer operation or set of transfer operations before personal data is transmitted.

6.4 Australia

6.4.1 Federal Privacy Act 1988

Outlines procedures for the collection, storage, security, and use of personal data by Federal Government agencies. Stipulates that Federal agencies must formally notify the Privacy Commissioner once a year of the systems they maintain that contain personal data. Agencies must also inform the Commissioner of the extent, purpose and contents as well as the uses of the personal data contained in the systems.

6.4.2 Privacy Amendment Act 1990

Extended the Privacy Act to include the credit reference industry. First application of the Privacy Act to the private sector.

6.4.3 Data Matching Programme (Assistance and Tax) Act 1991

Further amended the Privacy Act by regulating certain data matching activities by government departments, especially those that are defined as 'assistance agencies'[1]. 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. The government announced in 1990 that the tax file number would be used to match data in government systems in order to determine who may be fraudulently receiving benefits payments.

---

[1] These include the Department of Community Services and Health, Department of Employment, Education and Training, Department of Social Security, and Department of Veterans Affairs.

6.4.4 Telecommunications Act 1991

Imposes regulations on the carriers handling and storage of personal informant. Although an important part of privacy considerations, these regulations do not cover the activities of the carrier or service providers when acting as a commercial entity.

6.5 Articles

Orlowski, S. *Privacy Security and Law Enforcement,* Presented at a Conference at Charles Sturt University, November 1996

Discusses the conflict between privacy and law enforcement arising from the expanding use of cryptography by Internet users. As with cryptography, balances need to be struck between rights of individuals and the rights of the community as a whole. The paper does not attempt to specify what the balance should be, but argues that whatever the balance, the one thing which does apply is that governments should be accountable whenever they impinge on individuals' rights.

Briefly outlines the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The paper argues that these guidelines are useful as they establish not so much the measures which should be taken to secure information systems, but rather the framework within which security should be applied. They address issues such as: accountability; ethics; democracy; and awareness which are not traditionally seen as security matters. They are, however, an integral part of a holistic approach to information security management.

Argues that the major privacy concerns regarding the 'information superhighway' are: (i) the ability to collect and collate large amounts of data on individuals; and (ii) the possibility of the interception of private communications. While technology can provide some solutions to the former, the principle approach will need to be through interoperable legislation and other regulatory structures such as codes of conduct.

The paper notes that as information will be flowing between various countries, it will not be possible to rely on legislative or regulatory structures in the country where the user is located. Approaches involving national legislation or regulation will not work in isolation. It argues that what will be needed is an international approach which will operate regardless of where the data is provided, utilised or stored.

http://www.anu.edu.ap/people/Roger.Clarke/II/Orlowski4.html

Battcock, R. Data Protection: Where Next*?, International Journal of Law and Information Technology*, Vol 3, No.2.

Examines the changes that will be required by European countries as a result of the EU Directive on Data Protection and the widening social and technological scope of data protection in the 'information society'. Also gives consideration to some of the likely developments in data protection internationally.

The article begins from the standpoint that the great majority of countries involved in international trade and information exchange have no general data protection laws. Some, such as the US, have specific sectoral legislation, and the sectoral approach will doubtless continue to be important.

Developments in Europe suggest that a combined omnibus and sectoral approach may make for the best overall system. Concludes that the European system is clearly a strong international model. Argues that the privacy impact of new policing, surveillance and data matching developments will need to be faced by legislators and data protection bodies together by means of some new mechanisms to ensure adequate scrutiny of new laws and proposals. In the international sphere greater cooperation will be needed.

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

Outlines a possible co-regulatory approach to extending privacy protection to the private sector. While the current *Privacy Act* covers collection, storage and security, individual access and correction, use and disclosure of personal information held by the public sector, there are no legislative standards applying to the private sector.

The momentum for comprehensive privacy protection in the private sector has been building across the political spectrum, particularly when the European Union passed a Directive on Data Protection in early 1996. This discussion paper is a response to such international initiatives.

The co-regulatory regime outlined in the paper would apply privacy protections to records containing personal information. The scope of the regime would apply to all individuals and organisations, whether incorporated or not, in the private sector. The regime would rely on a range of Commonwealth constitutional powers.

Standards for data protection would be set down in Information Privacy Principles (IPPs) encompassing all the internationally recognised tenets of privacy protection. These would be complemented by Codes of Practice, to be developed in relation to specified 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 upon the IPPs.

The paper gives quite a detailed exposition of the proposed regime, including what the Codes of Practice should contain; the procedure for issuing Codes of Practice; and ways of amending or revoking the Codes. It is noted that the Codes of Practice should contain a provision to cover the transfer of personal information out of Australia to countries with inadequate levels of privacy protection.

The paper also provides an outline of the procedures for complaint resolution and procedures for the conduct of investigations following a complaint. Under the proposed scheme, 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.

OECD, *Report of the Ad Hoc Meeting of Experts on Information Infrastructures - Issues Related to Security of Information Systems and Protection of Personal Data and Privacy*, 1996

Reports on the meeting of experts held in Paris in November 1994 in which four key policy issues in the context of the development, operation and use of the information infrastructure were examined:

- security of information systems;
- the protection of personal data and privacy;
- cryptography; and
- protection of intellectual property.

The meeting considered the challenges in these areas and their possible solutions, including the pathways to reaching these solutions. Critical to this was a consideration of the appropriate roles for government, the private sector and international organisations in bringing about these solutions.

Covers the developments in each of these areas to date and the extent to which the information infrastructure raises issues that may require special treatment or new remedies.

The report also highlights the importance of striking an appropriate balancing act between often competing interests and rights. These include; rights to privacy and security *vs* requirements of criminal law and national security; rights of a sender of a message to anonymity *vs* the right of recipients to be left alone and the need for audit trails; data protection *vs* free flow of information; and individual *vs* public interests.

Post, D. Personal *Privacy and the Trail of Transactional Breadcrumbs*, Draft Paper, September 1996

Discusses the ease with which dossiers of personal information can be compiled by the collection and analysing of electronic records of where "we" have been in "cyberspace". As we conduct more of our business and personal activities via electronic media - purchasing goods and services through the World Wide Web, communicating with business associates and friends etc - we are leaving an electronic trail which, when combined with innumerable other such records, can form a detailed profile of who we are and what we do.

Claims that the lack of an overarching framework to deal with the use of personal transaction records threaten our privacy. US law has responded to perceived threats to personal privacy posed by government record keeping and has erected an array of protections against unreasonable government action in this area. However, the use of transactional records by the private sector and commercial companies is, at least in the US, largely unregulated.

Concludes that substantial reconceptualisation of the relevant legal principles is required. Discusses the approach of the European Union, but claims that it is too early to tell whether the US will follow the Europeans' lead. The US federal government's Privacy Working Group takes a cautious and measured approach, recommending no new legislative initiatives but instead seeking to define a set of principles to guide the development of the private sectors and government programs that use personal information. The paper questions whether this will be enough to ensure that "personal information should be acquired, disclosed and used only in ways that respect an individual's reasonable expectation of privacy (NTIA, Privacy and the NII, 1995).

http://www.cli.org/DPost/X0004_BCRUMB.html

Pollard, S. Electronic *Messaging and Privacy in the Workplace*, Presented at the IBC Conference, Sydney, 20-21 February, 1996, Gilbert and Tobin Lawyers

Explores the legal liability issues for messaging system operators and users; and how users can manage the legal and commercial risks of messaging over on-line services and BBS, including defamation, security and privacy issues.

The paper focuses on electronic messaging and not electronic trading. It notes the important differences between the two, namely that messaging is largely unstructured information communicated between individuals, while electronic commerce is concerned with formally structured electronic documents used for commercial trading purposes between trading partners. However, notes that the wider issues of security, the enforceability of digital signatures and privacy do overlap with the wider concept of messaging.

Discusses legal liability issues for both system operators (sysops) and users around electronic messaging.

With regard to privacy issues, the paper outlines the protective measures currently in place federally and the initiative of the NSW Government to implement the Privacy and Data Protection Bill in 1994.

Outlines liability issues with reference to the infringement of intellectual property, and provides examples of cases brought before the courts that have established precedents with regard to copyright infringement. Claims that it is likely that liability for copyright infringement will continue to rest with sysops, regardless of whether they know that they are infringing copyright.

Concludes with a number of rules that emerge for organisations dealing with personal messages. Recommends that adequate steps are taken to maintain confidentiality of message contents, and ensure that data security program accords with the laws and regulations of both the Commonwealth and the controlling state.

http://www.gtlaw.com.au/gt/pubs/elecmessage.html

Cavoukian, A. *Go Beyond Security - Build in Privacy: One Does Not Equal the Other,* Presented at Cardtech/Securtech 96 Conference, Atlanta, Georgia, may 14-16, 1996.

Argues that the concepts of privacy and security are not the same thing, despite the fact that they are often used interchangeably.

The full spectrum of data security, computer and network security, physical security and procedural security and procedural controls must be deployed to protect personal information from a wide range of threats. Measures that enhance security enhance privacy: the two are complementary, but not one and the same. As a result, simply focussing of security is not enough. The paper argues that for true privacy protection the code of fair information practices must be honoured.

Yet, to ensure true privacy protection, emerging technologies must be utilised. The paper argues that anonymity is a key component of maintaining privacy. Protecting one's identity is synonymous with preserving one's ability to remain anonymous. Technologies that provide authentication without divulging identity not only address privacy concerns, but also provide much needed assurances to organisations regarding the authenticity of individual they are doing business with.

Two examples of privacy-enhancing (anonymizing) technologies are provided, each of which rely upon the blinding of identity through the use of encryption - in the first case through an extension of public key encryption, in the second through the use of biometric encryption. The use of these technologies minimise or entirely eliminate personally identifiable information and, it is concluded, serve the needs of both individuals and organisations in so far that personal privacy is maintained through anonymity, while organisations are assured of the authenticity of the individuals that they are doing business with.

US Federal Trade Commission, *Staff Report: Public Workshop on Consumer Privacy in the Global Information Infrastructure*, December 1996

The US Federal Trade Commission has initiated a study to examine the range of issues posed by the developing technology-based marketplace. As part of this, the US Bureau of Consumer Protection undertook a Consumer Privacy Initiative to examine consumer privacy issues in the online context, and to promote consumer and business education about the use of personal information online. The staff report presents the findings from a workshop convened on this topic.

The report discusses current online uses of personal information, the core elements of voluntary privacy protections, and the government's role in protecting consumer privacy online.

Outlines a number of voluntary codes of conduct that have been developed by groups such as the Direct Marketing Association (Guidelines for Personal Information Protection), the Information Industry Association (Fair Information Practices Guidelines) and the Interactive Services Association (Guidelines for Online Services: The Renting of Subscriber Mailing Lists) to protect the use of personal information in an online environment.

Examines different approaches to enhancing consumer privacy online through technological innovation, education, self regulation, and law enforcement. Discussion revolved around whether the government should play a role in protecting individual privacy online. Some argued that purely self regulatory approaches to protecting privacy have failed, while others saw emerging technologies as alternatives to government regulation in the global online marketplace.

Focussed on the issue of collecting data about children using online services, and the associated privacy concerns. A coalition of children's advocacy organisations urged the Commission to adopt guidelines prohibiting deceptive and unfair data collection activities involving children.

The report concludes that there is a wide range of views about privacy in the online marketplace. There was broad agreement on the necessary elements of effective consumer privacy protection online, namely, notice, choice, security and access. The report also noted agreement amongst workshop participants that consumers should be able to exercise choice about whether and how their personal information is used, that security of personal information is crucial and that consumers should have access to their information. Viewpoints varied considerable, however, on more specific issues of implementation, such as the form notice to consumers should take, how consumer choice is to be exercised, and when and how to obtain parental consent when information is collected from children.

Regarding the issue about whether government regulation is needed, or whether privacy issues should be addressed by emerging technologies, there was a wide range of views.

7. Current Australian and Overseas Activities

7.1 Individuals and Academic Organisations

7.1.1 Professor William John Caelli

Head of School of Data Communications, Faculty of Information Technology, Queensland University of Technology. Within the School is the Information Security Research Centre (Director A/Professor Ed Dawson), whose research interests cover: cryptology, risk analysis/assessment, secure data networks, electronic data interchange, messaging and electronic funds transfer.

http://www.qut.edu.au/qut/centres/isrcx.html

7.1.2 Centre for Electronic Commerce

Located within the School of Business and Electronic Commerce, Gippsland Campus of Monash University. Executive Director is Jo-Anne Fisher. Among other items, the Centre has produced a detailed study for the Queensland Information Industries Board on "Electronic Commerce for Small to Medium Sized Enterprises (SMEs)".

The first stages of the establishment of the Australian Electronic Business Centre (AEBC) were announced on 24 January 1997. It is progressing under the Chairmanship of Mr. Russell Fynmore, with the support of the Victorian Government Office of Multimedia, the Federal Government Department of Industry Science and Tourism, ECA/Tradegate, a number of private sector organisations, other State governments and a select group of Australian universities.

The primary objectives of the AEBC are to:

1. Encourage business to take up productive information and communication technologies to improve business and ensure competitiveness,
2. To ensure "brand recognition" of Australia and its skill base in electronic commerce products and services, and
3. To support and encourage development of the Australian IT&T supplier industry to provide world-beating electronic commerce solutions.

The purpose of the AEBC is to create a single resource entry point for business and governments interested in electronic business. The services and functions of the AEBC will include information dissemination, education, consultancy, demonstration facilities, test-bed facilities and pre-competitive research. The AEBC is proposed to be operational by July 1 1997.

http://www-cec.buseco.monash.edu.au/

7.1.3 Roger Clarke

A consultant specialising in electronic commerce, information infrastructure and data surveillance and information privacy. He has produced a report titled: "Chip-Based Payment Schemes: Stored-Value Cards and Beyond" and supervised another: "Financial Electronic Data Interchange in Australia". His home page provides references to an extensive range of his writings.

http://www.anu.edu.au/people/Roger.Clarke/

7.1.4 Chris Connolly

Director, The Policy Network, Level 14/49 York Street, Sydney. Chris Connolly is a consultant who specialises in the legal and social impact of new technologies. For the last three years he has carried out extensive work on smart cards, Internet transaction systems and electronic commerce generally.

His employment history includes work for the United Nations, the Privacy Committee of New South Wales and the Communications Law Centre.

As well as consulting, he is the Co-ordinator of the Smart Card Advisory Network (SCAN), and has received a grant to establish an Electronic Money Information Centre (EMIC), of which he will be the director. EMIC will be a non-profit community organisation dedicated to quality research and information on electronic money policy issues. It will be launched in March 1997.

email: chrisc@socialchange.net.au

7.1.5 Ms Robyn Lindley

Lecturer in the Department of Information and Communication Technology, University of Wollongong. She conducts research in the areas of strategic telecommunications network planning and smart card technology.

http://www.uow.edu.au/informatics/iact/robynprof.html

7.1.6 Associate Professor Mark Sneddon

Faculty of Law, University of Melbourne. He lectures and undertakes research in the field of electronic banking, commercial transactions, banking law and telecommunications law.

http://www.law.unimelb.edu.au/hp.htm

7.1.7 Associate Professor Paula Swatman

Deputy Head of Information Systems, Monash University. She has extensively written on Electronic Commerce, initially EDI and now more recently related to the Internet. Leads the Electronic Commerce Research Group within the Department.

http://www.is.monash.edu.au/~pswatman/

7.1.8 Professor Alan L Tyree

Landerer Professor of Information Technology and Law, University of Sydney. He has published a number of seminal textbooks on banking law since 1987, and more recently has written prolifically on a wide range of electronic commerce topics. Major areas of research are: artificial intelligence, computer assisted learning, banking law, and technology and international trade.

http://www.law.usyd.edu.au/~alant/

7.1.9 Associate Professor Graham Wrightson

Professor Wrightson heads the Monetary Systems Engineering Group of the Department of Computer Science and Software Engineering, University of Newcastle. A non-commercial initiative of the Group for the second year running is the Australian Computer Money Day which is intended to bring together researchers, regulators and practitioners in electronic payments and electronic commerce.

This event gives an overview of the technology used in innovative electronic payment systems, the commercial implementations under way in the area, and the concerns of regulatory authorities about these developments.

http://www.cs.newcastle.edu.au/CMD97/CMD97.html

7.2 Government Organisations and Inquiries

7.2.1 Attorney General's Department

Commencing early 1997, the Federal Attorney General's Department is forming an Electronic Commerce Expert Group comprising representatives from the AGs Dept, State Govt Depts, academia and private legal practices. The terms of reference will include matters such as the changes to the law necessary for digital signatures to have the same legal standing as written signatures. Jurisdictional questions are also understood to be of paramount importance. Contact: Jenny Clift, International Trade Law Section, AG's Dept.

7.2.2 Australian Securities Commission, Electronic Commerce in the Financial Service Industry: Challenges and Opportunities, 1996

The Australian Securities Commission (ASC) initiated a project in 1995 to examine the likely impact on the financial services industry and the operation of Australian capital markets of developments in electronic commerce.

A *Concept Paper,* released in mid 1996, presents a set of working principles which the ASC considers are likely to be useful n ensuring that decisions taken in response to proposals for electronic communications between issuers and investors under Corporations Law are clearly articulated, conceptually coherent and facilitate adoption of new technologies by financial service providers.

The paper does not consider the issues of computer based markets or electronic lodgement with the ASC. These will be considered in the future work of the Electronic Commerce Project. This paper focuses on principles for electronic communications between issuers and investors. The working principles developed by the ASC for electronic communications between issuers and investors deal with:

- standard of information;
- sending information to an investor;
- accessibility;
- authentication;
- integrity and security of electronic communications;
- electronic payments; and
- preservation of records.

A policy has also been adopted by the ASC to outline the requirements for the use of electronic prospectuses.

The ASC recognises that electronic commerce is an area where it is important that the regulatory infrastructure respond in a positive and timely way to facilitate market developments and not hinder innovation in market products and processes. There are important benefits to be gained through facilitation of market developments in this area for the competitiveness of the Australian financial services industry, efficiencies in the operation of our capital markets and the better meeting of investor needs at lower costs. It also offers the possibilities for a reduced compliance burden on entities through more extensive use of electronic lodgement of information with the ASC and the use of that information in ways that can add value to commerce more generally.

The ASC is concerned to ensure that no more onerous requirements are imposed on electronic communications under law than those imposed on printed text communications, provided that regulatory objectives are met.

http://www.asc.gov.au/frames/328.html

http://www.anu.edu.au/people/Roger.Clarke/EC/ASC97.html

7.2.3 Australian Taxation Office, *Internet and Electronic Commerce Project*

The Australian Taxation Office (ATO) is examining the potential impact of the Internet and related technologies such as electronic cash on compliance with existing tax laws. The terms of reference for the project include examination of:

- impact of the information superhighway, in particular the Internet and electronic cash and commerce, on taxes, the evasion of tax law and the potential erosion of the tax base from commercial use of the Internet;
- development of appropriate audit methodologies for use in relation to electronic commercial activities;
- potential impact on tax compliance of banking, finance and payment systems on the Internet;
- potential impact on tax compliance of technical issues such as security, auditability and network bandwidth;
- implications for Australia's administration of its tax laws and international taxation agreements;
- evidentiary issues relating to Internet commerce;

http://www.webaustralia.com.au/ato/ecash/ecash1.htm

7.2.4 Australian Transactions Reports and Analysis Centre (AUSTRAC)

An Electronic Commerce Task Force chaired by AUSTRAC has been examining the law enforcement and tax revenue implications of the Internet and smart cards. Its report to the Attorney General strongly recommends adoption of a whole-of-government approach to further policy setting and changes to legislation, with the AG's Department more than likely taking prime responsibility. The report titled "Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board" is pending release after approval by the Minister. Contact Paul Ryan.

7.2.5 Department of Administrative Services (DAS)

The Office of Electronic Commerce, directed by an interdepartmental steering committee, is concerned with purchasing both within DAS and the Commonwealth Government at large.

On 20 August 1996, the Minister for Administrative Services announced the Government's new Statement of Direction for Electronic Commerce. This affirmed the Commonwealth Government's commitment to expanding its electronic capabilities for the benefit of the Australian community, and to working with other tiers of government towards a whole-of-government approach to electronic commerce.

The Commonwealth Government will:

- set strategic directions for the continued expansion of electronic commerce activities in its program delivery and program support functions especially Commonwealth Government purchasing; and
- work through the Online Government Council for consistency in inter-governmental efforts, encouraging collaboration where appropriate, and avoiding duplication wherever possible.

Although the above initiative was historically substantially EDI-focussed, reference to the Online Government Council ensures that Internet implications and applications are considered. DAS also provides the secretariat for the National Procurement Board.

http://www.das.gov.au/~corpcomm.world/media/budget/item4.html

7.2.6 Department of Communications and the Arts (DOCA) & the OGC

DOCA provides secretariat support to the Online Government Council (OGC) which is to first meet on 7 March 1997. It will comprise ministerial representatives from the Federal and State Governments, in addition to the President of the Australian Local Government Association. The aim of OGC is to coordinate government approaches to online issues across Australia and it's initial focus will be on the electronic delivery of government services and user authentication. It will later explore issues of networking and cooperation between all levels of government.

Internet site pending

7.2.7 Department of Industry Science and Technology (DIST)

With the prime focus being on industry development, two programs are currently being supported by DIST, viz:

- Electronic Commerce Demonstration Program - which funds work by ECA/Tradegate and Australian Business Online (NSW Chamber of Manufacturers); also contributes to development of the Victorian pharmaceutical venture PECC;
- Information Online Program - which will focus more on applications for small business.

To date, the programs have exploited EDI and other closed-type systems but will inevitably move towards Internet-based applications when they mature. Administered from within the Information Industries Branch of Division A. The role of that Branch is to advise on policies and programs to promote the growth and competitiveness of the Information Technology, Telecommunications and Multimedia industries, as well as encouraging viable investment by both individual and indigenous companies in these industries.

http://147.211.50.102/dept/telephon.html#bkmark16
http://www.dist.gov.au/

7.2.8 Federal Bureau of Consumer Affairs

Administratively located within DIST, the role of the Bureau is to provide consumer policy advice at the national level and increase awareness of the rights, responsibilities and obligations of consumers and suppliers of goods and services.

A 46 page report by the Bureau, released in March 1997, deals with Electronic Commerce issues such as: consumer confidence, privacy, security of payment and cross-border transactions. In brief, the main conclusions were:

- Unless online payment systems provide a level of consumer utility at least comparable to existing payment systems, the Internet marketplace will be at a comparative disadvantage into the foreseeable future;
- Existing industry based initiatives such as codes of practice and dispute resolution schemes are unlikely to apply to cross-border transactions; consumers will need to be aware of the potential for some practical difficulties associated with online purchases from overseas suppliers;
- There is little legal restriction on Australian Internet vendors collecting, re-using or disclosing consumer information at present; even if consumers were to gain protection from such activities for within-Australia transactions, this would not address the need for privacy by Australian consumers dealing direct with overseas businesses.

Contact: Geoff Bennett

http://www.dist.gov.au/consumer/about.html

7.2.9 Office of Government Information Technology (OGIT)

Under the aegis of the Department of Finance, OGIT has a number of committees dealing with issues in the area of Electronic Service Delivery including the Information Technology and Telecommunications Policy Advisory Committee (ITTPAC), Government Technology & Telecommunications Conference (GTTC), State/Commonwealth Electronic Service Delivery Reference Group and international groups including sub-committees.

http://www.ogit.gov.au/

7.2.10 Purchasing Australia

The Electronic Commerce Office (ECO) was established in 1994 by Purchasing Australia, a division of the Department of Administrative Services. ECO is facilitating the implementation of electronic commerce in Australian Commonwealth Government purchasing.

http://www.gems.gov.au

7.3 Industry Bodies

7.3.1 CommerceNet

CommerceNet Australia aims to establish itself as the peak Australian body for Internet Commerce. It is a non-profit, industry-led, membership-based and nationally-focussed organisation whose charter is to:

- accelerate the adoption of the Internet as a business tool in Australia and New Zealand;
- assist in the creation of an on-line environment which is conducive to Internet Commerce;
- assist in the development of a critical mass of on-line users, services and applications; and
- encourage best-practice in the Australian on-line community representing Australian interests in cooperative efforts to develop global standards.

CommerceNet Australia is currently in the process of recruiting initial founding members to form a national board. Its predecessor was ***Internet Commerce Australia (ICA).*** The head office for CommerceNet Australia will be located in Adelaide, with Chapters established in all States of Australia during 1997. It is a Global Partner of the industry grouping CommerceNet Consortium (USA).

http://www.syd.dit.csiro.au/projects/ica/mail/maillist.html, message from Philip Moody dated 10 January 1997.

7.3.2 ECA/Tradegate

Electronic Commerce Australia (ECA) is a peak body with approximately 450 members covering mainly companies with a technological interest in electronic commerce. ECA has established a number of working parties and prepares papers from time to time on issues relating to interoperability and on-line regulation for example.

ECA and Tradegate merged on 23 December 1996. The new organisation promotes projects that stimulate electronic commerce in Australia.

http://www.syd.dit.csiro.au/projects/ica/mail/maillist.html, message from Grant Butler dated 10 January 1997.

7.3.3 Smart Card Advisory Network (SCAN))

This group currently has a total membership of at least 90, some of whom are mentioned herein. Its coordinator is Chris Connolly.

email: chrisc@socialchange.net.au

7.3.4 Standards Australia

Standards Australia has technical committees IT/5 on Financial Transaction Systems and IT/11 on Electronic Commerce. Although IT/5 mainly deals with EFTPOS and stored value card matters, IT/11 encompasses all aspects of electronic commerce. Nevertheless, IT/11 has been inactive for some years.

The Public Key Authentication Framework (PKAF) Task Group issued its report late 1996 and made recommendations for necessary changes in the legislative and standards arena relating to digital signatures and certification.

http://www.standards.com.au/~sicsaa/iacgtc.html