ELECTRONIC COMMERCE: PROMISES, PROBLEMS AND PROPOSALS

MELISSA DE ZWART*

ABSTRACT

You are sitting in front of the luminescent screen of your computer, using your mouse to scroll through the on-line catalogue. Suddenly, you see something you like. You click on the image of a stylish designer label suit and drag it across the screen onto a rotating 3-D image of yourself. Does it fit? Is it the right colour for your skin tone? If not, try another size or colour or send an electronic order to the manufacturer to tailor a suit to the specifications of your 3-D model.

Alternatively, you are looking at an image of a car, scrolling through the options, two-door/four-door, interior, colour, sunroof, manual or automatic, power steering, radio and so on. You select your desired options, click on the send button and wait to be contacted by the nearest dealer with the price of your new car.

Are these images from science fiction or the ultimate trip for computer junkies? No, these are examples drawn from a recent US Government report on the potential of electronic commerce, *The Emerging Digital Economy*.[1]

Electronic commerce is being targeted by governments worldwide as 'the next big thing'. Vast amounts of time and energy are being devoted to examining the issue of how to make electronic commerce an efficient, effective and widely accepted means of doing business. Recent predictions suggest that the Internet will be used for business worth more than US$ 300 billion annually by 2002.[2] Although it seems it is already taken for granted that electronic commerce is an essential aspect of future business development worldwide, there is currently little tangible evidence of broad consumer acceptance. For the moment, there are still many unanswered questions concerning three main aspects of electronic commerce: How will it operate in practice? How will security concerns be

* BA (Hons) LLB (Hons) LLM (Melb); Lecturer, Law Faculty, Monash University.

1 United States Department of Commerce, *The Emerging Digital Economy*, April 1998 at 43-4.

2 *Ibid* at 7. These figures were also cited by Senator the Hon Richard Alston, "Australia in Context", presented at the Enabling Australia E-Commerce Summit, 16 April 1998: see <http://enablingaustralia.telstra.com.au/bkgrnd/trans/tsalsto2.htm>.

satisfied? What law will be applied to transactions conducted on the electronic frontier – the Internet?

This article will examine some of the most recent Australian government initiatives in this area. It will consider the recommendations of the report of the Electronic Commerce Expert Group to the Attorney-General, *Electronic Commerce: Building the Legal Framework*[3] (the ECEG Report) and the report of the Australian Taxation Office, *Tax and the Internet*[4] (the ATO Report) as well as a number of other government initiatives in this area. This article will also review a number of recent US reports on the development of a strong and secure on-line marketplace.

Reports both in Australia and in the US have identified several key issues. These include the need to establish efficient and universally accepted payment mechanisms which accommodate privacy and security concerns; jurisdictional problems and taxation. All of these issues raise questions about the appropriate legal solutions. The problems, like the Internet itself, are universal and their solutions need to be developed at an international level.

I. PROMISES: WHAT IS ELECTRONIC COMMERCE?

The best known use of 'electronic commerce' is possibly in the context of retail consumer purchases, such as a CD or a book via a site on the World Wide Web. However, electronic commerce encompasses a far broader field of endeavour. It covers activities such as banking and insurance services, ranging from account inquiries to loan transactions completed entirely on-line; information services for education or entertainment, whether for payment or free; ordering tangible products such as computers or flowers for delivery locally or overseas; dealing with after sale service inquiries; twenty-four hour shopping; advertising; travel bookings; inventory control, ordering, invoicing and account management.[5] These services may operate through a highly graphical user interface on the World Wide Web or consist of a simple email message.

There is no single accepted definition of 'electronic commerce'. One reason for this is that new uses of the medium are emerging every day. The reports themselves are not definitive about what electronic commerce encompasses. The ECEG Report states:

---

3 Report of the Electronic Commerce Expert Group to the Attorney-General, *Electronic Commerce: Building the Legal Framework*, March 1998, available at: <http://www.law.gov.au/aghome/advisory/eceg/single.htm>.

4 Discussion Report of the ATO Electronic Commerce Project, *Tax and the Internet*, August 1997, available at <http://www.ato.gov.au/ecp/ecp.htm>.

5 The reports themselves contain numerous examples of electronic commerce, see for example: ATO Report *ibid* at 28-33; M Adams, R Kuras and J Law, *Putting Australia on the New Silk Road: the Role of Trade Policy in Advancing Electronic Commerce*, Department of Foreign Affairs and Trade (1997) at 45-63 (the DFAT Report); and *The Emerging Digital Economy*, note 1 *supra* at Appendices 3, 4 and 5. See also D Tapscott, *The Digital Economy, Promise and Peril in the Age of Networked Intelligence*, McGraw-Hill (1996); and E Schwartz, *Webonomics: Nine Essential Principles for Growing Your Business on the World Wide Web*, Penguin (1997).

> Electronic commerce is a broad concept that covers any commercial transaction that is effected via electronic means and would include such means as facsimile, telex, EDI, Internet and the telephone. For the purpose of this report the term is limited to those trade and commercial transactions involving computer to computer communications whether utilising an open or closed network.[6]

One form of electronic commerce, Electronic Data Interchange (EDI), was first introduced in the sixties. EDI is a standard used to transmit information such as orders, invoices, shipping instructions and bills, between computers. The main advantage of EDI was that it created a paper free system of inter-business communication, linking companies such as manufacturers, suppliers and transport providers. For example, the manufacturer's computer would identify that supply of a particular part was running low and send an electronic order to the parts supplier's computer for a shipment of that particular part. This created considerable savings in terms of employee time, wasted stock, lost customers, stationery and fax and phone bills. However, its use was limited by cost and compatibility problems. All parties involved in the transaction needed to have the same system installed.[7] Nevertheless, EDI demonstrated that enormous cost savings could be made in the design, ordering, processing and warehousing of products, particularly in the areas of stationery, employee time and postage.[8] With the emergence of the Internet, more businesses and smaller businesses can access the advantages offered by EDI without expensive proprietary systems.

According to the ECEG Report, electronic commerce will:

> [r]educe the cost of transactions, reduce barriers to entry into business and in some cases remove the necessity for a physical presence into any particular market.[9]

Electronic commerce will provide the means for developing an ongoing business relationship with new customers and partners around the world. A consequential benefit to consumers will be increased choice and increased competition. It will facilitate the provision of information around the clock and it will enable the automation of purchases and inventory control and ordering. It will save time and money and increase efficiency as well as providing a fast means of monetary transfers.

In light of the potential benefits on offer and the pressures of international competition, it is essential to provide assistance to Australian businesses to move onto the information superhighway. The Report of the Information Industries Task Force, *The Global Information Economy: The Way Ahead*, stated that it is necessary, as a matter of urgency, to get Australian businesses on-line:

> Doing business on-line provides new opportunities in the nature of business and new business opportunities. It also provides new one-to-one, as well as the more traditional one-to-many, customer relationships and greater opportunities for

---

6 Note 3 *supra*, para 1.21.

7 D Petre and D Harrington, *The Clever Country: Australia's Digital Future*, Lansdowne Publishing (1996) p 174.

8 Note 1 *supra* at 14. One company has reported a 30 per cent saving in labour costs and 20 per cent saving in material costs by moving to an on-line procurement system. This has also facilitated access to a wider supplier base, resulting in further cost savings.

9 Note 3 *supra*, para 1.2.

customer-supplier interaction. New skills are required to take full advantage of these new opportunities.[10]

This view is endorsed by a Report released last year by the Department of Foreign Affairs and Trade.[11] That Report considers the export opportunities created by the Internet for Australian businesses in accessing international markets and is intended to stimulate and encourage further discussion on the potential of electronic commerce, particularly for small to medium sized enterprises.

II. PROBLEMS

Australian businesses have been slow to take up the new opportunities offered by electronic commerce. The Information Industries Task Force recognised that it may be necessary for the government to 'kick start' electronic commerce by encouraging and coordinating industry development and by leading by example.[12] There are a number of reasons for the relatively low activity of Australian businesses in the on-line marketplace.

A. Payment Mechanisms

The Internet facilitates transactions between parties on opposite sides of the globe, at any hour of the night or day, for small or large amounts. This creates some unique problems in terms of payment.

Currently the most popular way of paying for a consumer transaction completed on the Internet is by credit card. Due to the nature of the Internet itself, there are risks involved when credit card information is not sent through a secure server or encrypted before transmission.[13] Further, a credit card is not acceptable for all forms of transactions. Sometimes the amount involved is too small or the purchaser wishes the transaction to be anonymous or may not have access to a credit card. Another issue is that consumers face the risk of misunderstanding the amount of the charge they are incurring when the price is quoted in foreign currency.

A great deal of attention has been focussed on the development of digital cash, which promises to allow consumers to make small anonymous purchases on the Internet. Digital cash is a string of digits, issued by a bank and attributed with a defined value (a ten dollar token for example). Each token is validated by the bank with a digital 'stamp' which it uses to verify the token when it is redeemed by the merchant to whom payment has been made. Although strings of digits may be easily replicated the inclusion of the authentication stamp by the bank ensures that each token is unique and may be used only once.

A further option is the digital cheque, which essentially operates on the same principles as a paper cheque, in that it acts as an authority to transfer funds from

---

10 Report of the Information Industries Task Force, *The Global Information Economy: The Way Ahead*, July 1997 at 63.

11 DFAT Report, note 5 *supra*.

12 Note 10 *supra* at 66.

13 See 'B. Security Risks' below.

the payer's bank to the payee. One advantage over paper based cheques is that the electronic cheque can be encrypted to keep the account details of the payer a secret from the payee.

Smart cards or stored value cards, similar to cards commonly used for photocopying or telephone calls, are also available. These cards carry a value, which may or not be rechargeable. More sophisticated versions are called wallets which may be recharged by the user from their bank account in the same sense as they would fill up a real wallet. Each time a transaction is made value is debited from the card and transferred to the merchant. A smart card can be made more secure with the addition of a Personal Identification Number (PIN).

B. Security Risks

The major impediment to the development of electronic commerce is the inherent security risk involved in transferring information such as credit card details and personal information over the Internet. There are two major concerns: first, identification integrity: you are who your signature says you are; and secondly, message integrity: you may have sent the message but has it been tampered with in between the time that it was sent by the sender and received by the intended recipient? These concerns create problems for both parties to the transaction. The purchaser risks theft or misuse of their personal and account information and the merchant risks repudiation of the transaction and resultant non-payment.

The Internet is an open system, a 'network of networks', with no single authority in charge of its use or development. When a message is sent over the Internet it is broken down into 'packets' of a fixed size, which are individually addressed to the Internet Protocol (IP) address of the intended recipient. Each packet is then sent to that address. The packets may take a different route to reach the final destination point where they are reassembled into the complete message. As each of the packets travel through the global network of computers that makes up the Internet, any of these packets of information may be intercepted, read and altered. For example, a credit card number is small enough to consist of only one packet of information. That number may be intercepted, read and used by any person with sufficient skill and inclination to do so.[14] However, encryption techniques are now available to prevent this interference by encoding the relevant data.[15]

Encryption involves the encoding and decoding of information by use of an algorithm.[16] With public/private key encryption, each user has two 'keys'.[17] The

14 There is of course always a risk that a credit card number, provided to a merchant during an authorised transaction, can be misused in the real as well as the virtual world. For example, when giving your number over the telephone to make a theatre booking or place a purchase order, the number may be overheard or may be used by the service assistant in an unauthorised manner.

15 In Australia, for example, strong encryption systems such as 'PGP' ('Pretty Good Privacy') are available.

16 The algorithm is a mathematical equation which transforms the plain text of the message into code which can then be unencoded with the correct 'key'. Different algorithms form the basis of different forms of cryptographic systems.

17 The 'strength' of the encryption depends upon the length of the key, the longer the key, the harder it is to 'crack'. It also takes longer to encode/unencode the data.

public key is made available for use by anyone who wants to send a message to the owner of the key. The sender uses the public key to encrypt the message which can then only be decrypted by use of the private key. The private key may also be used to encrypt a message which can be decrypted by anyone with access to the public key. The primary purpose of public/private key encryption is to maintain message integrity in the sense that the message can be identified as having originated from the person with access to that private key, that is, authorship integrity.[18] To some degree it also protects the security of the information in transit, although it may be read by anyone, in addition to the addressee, who has the sender's public key.

For this system to be effective there must still be some means of initially ensuring that the person issued with the keys is who they purport to be. Therefore there must be some certification or authentication authority who is responsible for the verification of keyholders.[19]

Other technological solutions based on encryption techniques operate at various levels of the Internet. Secure Electronic Transactions (SET) is a protocol developed jointly by MasterCard and Visa to secure credit card transactions over the Internet. It both protects the confidentiality of the transmission and ensures the authentication of the user. Secure Sockets Layer (SSL) is a protocol to provide security for Web transactions by encrypting packets of information transmitted to the Internet site. Encryption does not ensure absolute secrecy of information. Once information is unencoded at the end of the transaction it is still vulnerable to misuse by people having access to the computer storing that information.

Another problem is identity. Some readers may be familiar with a cartoon of a dog, seated at a computer, surfing the Internet for recipes, the joke being that on the Internet no one knows that you are a dog. Jokes apart, this issue has serious ramifications. It is difficult to tell if anyone on the Internet is who they say they are. Digital technology makes it cheap and easy to imitate or copy another person's trading name or image. The design and development of a glamorous Web page is far cheaper than the creation of an imposing shop front. One of the key attractions to many users of Internet facilities such as discussion groups, multi user dungeons and Internet Relay Chat is that you can assume an identity which bears no relation to who you are in the real world.

The Australian Competition and Consumer Commission (ACCC) Discussion Paper[20] refers to a recent example which demonstrates the ease with which consumers on the Internet can be deceived into believing they are dealing with a legitimate business. In April 1997, Microsoft became aware that a number of its customers had received an email stating that "[d]ue to a complicated problem with our system, we have lost the information that links your account's sign-on name and password with our billing record". The message requested customers to forward their credit card number, bank details, address and other confidential

---

18 Also called a 'digital signature'.

19 Australia Post currently offers such a service in Australia called KeyPost.

20 Australian Competition and Consumer Commission Discussion Paper, *The Global Enforcement Challenge: the Enforcement of Consumer Protection Laws in a Global Marketplace*, August 1997 available at: <http://www.accc.gov.au/docs/global/httoc.htm>.

information to "MSN Credit Department", to attract a 50 per cent discount off the next month's bill.[21]

In addition there are other general concerns about unauthorised access. Companies are anxious that if they connect their corporate system to the Internet, this will encourage and facilitate the 'hacking' of their systems. Again, systems are available to minimise the likelihood of a security breach. The installation of a firewall will prevent unauthorised access to company data.[22]

C. Copyright

The Internet is perceived as a "natural, low-cost distribution channel"[23] for information and entertainment products such as films, music and books. Such products are currently distributed in physical formats as videos, compact discs and paperbacks, but could easily be downloaded from the Internet by the consumer. Concerns about inadequacy of current copyright protection have prevented further developments in this area.

The Australian Federal Government has recently announced that reforms will be made to the *Copyright Act* 1968 (Cth) to include a broad based, technology neutral right of communication to the public which will apply to works made available through the Internet and other on-line services.[24] To further strengthen rights of copyright owners in the face of technological challenges, the reforms will also deal with abuse of copyright protection mechanisms, such as program locks. The reforms also address issues associated with tampering with and alteration of rights management information. These reforms should go some way towards easing the concerns of businesses wanting to deal in copyright materials on the Internet, but who have been reluctant to do so because of copyright concerns.[25]

D. Consumer Issues

As the use of the Internet for consumer transactions increases, so will a range of consumer problems. Particular concerns regarding exploitation of unwary customers will stem from factors such as:

- the Internet merchant may have no physical address or may be located in another country, making it difficult to return the product;
- there may be no access to local follow up service or repair;

---

21 *Ibid* at 24.

22 A 'firewall' is a security system, incorporating both hardware and software devices, providing a barrier between the company's internal computer network and the Internet. It operates as a single point of control for network security, filtering all incoming and outgoing messages.

23 Note 1 *supra* at 33.

24 The Hon Daryl Williams, Attorney-General and Senator the Hon Richard Alston, Minister for Communications, the Information Economy and the Arts, "Copyright Reform and the Information Economy", Joint Media Release, 30 April 1998: <http://law.gov.au/aghome/agnews/1998newsag/Joint_6_98.htm>. These reforms build on the proposals outlined in the Discussion Paper prepared by the Attorney-General's Department and the Department of Communications and the Arts, *Copyright Reform and the Digital Agenda: Proposed Transmission Right, Right of Making Available and Enforcement Measures*, July 1997.

25 The US is also introducing copyright reforms in this area. The *Digital Millennium Copyright Act* was passed by the US Senate on 14 May 1998.

- the product may not be suitable for local conditions or incompatible with local requirements;
- the Internet provides numerous ways to conceal the identity of traders, making it difficult to obtain redress in the event that the consumer is dissatisfied with any aspect of the transaction or if delivery is not made; and
- growth in privacy concerns, particularly where sales are targeted at children, who may naively reveal their address or hand out credit card or other sensitive information.

The ACCC released a Discussion Paper in August 1997 which intended to stimulate discussion on the issue of how best to protect consumers in the global marketplace. It acknowledged the existence of a broad range of consumer issues and the difficulties of regulation. The Discussion Paper notes that because of difficulties of jurisdiction, cost, delay and enforcement, reliance upon legal remedies alone for resolution of these kinds of cross-border disputes is not sufficient. It recommends the development of new consumer protection initiatives including coordinated law enforcement and compliance strategies, industry self-regulation and cooperation in the formulation of rules for the global marketplace.[26]

Clearly, with regard to consumer issues, there is a need for an international approach through initiatives such as harmonisation of laws and cooperation by law enforcement agencies. The Discussion Paper outlines a set of strategies for consideration by government, industry and consumer groups.[27] These include: improved cooperation between government enforcement agencies and industry bodies, consumer education programs, maintenance and sharing of information databases relating to scams and fraudulent dealing, the development of industry certification standards and codes of conduct, harmonisation of international standards and development of dispute handling mechanisms. The strategies consider a broad range of alternatives and involve a detailed consideration of all relevant bodies who may be involved in the process.

The Internet Industry Association of Australia has produced an Internet Industry Code of Practice, now in its third draft.[28] One of the aims of that Code is to "establish confidence in and encourage the use of the Internet". As part of that aim, the Code includes a requirement for all parties subscribing to the Code to provide details on their website of their Australian Company Number, their physical office address and contact telephone number, when entering into a transaction with a user. It also includes a prohibition on engaging in conduct which is misleading or deceptive, unconscionable or exploitative.

These initiatives should go some way towards easing consumer concerns, but in order to be efficient, they clearly require global cooperation.

---

26 Note 20 *supra* at xv.

27 *Ibid* at 92-100.

28 <http://www.iia.net.au/news/code3.html>.

E. Jurisdictional Issues

Just as electronic commerce opens up new opportunities for international trade, it also opens up new questions regarding application of laws to transactions conducted wholly or partially, on-line.

The ACCC has already noted an increase in complaints it receives from both Australian consumers regarding products and services purchased from other countries and complaints from overseas consumers about products purchased from Australia.[29] Consumer complaints regarding purchases made over the Internet from overseas entities are difficult to resolve on an individual basis because of questions about jurisdiction, enforceability and the resultant costs and delays. Jurisdictional rules such as place of transaction and the law of the contract are made obsolete by the borderless nature of the Internet. Unscrupulous traders will find it easy to avoid regulation in the electronic marketplace without a cooperative global approach to these issues.

F. Taxation

As with any new business venture, the viability of electronic commerce is going to be at least partially determined by the applicable tax regime. The US has taken the position that there should be "no discriminatory taxation against Internet commerce".[30] In particular, it advocates that the Internet should be a tariff-free zone. The ATO Report notes that the tariff-free policy advocated by the US does not extend to tangible products ordered and paid for on-line but delivered in the conventional manner.[31]

The ATO Report follows an extensive review of the impact of electronic commerce on the Australian taxation system. The Report is intended to stimulate further discussion at both national and international levels, prior to formulating the ATO's final recommendations to be made to the Australian government. The Report states that key principles of international taxation, such as source of income, residency and place of permanent establishment are "seriously challenged" by the emergence of electronic commerce.[32]

The Report makes a number of "findings"[33] including:

- the lack of a legal infrastructure supporting a secure, consumer friendly environment is likely to be an impediment to electronic commerce, particularly in the context of larger transactions;
- the development of reliable, easy to use electronic payment systems is fundamentally important to the efficiency of Internet markets;
- electronic commerce will increase the number of businesses engaged in international trade and reduce the average transaction size;
- in the short term, electronic commerce may adversely affect Australian

29 Note 20 *supra* at 28.
30 Note 1 *supra* at 51.
31 Note 4 *supra* at 40.
32 *Ibid* at 34.
33 *Ibid* at 76- 89.

business, but this trend could be reversed in the longer term. This could lead to some medium term impact on Australia's tax base, which would be corrected in the longer term;

- the impact on the taxation system of electronic commerce varies between industries;
- some electronic payment systems, such as digital cash, have significant potential for tax evasion because it facilitates rapid global anonymous transactions;
- the application of existing jurisdictional rules which rely upon some physical or territorial nexus to Australia, is doubtful. Further, the digital environment provides significant scope for manipulation of factors applied to establish jurisdiction, such as place of business and the law of the contract;
- due to the fact that different nations have different economic interests to promote with respect to electronic commerce, allocative[34] tax rules may be difficult to clarify but enforcement rules, because they are mutually beneficial, should be easier to determine;
- broad based international cooperation will be necessary to effectively administer domestic taxation laws with respect to electronic commerce;
- electronic commerce technologies, such as encryption, can be used to reduce the availability and reliability of information required for taxation administration, such as transaction accounts and business records;
- encryption presents difficulties in terms of the facilitation of crime and tax evasion but is an inevitable component of the successful development of electronic commerce;
- laws regarding the ATO's information gathering powers and rules regarding record keeping and retention will need to be modified to apply to the electronic environment; and
- the effectiveness of existing collection mechanisms is reduced by electronic commerce because it facilities numerous, small and direct transactions, removing the need for an intermediary, such as the importation agent, who has often been responsible for the collection of tax.

The Report makes a number of recommendations on the basis of these findings. Of particular relevance is the need for international consultation and cooperation with respect to the regulation of electronic commerce and the enforcement of taxation laws. The Report also recognises that taxation policies associated with electronic commerce should be developed in cooperation with other federal government agencies who are currently examining a range of other issues related to the on-line environment.

---

34 'Allocative rules' deal with the allocation of taxation rights between nations and 'enforcement rules' deal with how those taxation rights may be enforced on the basis of those rules, *ibid* at 35.

Whilst the Report recognises that "the ATO should be sensitive to the effect of e-commerce regulation on the nascent Internet commerce industry in Australia"[35] it also makes a number of recommendations which the industry may regard as controversial. For example, the ATO advocates the licensing of both 'web shops'[36] and organisations that operate or host web shops.[37] In order to ensure a greater degree of control over tax reporting, the Report also suggests that a framework to monitor commercial Internet traffic should be established in consultation with the Attorney-General's Department, the Department of Communications, the Information Economy and the Arts and AUSTRAC.[38] As part of this process, a record of the range of IP addresses assigned to Australian based computers should be maintained and the reporting requirements relating to a 'cash dealer' under the *Financial Transactions Reports Act* 1988 (Cth) should be reviewed to capture digital cash transactions. The ATO should also negotiate with software manufacturers regarding the inclusion of some form of 'date stamping' or other means of ensuring the integrity of transactional records in software used for electronic commerce.[39] The Report also recommends that major international credit card and other electronic payment system providers should be requested to provide access to transaction records held outside Australia.[40] With regard to electronic cash, the ATO recommends that the same arrangements that currently apply to reporting of physical cash transactions should be applied and reloadable cards which do not carry proper identification should have a maximum value of $100-$500.[41]

The efficient functioning of electronic commerce requires all of these issues to be dealt with in ways that are both technology neutral and which have worldwide endorsement and recognition.

III. PROPOSALS

A. Australian Government Initiatives

This flood of government reports relating to electronic commerce which has been raging over the last six months, indicates that there has been a great deal of consideration given to the problems inhibiting the growth of on-line commerce.

In addition to the various specific working groups involved in the preparation of these reports, the Government has established the National Office for the Information Economy (NOIE).[42] NOIE is responsible to the Minister for Communications, Information Economy and the Arts and is responsible for the

35 *Ibid* at 97.

36 A 'web shop' is any site which offers for sale goods or services, and may vary in size from a single person operation to a large commercial enterprise, *ibid* at 14.

37 *Ibid* at 106-7.

38 *Ibid* at 108.

39 *Ibid* at 109-13.

40 *Ibid* at 114.

41 Intended to be roughly equivalent either to the size of the largest unit of a cash transaction, the $100 note, or to the amount available when withdrawing cash from ATMs, *ibid* at 119-20.

42 <http://www.noie.gov.au/aboutnoi.html>.

development, coordination and overview of policy relating to the facilitation of electronic commerce.

B. Report of the Electronic Expert Group to the Attorney-General

The ECEG Report conveys a strong sense of the complexity of the questions discussed above. Clearly there is a recognition of the need to formulate some infrastructure to accommodate the development of a strong Australian presence in an on-line marketplace. The Report recommends the introduction of Commonwealth electronic commerce legislation. This is intended to create a basic legislative framework, providing a national scheme that "reduces uncertainty about the use of electronic commerce and removes existing legal obstacles to its use".[43]

The legislation would deal with the following issues:

1. the legislation should so far as practicable be technology neutral;
2. the legislation should apply to "data messages"[44] used in trade or commerce or with government;
3. careful consideration needs to be given to any exceptions made to the legislative framework in respect of particular instruments or transaction types;
4. variation of the terms prescribed by the legislation should be permitted by agreement between the parties. Any variation should be subject to a reasonableness test akin to that prescribed by s 68A(3) *Trade Practices Act* 1974 (Cth);
5. the legislation should contain a specific acknowledgment that information, records and signatures should not be denied legal effect solely because they are in electronic form;
6. where a law contains a requirement of "writing" this should be satisfied by a data message;
7. where a law contains a requirement of a signature or a signed document, electronic signatures may be given legal effect, subject to minimum standards relating to authentication technology giving equivalence to traditional signatures;
8. legal requirements of 'originality' contained in statute or common law could be satisfied by reference to information integrity or authenticity;

---

43 The Report identified the Constitutional basis for the power to legislate in this area as the posts and telegraphs power (s 51(v)), the banking power (s 51(xiii)), insurance (s 51(xiv)), bankruptcy and insolvency (s 51(xvii)), the corporations power (s 51(xx)), external affairs power (s 51(xxix)), the incidentals power (s 51(xxxix)), freedom of interstate trade (s 92) and the territories power (s 122); note 3 *supra*, para 4.4.12.

44 "Data message" is defined in the United Nations Commission on International Trade Law, "UNCITRAL Model Law on Electronic Commerce with Guide to Enactment", United Nations (New York 1997), Article 2 as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy." See: <http://www/un/org/at/uncitral/-en-index.htm>.

9. the Commonwealth and NSW Evidence Acts[45] provide an appropriate model regarding the admissibility and evidentiary value of electronic documents and data messages;
10. the record retention requirements for paper based and electronic commerce should be equivalent;
11. there is a need for clarification and certainty regarding the elements required for conclusion of a valid contract via the transmission of data messages;
12. default provisions regarding attribution should provide that a person purporting to be the originator of a message should only be bound if they in fact sent that message or it was sent upon their authority. The onus of proving this should remain with the addressee. In general, rules of attribution should be determined by agreement between the parties, a party only being able to rely on such rules if it is fair and reasonable in all of the circumstances;
13. no legislation is needed to deal with the question of acknowledgment of receipt;
14. provisions dealing with time and place of receipt need to be developed;
15. no specific action is necessary at this stage with respect to electronic sea carriage documentation; and
16. recognition that there is a need for an international approach to these issues.

These recommendations were based upon a detailed consideration of the United Nations Commission on International Trade Law (UNCITRAL) Model Law. UNCITRAL is an international organisation which formulates rules and model operating principles designed to facilitate international commerce. The Model Law was completed in 1996. It is intended to provide national legislators with a set of basic rules that would remove a number of existing impediments to the encouragement and growth of electronic commerce. It is not a treaty or convention and therefore this scheme provides national legislators with greater flexibility of application. It may be enacted in whole or in part or used as the basis for amending existing legislation.

The Model Law was used as the basis for the ECEG considerations because it provides an internationally accepted set of rules. The report deviates from the wholesale acceptance of the UNCITRAL Model Law with respect to questions of attribution and acknowledgment of receipt of data messages. The Report states that whilst articles six to twelve are primarily concerned with the facilitation of electronic commerce by removing existing legislative and other legal impediments, articles thirteen to fourteen create new rules for the allocation of risk which may result in electronic commerce being treated differently from paper based commerce.[46]

45 *Evidence Act* 1995 (Cth) and *Evidence Act* 1995 (NSW).
46 ECEG Report, note 3 *supra*, para 4.5.77.

A number of jurisdictions have already adopted or are considering legislation based on the Model Law.[47] These provisions were also considered by the ECEG.[48]

The UNCITRAL Guide to Enactment states that the general principles on which the Model Law is based include:

- facilitating electronic commerce among and within nations;
- validating transactions entered into by means of new information technologies to promote and encourage implementation of new information technologies;
- promoting the uniformity of law; and
- supporting commercial practice.

The ECEG supported the inclusion of an interpretation provision articulating these principles in any legislation developed as a consequence of the recommendations.[49]

C. Digital Signatures

The issue of digital or electronic signatures was directly considered by the ECEG Report. Electronic signatures are principally concerned with ensuring message integrity. They ensure that the sender is the person whom they purport to be. This is akin to the role performed by 'real' signatures, however real signatures may also be intended to serve as an acknowledgment or acceptance of the contents of the document. The Report acknowledged that electronic signatures provide a means of promoting consumer confidence in one-off transactions because they provide some means of identification and the possibility of recourse in the event of problems with the transaction. However the ECEG declined to recommend that any one specific electronic signature regime should be endorsed. Instead, they recommended that any electronic commerce legislation produced as a result of the Report should deal simply with the effect of the electronic signature, stating that this is consistent with the 'principled', non-prescriptive approach of Article 7 of the Model Law and will avoid any legislative model proving to be technologically unworkable.[50]

In 1996 Standards Australia proposed a national system for the creation and management of digital signatures, based on public key/private key cryptography (PKAF).[51] The Standards Australia report recommended the development of a national framework to support authentication of users involved in electronic commerce, based on the creation of a single national authority, described as the Policy and Root Registration Authority (PARRA). PARRA would have responsibility for accrediting certification authorities in accordance with

---

47 For example, *Uniform Electronic Transactions Act* (November 1997) (US Bill), *Electronic Commerce Security Act* (December 1997) (Illinois Bill) and *Electronic Records and Signatures Act* (November 1997) (Massachusetts Bill). See ECEG Report, note 3 *supra*, para 2.0.11- 2.0.12.

48 See also note 1 *supra* at 22.

49 Note 3 *supra*, para 4.1.5.

50 UNCITRAL is currently formulating Uniform Rules on Electronic Signatures.

51 Standards Australia, *Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia*, SAA MP75-1996.

established criteria based on internationally agreed standards where available. Its role would also include cooperation with other national authorities to ensure a consistent international standard.

NOIE has been delegated with the responsibility for developing the National Public Key Authentication Framework and has commenced work towards establishment of PARRA.

Australia's international involvement in these issues has also extended to contributing to the development of the Cryptography Policy Guidelines by the OECD, which were adopted as the basis for Australia's domestic cryptography policy in March 1997.[52]

D. Project Gatekeeper

In October 1997 the Australian Government's Office of Government Information Technology (OGIT) established Project Gatekeeper in order to streamline the use of public key technologies by government agencies for electronic transactions. This was considered necessary because several government agencies had been separately developing their own Public Key Encryption systems, based on differing standards, which, if allowed to continue, would undermine the transactional efficiency of electronic dealings. The Gatekeeper Report was issued by OGIT in May 1998.[53] It recommended the establishment of a Government Public Key Authority to determine policy and standards for the use of public key technologies, products and services by the Australian Government. It would also be responsible for the accreditation of public key technology service providers.[54]

The Internet is a global phenomenon and the promise of electronic commerce is that it will allow traders to reach out beyond national boundaries. It becomes abundantly clear that it is inappropriate and unproductive for these issues to be dealt with solely at a national level. The ECEG report recommended that, in order to facilitate electronic commerce, Australia should promote consideration and adoption of the UNCITRAL Model Law at an international level. This policy is consistent with current US initiatives.

E. US Initiatives

The US is recognised as a global leader in the development of electronic commerce. Given the fact that the Internet sprang from a US Department of Defence initiative and has been nurtured since the sixties by US Government and academic agencies, this fact is hardly surprising. The Internet was only opened to

52 <http://www.oecd.org>.

53 Office of Government Information Technology, *Gatekeeper: A Strategy for Public Key Technology use in the Government*, 6 May 1998, available at <http://www.ogit.gov.au/>.

54 The technology and systems structure proposed by the Gatekeeper report is based on the Standards Australia proposals outlined in SAA MP75 (discussed above), however, it is envisaged that the Government Public Key Authority will be absorbed into the general national framework once this is established pursuant to the initiatives being undertaken by NOIE.

commercial traffic in 1991, shortly before the creation of the World Wide Web in 1993-94. The US still accounts for two thirds of all Internet users.[55]

On 1 July 1997, *A Framework for Global Electronic Commerce*[56] (the Framework) was released by the White House. It is intended to be a clear statement of the Clinton administration's vision for the future of the Internet as creating "a vibrant global marketplace", outlining US policies in the area and stimulating international consideration of these issues. It has been widely circulated and has been influential in shaping the thinking of other governments on the issue of electronic commerce. The basic premise of the document is that electronic commerce has enormous potential to revolutionise all forms of commercial transactions. For this potential (estimated in the order of tens of billions of dollars) to be fully realised "governments must adopt a non-regulatory, market-oriented approach to electronic commerce, one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce".[57]

The principles outlined in the Framework include an emphasis on the role of the private sector in the development of electronic commerce. There is a particular focus on the significant questions of industry self regulation; minimisation of government intervention and recognition of the value and the unique nature of the Internet. The Framework document also explores the modification of existing laws needed to accommodate growth of the Internet. It fully accepts that the Internet "is a global marketplace" and that rules should be predictable and consistent regardless of where the buyer or seller resides.

The Framework identifies nine key areas in which international agreements are necessary: customs and taxation; electronic payments; Uniform Commercial Code for electronic commerce; intellectual property protection; privacy; security; telecommunications infrastructure and information technology; content and technical standards.

With respect to taxation, the Framework advocates no new taxes on electronic commerce. In particular, goods and services delivered on-line should be tariff-free. Any taxation of Internet commerce should be based on three principles:

- the taxation system should be neutral. It should not discriminate between electronic or paper based forms of commerce, nor should it distort or hinder any form of commerce;
- the taxation system should be easy to use and administer for all parties involved;
- any amendment to the taxation framework should accommodate existing taxation principles and regimes.[58]

The Framework's findings with regard to the development of a commercial code to regulate electronic commerce sit well with the conclusions of the ECEG. Like

---

55 DFAT Report, note 5 *supra* at 12.

56 WJ Clinton and A Gore Jr, *A Framework for Electronic Commerce*, Whitehouse (1997), available at <http://www.ecommerce.gov/framewrk.htm>.

57 *Ibid.*

58 *Ibid.*

the ECEG Report, the Framework document states that any such code should be technology neutral; existing laws should only be modified so far as necessary to support the use of electronic commerce and parties should be free to modify their relationship by contract.[59] It also supports the use of the principles outlined in the UNCITRAL Model Law as a starting point for the development of an "international set of uniform commercial principles for electronic commerce".[60]

The US has already issued two joint statements on electronic commerce, one with the European Union and one with Japan. The "Joint EU-US Statement on Electronic Commerce"[61] recognises the importance of electronic commerce to worldwide economic growth and commits both parties to work towards international cooperation on issues affecting electronic commerce. The convergence of these two major powers in this project promises significant progress in the consideration and resolution of these issues.[62] That Joint Statement has made it clear that no new taxes should be imposed on goods ordered electronically and delivered physically and no duties should be imposed on electronically delivered goods and services. It emphasises the importance of industry self regulation. The "US-Japan Joint Statement on Electronic Commerce"[63] discusses a number of issues, including the need for a global framework for the recognition of authentication techniques and the development of consumer confidence in electronic payment systems. These documents indicate broad based international acceptance for the principle that leadership on these issues should be taken by the private sector supported by a non-discriminatory approach from government.

IV. CONCLUSIONS

It is apparent that governments worldwide perceive this as an area in which they can play a role but in which industry should lead.[64] Each of the documents referred to in this article begins with a statement about the potential and promise of electronic commerce to increase global trade, create economic prosperity, lead to greater choice and diversity and create new jobs. There is no absolute guarantee that electronic commerce will fulfil these expectations, or that necessary global cooperation will continue beyond the current initiatives. However, there appears to be at least a general agreement between some of the major powers about what needs to be done.

---

59 In the ECEG recommendations, this was limited by some reasonableness requirements, see above.

60 Note 56 *supra*.

61 "Joint EU-US Statement on Electronic Commerce", 5 December 1997, available at: <http://www.qlinks.net/comdocs/eu-us.htm>.

62 However, it should not be assumed that there is total harmony between the two powers. For example, the issuing of new Internet domain names, presently controlled by the US has yet to be resolved.

63 "US-Japan Joint Statement on Electronic Commerce", 15 May 1998, available at: <http://www.ecommerce.gov/usjapan.htm>.

64 See for example: the Framework, note 56 *supra*; *The Emerging Digital Economy*, note 1 *supra* at 50; and the DFAT Report, note 5 *supra* at 39.

The Australian government can best contribute to realising the potential of electronic commerce by:

- leading by example as an early adopter of electronic commerce;
- establishing an effective physical infrastructure for on-line communication;
- establishing a minimum set of rules ensuring at least the equivalence of electronic with paper based transactions;[65]
- ensuring a level of consumer confidence regarding security and privacy concerns; and
- continuing to cooperate in the resolution of these issues at an international level.

One positive dimension to the dialogue that has been explored in this paper is the ready acceptance of the fact that the Internet is a valuable new medium and that it needs separate and urgent consideration. Early regulatory attempts had a tendency to view the Internet as something between the telephone and the television. It is also pleasing to note that this refreshing new understanding of the Internet as a commercial tool has led to a recognition of the need for regulators to consider concurrently issues from other areas of concern, such as privacy, intellectual property and defamation, which were previously being considered as isolated regulatory issues.

Having surveyed the lands of electronic commerce and produced a rudimentary road map of how to proceed, it is now necessary, as a matter of urgency, to identify the appropriate forum for the essential international discussions. It is important that the fundamental work represented in the these reports is continued and that the whole issue is not relegated to the 'too hard basket'. Clearly the bulk of the work of developing electronic commerce will be left to the private sector but some government input is still required to protect consumers and to establish and maintain standards. The real problems are yet to emerge, as the bulk of consumers and merchants are currently kept out of the on-line marketplace by security concerns and payment difficulties. Once a secure, efficient and international model of digital payment is established it will be too late to step in and consider how best to impose regulation. Now is the time to recognise the promise and potential of electronic commerce and to ensure it works for all Australian businesses, rather than leaving us behind, bound by the shackles of a paper based commercial system.

65 See for example: the Report of the Information Industries Task Force, note 10 *supra* at 71; the ATO Report, note 4 *supra* at 92.