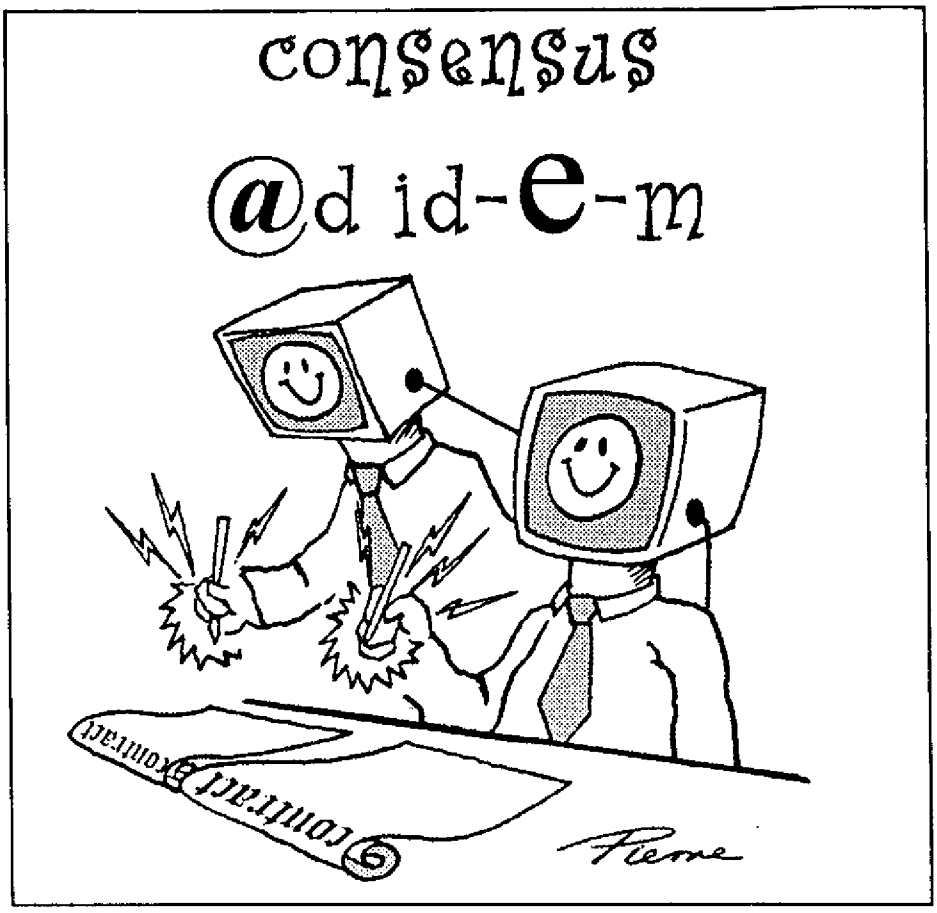
Overcoming the Legal Barriers to E-business

The jury is out on the scope and extent of regulation of the Internet. Catherine Dickson provides a compelling analysis of the issues.

By just about all accounts, the pace of growth and take-up of the Internet is enormous, outstripping every other technological development in recent times. E-commerce is not only becoming an important part of retail business, but also business-to-business transactions. Alan Greenspan was stating the obvious when he said that information technologies have begun to alter the manner in which we do business and create value, often in ways not readily foreseeable even five years ago. Despite the recent spate of computer hacking and viruses, the Internet is establishing itself as the most likely mechanism that business will use to effect electronic commerce.



The Internet is a technological innovation that has expanded over the last five years at an exceptional rate. The Department of Trade & Industry in the UK ("ÐTI") published some revealing figures in April this year showing that 33% of businesses in the UK are buying and selling over the Internet. However 60% of businesses have had a security breach in the last two years and 43% of these breaches were serious. Despite this, only 14% of companies have any formal information security in place. No wonder consumers are concerned about the safety of the Internet. General consensus is that consumer confidence will grow once the security issues have been solved and properly explained to the public. Trust must be established in the electronic environment. At the moment:

> *"[c]onsumers new to e-commerce sense a kind of chaos in the Web, where information is vulnerable to hackers, technology is unreliable and good intentions may lead to unpredictable results"*[1].

Online trading is not necessarily as simple as it may appear at first. Take as an example a business-to-consumer electronic trade where you, the seller, and your customer are in the same jurisdiction, and ask yourself these questions:

- are you allowed to trade in the goods and services at all?
- if you are, do you need regulatory approval beforehand?
- are you allowed to advertise this online trade?
- have you structured the trades to recognise local contract formation rules, like invitations to treat, offers and acceptance?
- have you effectively incorporated in your online contract all the terms of trade and managed your legal risk?
- what law is there in the jurisdiction that could override your terms and grant your online customers rights and greater redress than you had ever intended?

Until recently lawyers have had to look to the laws of one or maybe two jurisdictions to answer these questions. However, by definition electronic business transcends national borders making the above questions almost impossible to answer confidently. It is also paperless, there are no handwritten signatures or original paper documents that can validate the contract. To add to this, most modern contracts are effected by means of some personal interaction – usually a face-to-face meeting between the parties. In the e-commerce environment it is highly likely that the parties to the transaction will never meet. To overcome this lack of face-to-face involvement it is necessary to rely on identity authentication mechanisms.

There are a number of uncertainties and risks associated with electronic commerce. However, identifying the risks should not stop the pursuit of opportunities that the Internet presents. The Internet has flourished because of people learning by getting in and *having a go*. Like all other business risks, the risks associated with e-business need to be identified and managed.

CATEGORISATIONS OF RISK

There are three kinds of risk. These are:

- service dependency/liability risk;
- regulatory risk; and
- systemic risk.

Service Dependency/Liability Risk

These are risks inherent in using the technology. For example, delivery of a product online carries with it far more risk to the supplier than physical delivery. Once an electronic message leaves the network, neither party is likely to have any control over it as the message is carried by countless different pathways over land, sea or in space. There are few, if any, legal rules that allow a supplier to argue that it should not be held liable for non-delivery or late delivery even though these events are outside the supplier's reasonable control. In this context, there is a clear legal risk in online trading that contracting parties must accept. To manage this risk the parties need to be aware of the laws governing the contract and the terms of the contract should be worded so as to allocate the risk fairly between the parties.

Regulatory Risk

This is the risk that the relevant law either prevents or severely restricts electronic trade. This category is different from systemic risk because the laws here are specifically aimed at electronic business or other electronic transactions, *eg* data protection laws, consumer protection legislation and online gambling legislation.

Systemic Risk

This is the risk that legal systems do not recognise, or create uncertainty in, online traders' legal rights and responsibilities. Despite recent progress, all legal systems suffer from systemic risks. The most common of such barriers are:

- the need for some transactions to be in writing and the need for an original document that is signed or delivered in some way;
- limitations on the extent to which electronic data can be used in court as evidence;
- lack of clarity of the rules for electronic contract formation. For example, does the postal acceptance rule apply or does a communication via the Internet have more in common with the more instantaneous forms of communication *eg* telephone or facsimile? If so, the recipient must receive the communication in order for the message to be effective. And when is communication received? When it hits the mail server? Or perhaps when it arrives at the recipient's PC? Or is it when it is opened by the recipient?
- electronic signatures are not yet recognised. Governments need to put frameworks into place that will establish a method of signing electronic contracts which will establish the integrity and authenticity of electronic communications as well as possibly the identity of the sender;
- that in some countries, electronic invoicing and electronic payments are not always specifically or adequately recognised;
- as things currently stand, Governments and the World Intellectual Property Organisation are in the process of adapting intellectual property rights protection to digitised products and services. There continues to be real risks that intellectual property rights in online trades cannot be enforced effectively;
- there is no internationally agreed way of resolving, cost effectively (or at all), disputes arising from online trades; and
- there are no internationally agreed rules and procedures for determining jurisdiction issues.

Systemic risk is the most difficult kind of risk to manage because the risk is the inherent uncertainty in the legal environment in which the transaction is made. Generally the law has to be changed to reduce this risk. Nevertheless, to an extent this risk can be overcome and worked around where the parties set their own contractual rules, for example determining how and when binding contracts will be formed and where and when electronic messages will be received. This is common in electronic data interchange agreements. However, this is generally recognised as an area where regulation can assist in creating certainty and trust in the Internet as a medium for business and consumer transactions.

IS REGULATION HELPFUL IN OVERCOMING LEGAL BARRIERS?

As our understanding of e-business matures we recognise that domestic legislation as we know it is ineffective in controlling cyberspace. Only laws which can be enforced on a global scale can impose any restraints on the rules in cyberspace.

It is also being recognised that to a large extent the self-regulating structures of business are better suited than territorial laws to deal with on-line legal issues. Apart from acting as exemplars, governments should only step in where it is necessary to create certainty or to protect citizens. Nevertheless governments need to act consistently and authoritatively. Any such authority needs to be derived from international, rather than territorial institutions.

It has been recognised world-wide that the systemic risks described earlier are one such category of problems that can be assisted, by regulation if only to establish trust and certainty in the Internet. There will certainly need to be international co-operation as to how to approach these problems. Possibly also some kind of international arbitration body or international court to provide a last resort determination. There needs to be agreement on an international level as to what systemic risks in Internet transactions require legislative intervention and which can be left to the contract to rectify.

INTERNATIONAL INITIATIVES

There have been various international initiatives to harmonise national legislative initiatives including those of the OECD and APEC. An influential third international initiative is driven by the United Nations Commission on International Trade Law ("UNCITRAL"). UNCITRAL developed the Model Law on Electronic Commerce in 1996. The basic purpose of the Model Law was to establish an equivalence between electronic and paper transactions through a process of "functional equivalence". UNCITRAL says the function of a signature is to identify the signatory (establish authenticity) and the consent of the signatory to the contents of a document (establish integrity). Consequently, any electronic message that fulfils both these functions ought to be regarded as legally acceptable. Similar considerations were used to establish the types of electronic documents that ought to be considered legally valid. Legislation based on the Model Law has been adopted in Singapore, USA and Australia and has been tabled in Colombia and Canada.

The Model Law is also under consideration in Mexico, New Zealand and Thailand. UNCITRAL is now preparing Draft Uniform Rules for Digital Signatures to supplement the Model Law on Electronic Commerce.

The latest draft UNCITRAL framework has moved away from the concept of digital signature technology tied to a specific signing method. However, the draft rules still incorporate a definition of "enhanced electronic signature" that favours public key infrastructure ("**PKI**"). Concerns have been expressed that this emphasis on enhanced signatures tends to make too complex what should be a minimalist framework.

The European Union

The European Union ("**EU**") Directive on a common framework for electronic signatures took effect on 13 December 1999. Member States are required to implement the Directive by 19 July 2001. The explanatory memorandum to the Directive explains that electronic commerce presents the EU with an excellent opportunity to advance its economic integration.

This EU Directive concentrates more on the problems associated with identity than does the Model Law. The explanatory memorandum agrees that electronic signatures should allow the recipient of electronically sent data to verify the origin of that data and to check that the data is complete and unchanged and thereby safeguard its integrity. However, according to the EU, verification of authenticity and integrity does not necessarily prove the identity of the signatory who creates the electronic signature. The Directive therefore establishes a legal framework for electronic signatures *and* certain certification procedures to satisfy the identity problem. It does not, however, cover aspects related to the conclusion and validity of contracts or other legal obligations.

Complementary provisions regarding on-line contracts are contained in the Electronic Commerce Directive that was approved by the European Parliament on 4 May 2000. Members are required to make these provisions law within 18 months. of its publication The on-line contracts section of the Directive obliges Member States to remove any prohibitions or restrictions on the use of electronic contracts. It also provides for when and where an electronic communication is concluded.

LEGISLATIVE DEVELOPMENTS

Recent developments suggest that the world is moving closer to agreement and co-operation in relation to regulation of electronic signatures and other systemic risks associated with the existence of electronic transactions, contracts and notifications. A technology neutral, minimalist approach is now preferred. Many governments in the US, in Europe and in Asia have attempted to take this approach. The UK has the Electronic Communications Act and Australia has enacted *Electronic Transactions Act 1999* ("**ETA**"). Both of which are *minimalist*.

The US in particular demonstrates a movement towards a minimalist approach especially with regard to electronic signatures. Initially, the *Utah Digital Signature Act 1995* was very prescriptive. However, since then the majority of states like California and Illinios have taken a more minimalist approach.

In 1999, the US Congress initiated a number of Federal Bills relating to e-commerce, the most notable of which was, for our purposes, the *Electronic Signatures in Global and National Commerce Act*[2] . The purpose of this Bill is to promote the use and acceptance of electronic signatures on an international basis using free market and technology neutral principles.

The argument for specifically adopting asymmetric cryptosystems is that a detailed regulatory system can be developed which should provide not only certainty, but will also allow for infrastructure development.

The arguments in favour of remaining technology neutral are flexibility and allowing for the development of new technologies to be market driven. Legislators are not necessarily in a position to predict the future with respect to either technological or legal developments. Rather than facilitating electronic commerce, it is argued that picking winners may fundamentally skew an infant market place and "lock in" a set of business models that the market would otherwise reject[3].

Electronic Communications Act ("UK Act")

The UK Act implements the EU Directive on a community framework for electronic signatures. The main purpose of the Act is to help build confidence in electronic commerce by providing for an approval scheme and legal recognition of electronic signatures. It also provides for the removal of obstacles in other legislation to the use of electronic communications and storage in place of paper. This is limited to the mechanism set out in Section 8 which gives the appropriate Minister the power to remove restrictions arising from other legislation and to enable the use of the electronic alternative. The DTI intends to use the power to amend the *Companies Act 1985* so that company communications, shareholder proxies and voting instructions can be delivered and received electronically.

Similar to the-ETA and the Model Law, electronic signatures are given explicit legal recognition on the basis that the courts will decide whether an electronic signature has been correctly used and what weight it should be given. The Act also establishes a scheme where trusted third party verifiers can be registered.

The UK Act as it currently stands is more flexible and market driven that the initial draft. The mandatory key-escrow provisions have been omitted. The Government dropped this in favour of a "*co-regulatory*" approach with industry. Further illustration is the preferred approach to the voluntary register of approved providers of cryptography support services. The Government is allowing a self-regulatory scheme to establish itself and has indicated that if the "T" Scheme is successful it will not exercise its powers to establish a statutory scheme.

Electronic Transactions Act 1999 ("ETA")

ETA largely implements the UNCITRAL Model Law. It was enacted on 25 November 1999 and came into operation on 1 January 2000. The legislation ensures that a transaction is not invalid simply because it has been effected via an electronic communication.

In keeping with Australia's technology neutral policy, the legislation does not deal prescriptively with electronic signatures. It merely allows a legal requirement for a manual signature to be satisfied by an electronic communication that contains a method that identifies the person (identification) and indicates their approval of the information communicated (authentication). The choice of a particular method must be as reliable as is appropriate in the circumstances. Where the signature is

required to be given by a person who is not a Commonwealth entity, that person must consent to the use of the signature method. For Commonwealth entities, an electronic signature must comply with any information technology requirements of the Commonwealth.

The Australian approach to electronic signatures has been criticised for not providing effective guidance to the judiciary as to what is an appropriate electronic signature as at the date of signing[4]. Adrian McCullagh asks *"When it comes to traditional signatures there are approximately 700 years of precedence upon which the judiciary can rely. In the e-commerce environment there is no such luxury. Will it take another 700 years before the courts will have sufficient precedents to deal with all of the possible variations of technology that could be reasonably regarded as a valid electronic signature in the circumstances?"*[5]. In particular, in light of the EU Directive, and worldwide acceptance of PKI at least for the present, it remains to be seen whether the failure to legislate to establish certification procedures will hamper Australia's efforts to overcome uncertainty in its laws for e-business.

As a legal practitioner in the area, I can say that generally the ETA creates a framework rather than establishing any real certainty for e-business. For example, the provisions regarding time of receipt of electronic communications are clearer where parties to a contract do not designate email as an acceptable "information system" for the purpose of receiving electronic communications. If email is selected then the time of receipt of the communication is the time when the electronic communication enters the information system. Is this when it arrives at the server or when it arrives at the individual's machine? Whereas, if no information system is designated for the purpose of receiving electronic communications then the default time of receipt of the communication is when it comes to the attention of the addressee.

However, the approach is consistent with Australia's light touch approach. In 1998 the Australian Government's advisory group, the Electronic Commerce Expert Group ("**ECEG**")[6] recommended that accommodation of electronic signatures could be achieved by the use of a generic principled approach and not a broader regime. It was also recommended that the Attorney General's Department should continue to monitor international developments in relation to electronic signature legislation, and in particular of the UNCITRAL Working Group. The National Electronic Authentication Council ("NEAC") has been established to do this and to develop a national framework for electronic authentication of online communications.

CERTAINTY AND MARKET FORCES

There are two major differences when comparing the ETA and the UK Act. The first is in relation to the procedure included in the UK Act for cryptography support services. Following the EU Directive this has been included in the UK Act to create more certainty in the market for the authentication processes. In doing this, the UK legislation has to some extent tied itself to the digital signature technology and has not remained entirely flexible and technology neutral. It may therefore be distorting market forces by backing a technology that might not ultimately be preferred by the market. However, it does create more certainty for the courts in determining the likelihood of fraud and so determining the appropriateness of the electronic signature for the transaction.

The second major difference between the two approaches is that the ETA has taken a more detailed approach to the other systemic risks associated with e-business. The ETA gives "media neutrality" or "functional equivalence" to:

- the giving of information or writing;
- providing a signature;
- producing a document;
- recording information; and
- retaining a document.

So that if there is a requirement under Commonwealth legislation to do such acts, effecting them by means of electronic communication will satisfy that requirement as long as there is consent by the parties to the information being given by way of electronic communications. Provisions are also made in the ETA for determining the time and place of the despatch and receipt of an electronic communication.

The UK Act on the other hand has not dealt with functional equivalence for e-business other than for electronic signatures. In relation to electronic communications and storage generally it gives the relevant Minister power to remove restrictions from other legislation. This is potentially much narrower than functional equivalence. Clause 7 will apply whenever electronic signatures are used, including those cases where there is no legislative impediment to the electronic option. By not establishing functional equivalence, the UK Act has left it to the courts to determine whether electronic contracts and electronic documents generally will be acceptable. This does not create certainty in the short term. However, with the recent approval of the EU Directive on e-commerce, the UK will be shortly enacting legislation to deal with systemic risks identified earlier and in particular relating to electronic contracts.

In setting a framework to overcome the legal barriers to e-business, legislators are faced with the competing demands of avoiding being too technology specific while creating a framework that is certain. Whether the differences between the UK Act and ETA will prove significant remains to be seen. What is more important is that national legislators act harmoniously so as to effectively deal with the systemic risks and to avoid creating further legal barriers to e-business.

1 Alan Greenspan – Chairman US Federal Reserve Board 6 May 1999.

2 1999 House Bill 1714.

3 Proponents of biometric authentication methods argue that it is foolish to legislatively enshrine public key cryptography. They argue that biometric methods can currently accomplish many of the same goals as digital signatures. They also argue that public key cryptography can only be implemented using patents owned by a limited number of commercial entities. Biometrics uses a person's biological makeup as a means of identification eg finger-printing. However, now irises and retinas can be scanned and individual voices can be recognised. Biometrics can be used both for verification (are you who you claim to be?) and identity (who are you?). It has the advantage over a PIN in that it is impossible to either forget or steal.

4 Adrian McCullagh *Legal Aspects of Electronic Contracts and Digital Signatures*, Going Digital 2000 Legal Issues for E-commerce, Software and the Internet, Prospect Media Pty Ltd.

5 Ibid p205.

6 *Electronic Commerce: Building the Legal Framework* dated 31 March 1998.

Catherine Dickson is a Senior Associate in the Sydney Office of Pricewaterhouse Coopers Legal.

Editor's note: At the time of publication, only Victoria and NSW had enacted "mirror legislation" to the ETA. A bill in South Australia is currently working its way through Parliament.