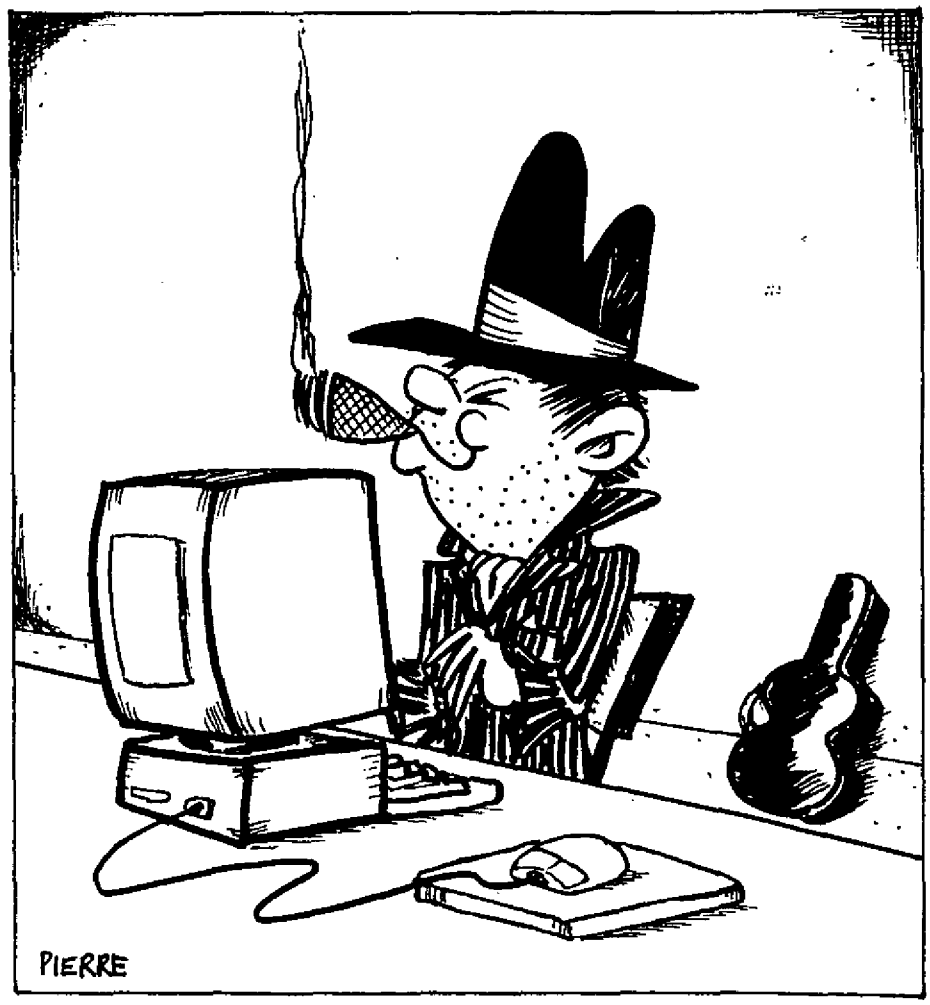
Convergence Towards the Millenium: Meeting the Challenges to Global Electronic Commerce

Diana Sharpe outlines some of the major issues challenging the development of legal and commercial rules for global electronic commerce and profiles some of the initiatives aimed at meeting the challenges.

The use of the Internet in electronic commerce is beset by a number of challenges and obstacles. There is no global business or legal structure to sustain a global electronic marketplace and ensure the security and privacy of transactions. There are no consistent business standards and practices for electronic commerce. The difficulty of addressing the challenges is heightened by the absence of a global forum for coordination and policy development.

The need for appropriate legal and commercial rules to support the use of the Internet is recognised and around the globe organisations are responding to the need to resolve the issues and remove the obstacles.



Major challenges to the use of the Internet in Global Electronic Commerce

Security and privacy issues

Commerce on the Net is an extremely complex topic for consumer protection, particularly when merchants, financial institutions, service providers and clients may be located in different states or nations. It can involve problems with client privacy, intellectual privacy, intellectual property, censorship, fraud and international money transfers.

There must be a basis for the trust that organisations place in commercial communication mechanisms. In some cases a level of security is built into the process: for example, by placing a document in a sealed envelope, the confidentiality of the information is considered to be maintained.

The knowledge that a mechanism is weak does not prevent its widespread adoption. The fax is an inadequate mechanism for commerce - there is no real authentication of the origin or destination, or any inbuilt confidentiality. However, its ease of use, instantaneous nature and obvious security benefits over the telephone (in that at least a hard copy is received) have meant that it has become widespread as a means of transacting business.

Some forms of open communication offer the same promise - Internet electronic mail has become widespread for all the same reasons: it is easy to use, inexpensive, widely accessible and offers soft-copy benefits over fax. It will, therefore, become widely used for electronic commerce, regardless of whether or not the security mechanisms are appropriate.

The introduction of electronic commerce is presumed to imply efficiency gains, increased competitiveness and opportunities for growth. This is why it receives government endorsement. The challenge is to provide security structures that enable all enterprises, whether large or small, to participate with confidence without affecting the accessibility and ease of use of the technology. Without these structures, uncertainty and mistrust will delay the adoption of the

mechanisms and all the threads of the fabric of commercial relationships will be weakened.

If electronic commerce is to make rapid inroads into business, it is essential that standards emerge rapidly, whether they be de-facto, through market dominance of one player, or through the national and internal standards bodies.

The uncertain legal status of message security mechanisms, such as digital signatures, is often quoted as a barrier to usage. It is true that it may take many years for unambiguous precedents to emerge or legislation to be enacted, but this should not be an impediment to electronic commerce. The law is not an instrument of technological change; it follows technology and serves the users as best it can, adapting in various ways as the new challenges emerge.

Computer crime

In recent years there has been a growing concern in many developed countries at the tide of computer-based or computer-enabled crime that threatens to wash over the world. In 1995 I undertook a review of the computer crime legislation in eleven countries in the Asian region and found that of those eleven only two had legislation remotely regarded as satisfactory. Since then, Japan and Korea have to a certain extent advanced their legislative regime. Australia is making progress, but in New Zealand computer crime is rarely reported, much less prosecuted.

In the meantime, fraud is rife. In Australia, some of the country's largest companies have been penetrated by organised crime resulting in the theft of millions of dollars through computer fraud. This could be as much as 10% of profits. In Britain and the USA, over eight out of ten major companies in these jurisdictions report big increases in fraud over the last five years. The cause is not always hacking as such but more a weakness in the general business transactions which are readily exploited. Most companies are reluctant to prosecute because they do not want embarassing publicity. Most cases exposed are database frauds, and misappropriation of stock which is hidden within the computer system. The technology which facilitates fraud also brings advances in detection methods but internal controls will only work if senior managers educate themselves about new technology. There are three parts to providing an effect strategy against fraud: discovery, correction and prevention, the latter being the most important.

Encryption

There has been much heated debate worldwide about restrictions on the use of encryption technology, so that law enforcement and national security agencies can continue to intercept communications. Two questions are worth asking in this debate.

Firs, is interception of private communication a governmental right, which must therefore be protected in the face of technological change, or is it an accidental consequence of the weaknesses of the communication techniques that we have been using? Some commentators argue that it is the latter and that there is no community obligation to protect it.

Secondly, is a country better served by a vibrant, efficient, electronic economy, using trusted secure communication techniques for its day to day business, or by attempting to reduce organised crime by restricting use of technology? So far, much of the opposition to restrictions on the use of encryption technology has centred around a right to privacy and civil libertarian issues. Perhaps, instead, we need to quantify the opportunity cost, in economic terms, of delayed and lower levels of adoption of electronic commerce by the business community because the security mechanisms are not sufficiently trustworthy. It may be that the cost to the economy of restricting the use of encryption technology outweighs the benefits to the community.

Intellectual Property

Intellectual property issues are certainly high on the list of concerns in an electronic environment. The ownership of images and text on the super highway has yet to be clarified. Does copyright still apply when the content has been altered, manipulated or adapted? The allocation of rights between the content creator and the content packager needs to be determined, as do various forms of transmission rights and usage rights. Policy makers are already grappling with issues relating to content. The information super highway has great potential to increase access to information and commercial resources that can be delivered quickly and economically; however, its potential will never be realised if products are not protected whilst being carried on the networks. Likewise, the public will not use the services available and generate the market necessary for its success unless access to a wide variety of works is provided under reasonable terms and conditions.

In the United States, the Department of Commerce has produced a White Paper report on intellectual property rights which attempts to assist the information resources of tomorrow and address how the rights of providers and users can be thoroughly protected. In Australia, there is now some prospect that the process of intellectual property review may all come together in the overall review being conducted by the Copyright Law Review Committee.

Meeting the challenges

The Internet Law and Policy Forum (ILPF)

The ILPF is a global non-governmental organisation sponsored by the major commercial stake holders of the Internet. It will be dedicated to resolving issues of importance to the use of the Internet for electronic commerce transactions, endeavouring to produce uniform solutions acceptable to a global Internet community - solutions which advance self-regulation and accelerated growth.

The Forum is intended to serve as a compelling alternative to inconsistent government regulation, by addressing issues which are difficult, if not impossible to resolve on a national or regional level: security, intellectual property, digital records management and access, jurisdiction, taxation, privacy, electronic payment and transactions, and the resolution of Internet disputes.

The ILPF will endeavour to develop suitable tools for achieving best business practices and resolving the legal aspects of electronic commerce and internetworking, including:

- uniform definition
- recommended business practices
- model agreements
- model national laws including statutes and administrative regulation

- codes of conduct
- codes of information practices
- treaties or conventions.

The IPLF will:

- promote policy dialogue and informed government reforms in partnership with business by establishing a clearing house of information involving laws, regulations and electronic commercial practices; and
- educate government on emerging uses, commercial practices and social ethics and the related work products of the Forum.

It will also facilitate the emergence of an efficient and predictable marketplace in which electronic commerce may advance by minimising legal uncertainties requiring resolution by litigation and maximising the return on investments for new infrastructure content and technology.

Global Information Infrastructure Commission (GIIC)

The mission of the GIIC is 'to force private sector leadership and private-public sector co-operation in the development of information, networks and services to advance global economic growth, education and quality of life'.

The GIIC is an independent, non-Governmental initiative involving diverse communications-related industrial leaders from developing as well as industrialised countries. The Commission has been established to respond to the recognition that traditional institutions and regulatory frameworks can no longer meet the increasingly complex challenges and opportunities of globalised information. Three factors stand out:

- the burden and opportunities of work developing the global information infrastructure are shifting away from governments to the private sector;
- developing as well as industrialised countries have a high stake in information infrastructure development;
- the policy challenges, as well as the market for information infrastructure, are becoming global in scope.

The GIIC was inaugurated in July 1995 at a meeting hosted by the World Bank and has a three year mandate. Unlike many such bodies the GIIC is committed to work with existing institutions and organisations as well as to facilitate new initiatives. Most of its activities will be undertaken in direct co-operation with others, including the ILPF. Its goals include the facilitation of activities and identification of policy options which foster the effective global application of telecommunications, broadcasting and information technologies and services. It has identified 5 major areas of focus: Commerce, Banking & Finance, Publishing, Education and Health Services, and has established working committees in each field.

OECD

In March 1996, the OECD established the Group of Experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure. This group will advance work already started on the standardisation of cryptography and work towards an international agreement on the role of government in public key encryption.

Australian Law Reform Commission (ALRC)

The ALRC was due to submit its report on Legal Remedies and Cross-border Transactions in July 1996. The report will have particular focus on remedy issues raised by the recent growth of international financial markets, the developments in electronic banking and clearing systems and bank secrecy. Part of the ALRC's brief is to examine issues of trade, intellectual property and regional regulatory harmonisation.

Strategic alliances

Hardly a day goes by without an announcement of, or speculation about, strategic mergers between companies in what used to be separate industry sectors. Many industry participants which, only a year ago, appeared to be unassailable are now rushing to catch up with these developments.

A recent example is the announcement by BeriFone, a Californian developer of electronic payment systems, that it will join NetScape, maker of the popular navigator WebBrowser, to develop a way to make electronic payments on the Internet more secure. Their stated objective is to develop a new system to accelerate acceptance of the Internet as a mainstream vehicle for commerce. These are only two of the many companies working with this objective. Credit card giants Master Card International and Visa International have stated that they have agreed on a joint technical standard which will allow for secure purchases over open computer networks. It is clear that this subject is not only timely, but that the issues to be raised should not be addressed in isolation.

International

Australia has been examining the challenges and opportunities posed by the rapid evolution of the Information Superhighway for some time. A number of expert groups have identified and worked through many of the issues, including the Bureau of Transport and Communication Economics (1993/94), the Australian Science and Technology Counsel (1993) and the Broadband Services Expert Group (December 1995). The Government's strategy has been assisted by the National Information Services Council, a national advisory forum comprising representatives from a broad range of areas covering academia, government, industry and the community. The ABA has completed its investigation into on-line services and favoured self-regulation. [*See the article by Kaaren Koomen at p 1-4 of this edition: Ed.*]

In the United States, amendments to the telecommunications legislation passed recently seek to limit what can be transmitted over the Internet, however, how this will operate in practice is far from clear.

More definite is the recent action in Germany to force Compuserve to limit access to offensive material. In December 1995, the German government, under pressure from the conservative Bavarian state government, forced Compuserve to block access to over 200 Internet news groups on the basis that some of the news groups contained sexually explicit material and were, therefore, in violation of German criminal law. Although there are only about a hundred thousand users in Germany, over four million Compuserve users in over 140 countries were adversely affected by this action. It was condemned by civil liberties advocates and privacy activists but defended by the Chinese Communist Party's Central Committee (in China, Internet users must

register with the police). Others in Europe criticised Germany for violating one of the major goals of the European Union, namely unrestricted access to the flow of information throughout the member states of the Union. However, countries which are just beginning to come 'on line' are watching the German and Chinese control policies with interest. Vietnam, for example, has decided to limit Internet access to one gateway with the objective of limiting massive use of the Internet. Similarly, Internet access and usage rates in India, Kuwait and Mexico are so expensive that social and political activist groups find its use prohibited.

In France, concern has been expressed over the ability of the Net to be used to circumvent court-imposed restrictions. In Singapore the Internet will be brought under the Singapore Broadcasting Authority (SBA) in new moves aimed at safeguarding public morals, political stability and religious harmony, although the SBA is coming to the view that self-regulation may be the preferred approach. In Korea, the government leadership in industry and research groups contributed much to the successful launch of the Korean information and telecommunication industries. However, it is commonly accepted today that this government leadership will lose its strength and that its role as an operator and regulator will fade away. It has recently revised its laws on intellectual property rights in order to conform with international obligations under the WTO/TRIPS Agreement and the government has established an Information Protection Centre to protect national information systems.

Japan has also recognised that the creation, distribution and sharing of knowledge will gain importance in an information oriented society. Concerns have been raised in that country about the exacerbation of existing social problems such as distribution of information detrimental to use, fraud and misleading advertisements, invasion of privacy and computer crime. The Minister of Posts and Telecommunications has set up a study group on electronic information and network utilisation to consider the protection of personal information and privacy and ways of ensuring the security and reliability of electronic information.

In the United Arab Emirates and Bahrain, the governments have decided to restrict wide spread use of Internet through their state-owned telecommunications monopolies. In Zimbabwe the government-owned Post and Telecommunications Corporation consistently refuses to make sorely needed upgrades to the national telecommunications network with the result that the public data network is barely able to keep up with access demand.

In Russia, the Federal Agency for Government Communications and Information has embarked on a program to control digital communications access points through the country. By having final authority to lease to private concerns the communications channels in which the Russian government has an interest, it is able to determine who has access to the Russian portion of the Internet and can monitor traffic transmitted over the digital links within the Russian federation.

CONCLUSION

It is now widely recognised that our economy will become more efficient through the effective use of communication technology, particularly inter-organisational business communication. Inevitably, this will change the way that we conduct our business relationships.

Lawmakers, both legislative and judicial, are struggling with revision of intellectual property and privacy law to bring order and commerce to cyberspace. The problem, however, is not only the legal concepts which underlie traditional protection but lack of security mechanisms readily available for use in a public data network. The old assumptions of rules and law may not be the best approach to fostering a successful converging communications industry. Policy makers and legislators may consider taking a fresh look at the market place. Some of the issues that could be impediments to the introduction of secure electronic commerce have to be tackled head on: the lack of standards, the role of certification authorities, the restrictions on use of encryption technologies and the rules of law. Only then will we be able to weave a strong fabric of electronic business relationships to supplement and replace those that support our paper economy today.

Diana Sharpe is a partner of Gillett Sharpe, International Lawyers, Sydney and Singapore.