feature

The Challenge of Regulation:

Charting the Legal Boundaries of the Internet

By Eugene Clark[1] and Brian Andrew[2]

The information economy continues to grow both locally and globally. Not only is its influence spreading, but products/services are becoming increasingly sophisticated giving rise to both new potential benefits and harms.[3] As the impact of the Internet spreads, governments are more likely to become both more interested and involved in responding to the needs of both the network of users and developers.

Views about the role of law in a web environment have evolved just as the business activity has grown and evolved. While some have proclaimed the Internet without borders as anarchical; others have been just as quick to draw the fence around cyberspace. The truth, however, is somewhere between the extremes. While the Internet has not fundamentally altered business law, it has nevertheless challenged many traditional notions of law and led to a new increasing international cooperation and new and creative laws and regulations which are fundamental to the framework and design of successful models of e-business and e-government.

In this new and rapidly changing environment, legal literacy and technology literacy are no longer an 'option' but part of the basic skill-set required of all who venture into and hope to prosper there.

Internet Regulation in the Context of Risk Management

Commercial law, including law of the Internet, should be viewed within the broader context of risk and strategic management.[4] In the context of legal compliance programs, Australian Standard AS 3806 suggests that at the broadest levels, the following must be in place:

* Positive commitment to compliance at Board and CEO level
* Positive promotion of compliance by all managers
* Continual monitoring and improvement of compliance program
* Integration of compliance into day-to-day operations, systems etc.
* Adequate resources: senior people and systems
* Ongoing education and training of all staff[5]

But how aware and prepared are managers in relation to the risks inherent in the technology context? A US study,[6] the E-Frontier, found the following:

* Only 25 percent of US companies and 30 percent of European companies surveyed had risk management committees or other structures to identify and monitor technology risk.
* Nearly all US and European companies had taken similar steps to protect themselves from technology-related risks, eg installing anti-virus software and firewalls, establishing standard security procedures, and auditing the security of their systems.
* Only six in ten companies had implemented employee-training programs to lower their technology risk.
* US and European corporate risk managers' understanding of technology risk is less than adequate, according to the managers themselves. About four in ten risk managers say they have only a "fair" to "poor" understanding of technology risk. Very few (about ten percent overall) say their understanding is "excellent." Only 52 percent of US corporate risk managers have inventoried and quantified the technology risks companies face, compared to 67 percent among European risk managers. Corporate risk managers both in the United States (65 percent) and Europe (57 percent) defer to their information technology departments.
* "The global nature of e-commerce, varying legal systems and the speed with which new innovations are brought to market further complicate the challenges facing companies today, leading many firms into uncharted waters of liability risks as well as those which affect their revenue streams."
* The "Y2K" issue, which required companies to prepare their computer systems for the rollover to 2000, sensitised many companies to technology risks, but 42 percent of US corporations and 38 percent of European corporations said the rollover had little impact on their firms' approach to technology risk."

One lesson from these figures is that law firms themselves have much to do to manage the technology risks relevant to their business as it becomes increasingly reliant on new technology. Secondly, there are great opportunities for lawyers who learn about this new area and apply their skills so that they can add value in finding solutions and managing risks while working with teams of professionals from other disciplines.

continued page 12...

[1] Professor of Law and Dean, Charles Darwin University. Both authors are in the Faculty of Law, Business and Arts, Charles Darwin University. Segments of this article were adapted from Eugene Clark's articles in The Canberra Times IT Section and available from their website. Email: Eugene.Clark@cdu.edu.au.

[2] Professor of Accounting, CDU. Brian Andrew is an economist, accountant and lawyer. Email: Brian.Andrew@cdu.edu.au

The Challenge of Regulation cont...

Law, however, is not just about avoiding risks. It can also be a vital element in achieving business strategic objectives. In some cases, the Internet transforms the dynamic between the law and business model adopted. For example, in the simple case of a B2C online site, the viability of the model may depend upon designing an online contract that can be legally enforceable (see discussion below). Or take the more complex scenario of the creation of a B2B supply chain involving hundreds of players across several countries, the underlying legal architecture or design to ensure that this works is a vital component. In still another case, if a business model can be easily replicated, the existence of an e-business method patent may be the major strategic device by which you keep competitors/copiers at bay while you take advantage of your first-mover advantage.

A Typology of Regulation

Weber[7] debunks the myth that cyberspace can ever be independent. There is no idyllic world, free from government regulation, where people and groups can exist. The online world is part of the offline world. So significant and widespread are its effects that there is no way that governments, industry and other forms of regulation can be avoided. As soon as these effects are felt (eg identity theft, pornography, fraud) in the real world, governments, for one, will and must intervene.

Weber and others also view law as a structural system. This is so in several senses. In one way, one can distinguish between the substance of the law, the change of the law and enforcement of the law. In another sense, the "legal system is embedded in other socially relevant systems with the market and social norms each serving regulatory as well as other functions. In particular, cybernorms depend on traditional social norms.[8] Further, the legal system should be linked to coded communications of other social subsystems."[9] In searching for the best regulatory models, therefore, we need to work towards a legal system that provides for mechanisms allowing for a change in the law. It is also important that the legal system be capable of enforcement.

According to Weber:

> "The Internet as a new forum for the exchange of information and communication has three [sic] features that distinguish it from previous technologies:
>
> * The Internet makes possible an instantaneous global transmission of messages (including graphic and audio-visual materials).
> * The Internet enables individuals and organizations to communicate with a large number of people, offering three different communication channels, namely one-to-one, one-to-many, and many-to-many communications.
> * The Internet allows communicating participants to retain their autonomy to a great extent."

The Internet has become a vehicle for unprecedented access to information through databases, search engines and robots. While cyberspace is indeed different, the extent, degree and nature of that difference is debatable. Even more debatable is what all this means in terms of regulation.

In most countries a combination of various regulatory models is employed in relation to the Internet. These include: no regulation; traditional government regulation, for example by legislation; international agreements; self-regulation and code regulation. These models would be familiar to most readers except for perhaps code regulation, a regulatory theory developed by Lawrence Lessig.[10] Lessig argues that the code can be described as the design of the software and hardware constituting a network and the communication protocols allowing these elements to interact with each other. The design of the code has a significant influence on human behaviour given architecture is one of the major forces and it influences whether certain activity is easy or hard or even possible. Accordingly, a code can do much of the work (in terms of control and regulation) that law used to do. Further, law will increasingly be replaced by code and sovereignty will give way to software.[11] In other words, many if not most of the issues about regulation of the Internet are more likely to be solved by technical rather than legal solutions.

The Internet, a cyber' free range' or 'commons', is increasingly being fenced in by government regulation. The most recent evidence of this trend is seen as Australia prepares to follow the lead of other countries in enacting tough anti-spam legislation. This action builds upon Australia's growing tendency (evident in its attempts to control gambling and online content) to extend Australian laws so that they have application outside of Australia's borders.

Yet it was only 1996 when John Perry Barlow issued his Declaration of the Independence of Cyberspace, stating:

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. ...You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society [with] more

> order than could be obtained by any of your impositions... Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."
> (http://www.eff.org/~barlow/Declaration-Final.html)

This Declaration of Independence could amount to a call for cyber anarchy. Or, as was argued by many, including US academics David Johnson and David Post, it could mean the regulation of the Internet as a special place and by self-regulation. These writers suggested that cyberspace is so unique that it demands its own special laws. Johnson, Post and others thus saw the need for a special cyber law, a *"lex informatica"* drawing inspiration from earlier times when England had evolved a special law for merchants (*lex mercatoria*) ."

Other writers, such as Stanford's Lawrence Lessig in *The Code and Other Laws of Cyberspace* (1999) and *The Future of Ideas* (2001) suggest that the very nature of the software and hardware that make the Internet possible, also work to provide a form of 'regulation' regarding what is possible and how things are structured. This is a new sense of 'code" and new form of 'regulation'.

Since 1996 governments around the world have tended not to respect the declaration of independence of cyberspace as a law-free zone. Nor have they relied upon software and hardware to form a new type of code. Countries such as Australia and the US were among the leading countries to develop special laws that facilitated the growth of e-commerce. An example is the legal recognition of electronic transactions and digital signatures. At the same time, Australia, US and other countries advocated a light-touch philosophy that sought to look to the private sector for leadership and to rely on self or industry-based regulation as opposed to government imposed regulation.

As the Internet has become an integral part of our daily lives, however, we are seeing the beginnings of a shift to greater government regulation. Australia is more and more turning to legislation to fence in, to control, the previously borderless realm of cyberspace.

By enacting legislation extending beyond Australia's borders, by increasing inter-governmental cooperation and a growing convergence of legal norms (such as notions of privacy in relation to transborder data flows) the Internet is rapidly becoming regulated and fenced in.

Perhaps this is inevitable and, on balance, a good thing. At the same time, we should acknowledge that it also has its dangers. For example, in this environment, all governments are compelled to display a type of conscious parallelism as they must choose either to pass similar legislation or face the prospect of not being a player in the economy of the Information Age. In this sense, not only the Internet commons, but also sovereignty of individual governments, is arguably diminished.

Case Study of Internet Taxation

Some of the major challenges to revenue authorities can be listed as:

i Establishing identity
ii Establishing location
iii Documentation and evidence
iv Dematerialisation of trade
v Impact on customs procedures
vi Disintermediation
vii Access to tax havens and off-shore banking
viii Cashless society
ix Tax treaties
x Loss of transactions-based taxes

ESTABLISHING IDENTITY

There is a need to identify the occurrence of a transaction, where it has taken place and who the parties were. This may be difficult in a world of commerce where it is a relatively simple matter to arrange for the untraceable use of an Internet site. The true owner of a website may not be ascertainable easily and any site could be used for Internet commerce by an unidentified third party. The Internet address will tell you who is responsible for maintaining the website but nothing about the computer that corresponds to the address or where the machine is located. The offshore location of websites makes this a major problem for revenue authorities in the future.

ESTABLISHING LOCATION

Once a transaction has been identified and the identity of the parties determined there is still a problem of jurisdiction for tax authorities to overcome. Those engaged in e-commerce will be able to create a website presence in almost any country irrespective of their country of residence or the source of the transaction.

DOCUMENTATION AND EVIDENCE

Revenue authorities have extensive authority to obtain documentation and other information from taxpayers who reside within their area of jurisdiction. Tax treaties provide for the sharing of information between authorities, but where the records are maintained in a tax haven where banking secrecy laws prevail it is impossible for tax authorities to obtain the relevant information. Further, some transactions conducted in cyberspace do not leave an audit trail or documentation which would be suitable evidence for the levy of tax.

DEMATERIALISATION OF TRADE

The expanding trade in services which has been a feature of the expansion of developed economies will flow over into the Internet and this will compound the problems for taxation administrators. If goods are bought and sold through the Internet there will be a physical movement of commodities across national borders which could attract tax and customs attention. Where services, such as insurance, are sold over the Internet, identification of the transaction becomes particularly difficult and tax authorities lose the capacity to make an assessment of liability based on the comparison of inputs and outputs. This rise in the service economy associated with electronic commerce

continued page 14...

The Challenge of Regulation cont...

is the major threat to the tax base of most countries. Serious erosion of the tax base could occur in this area.

IMPACT ON CUSTOMS PROCEDURES

Where goods and services are bought 'on-line' through the Internet and delivered 'off-line' through normal mail order, then normal Customs procedures should be able to identify the transaction and facilitate the levy of transaction taxes such as Customs duty or VAT payable. The transaction could also be 'logged' for other tax purposes. The major problem with this type of transaction is their likely expansion in the future and the need to ensure that Customs resources are increased to cope with the greater volume.

The supply of 'on-line' goods (eg. book reprints) and services (e.g. digitised information) presents serious problems for any tax system which includes transaction taxes, such as a VAT or Sales Tax. In such a case the place of supply may not be identifiable because the supplier has no identifiable physical presence and the result could be no tax or double taxation depending upon the arrangements made.

DISINTERMEDIATION

As noted above an 'information economy' will result in a substantial reduction in the intermediate processing of transactions. This will remove a number of convenient taxing points in the production and distribution cycle and it has the potential to disturb the existing audit trail which is used by revenue authorities to identify and tax certain transactions.

Revenue authorities should be aware of the capacity of Internet banking and electronic purse services to facilitate the development of the 'black economy'. Such services should be tightly monitored by taxation authorities with the awareness that the financial intermediation services traditionally provided by banks can be by- passed through the use of these technologies.

ACCESS TO TAX HAVENS AND ELECTRONIC BANKING

Tax havens and offshore banking facilities have always been available to the rich and to large corporations but the Internet will make such things accessible to a much larger range of taxpayers.

It cannot be emphasised strongly enough that the combination of tax havens, bank secrecy, transfer pricing arrangements and a cashless society present a great threat to the tax base. Revenue authorities need to be pro-active now before the proliferation of tax evasion through this combination of facilities develops to its full potential.

A CASHLESS SOCIETY

The cashless society based on electronic money technologies such as E-cash and smart cards promises many benefits in the form of speed, convenience and security of transactions. But real time E-cash transfers over the Internet may leave no audit trail and no physical record, such as bank statements, cheques, receipts or deposit slips. This will remove or reduce the capacity of tax authorities to monitor many transactions.

TAX TREATIES

Tax treaties will have to address new non-physical concepts of a permanent establishment, the attribution of profits to it and the allocation of tax jurisdiction between the treaty partners. Digitised information could be the source of income and this income could be characterised as royalty income or income from services.

LOSS OF TRANSACTION-BASED TAXES

As observed above, electronic commerce makes it possible for goods and services, previously available only in a tangible form, to be supplied and delivered in electronic form. This change will threaten the capacity of a sales tax, excise or VAT/GST to operate. It is certain that the tax base of all transaction-based taxes will be undermined by Internet trading to some extent.

EXAMPLE: A TRANSACTION

An Australian resident solicitor, with offices in Sydney, New York and Hong Kong, contracts with a barrister (an Australian citizen) to provide a legal opinion on an international banking matter for a client who carries on business in the USA, Hong Kong, the UK and India and who has a banking facility in the Channel Island of Jersey (a tax haven). The barrister normally resides in Bermuda (a tax haven with banking secrecy laws) on a yacht which has been fully equipped with all electronic and telecommunications facilities and which also serves as the primary office of the barrister. The contract was negotiated and confirmed over the Internet using servers located in a number of countries.

The opinion was provided to the Australian solicitor, via the Internet, at her Hong Kong office and the solicitor then provided the relevant advice to her client at the Hong Kong office of the client.

The barrister's fee was transferred from the solicitor's bank account in Hong Kong directly to a bank account in Bermuda and the solicitor's account was settled by transfer on funds from the Jersey bank of the client to an account in Hong Kong.

There are a range of jurisdictional issues here, focusing on questions of the residence of the parties and the source of the revenue generated by the transactions. The location of the computer servers which facilitated the transactions may also be an issue.

The Australian resident solicitor is subject to tax on income from all sources, the Hong Kong revenue authorities only levy tax upon income which has a source in Hong Kong and the barrister seems not to be subject to any clear taxation jurisdiction unless, as a non-resident, it is found that the income had a

source in Australia. Further, there is the major problem for the Australian revenue authorities of identifying and tracing the transactions and in following the money trail involving a range of international jurisdictions.

There are a number of questions raised by these events. These include, where were the various contracts entered into? What were the significant events that generated the revenue? Where were the revenue-generating activities carried out? Which revenue authority has jurisdiction?

Given that no legal authority will enforce the revenue laws of another country, there are significant problems for revenue authorities in any high level professional area where the rendering of advice or the transfer of intellectual property is the primary subject and this case study raises a number of questions which have not yet been answered.

Ongoing Issues

While a detailed discussion is beyond the scope of this short piece, just a few of the legal issues raised by the Internet include the following:

INFRASTRUCTURE

Design issues (including legal architecture) of the next version of the Internet.

JURISDICTION

What law applies? How do we work out the obvious conflict issues?[12] What will have to emerge is an international treaty and perhaps some sort of administrative structure to handle such issues.[13]

CONTENT REGULATION

There continues to be much debate in Australia about regulation of content on the web. This is especially so in connection with M-Commerce as 2.5G and 3 G mobile telephones, personal digital assistants (PDAs) and laptops with wireless connections (wifi) become increasingly capable of image capture, video playback, Internet access, portal access to subscriber services and greater functionality, eg in conjunction with GIS. Research in Europe, for example, estimates that sexual content over mobile devices will generate some $1.5 billion in revenues in 2005.[14] In summary form, the major legislation covering content on the Internet includes:

* Schedule 5, Broadcasting Services Act 1992 (Cth) (BSA) Online Content Scheme. Complaints-based regime using national classification system under Classification (Publications, Films and Computer Games) Act 1995. Seeks to protect end-users, especially children, from inappropriate content.
* Telecommunications (Consumer Protection and Services Standards) Act 1999 (Cth). Regulates access to premium rate voice sex services.
* Telecommunications Act 1997 (Cth), gives broad powers to make service provider determinations to regulate access to premium rate services.
* Regulation 3.12 of Telecommunications Regulations 2001, gives the ACA powers to make service provider determinations regarding the supply of, and access to, premium rate services (other than voice sex services). On 13 May 2004, the Minister of Communications required the ACA to make a service provider determination to require mobile service providers to put into place appropriate restrictions on access to adult content on specified proprietary networks.
* Interactive Gambling Act 2001 (Cth), regulates the delivery of interactive gambling services in Australia. Online casino-style gaming (eg poker and roulette) is illegal, online wagering on racing and sports events and online lotteries are permitted. This legislation is under review, especially as interactive gambling services become available via mobile communication devices.
* Commonwealth Crimes Act 1914, which makes it an offence to intentionally use an Internet carriage service with the result that another person is menaced or harassed, or in such a way as would be regarded by reasonable persons as offensive.
* BSA licence conditions.
* State and Territory laws imposing obligations on content and persons who upload or access content.

PRIVACY

Privacy continues to loom large as an issue in Internet law. In August 2004, the Minister of DCITA initiated a Review of the Legislative Framework on Spyware,15 computer software that secretly collect information from a computer and send it elsewhere or sometimes change settings and interfere with the user's computer. Possible abuses via spyware include: deceptive conduct, Internet banking fraud, unauthorised access, content modification, invasion of privacy, browser hijacking, cyber-stalking, computer hijacking, theft of computer software, resources or bandwidth, anti-competitive conduct, denial of service attacks, impairment of security, damage to computer settings, cyber harassment, identity theft and harvesting and collection of personal financial information.[16]

The review concluded that the use of spyware was extensive[17], existing laws were adequate to deal with possible abuses by use of spyware. This legislation includes: Trade Practices Act, Criminal Code Act 1995 (Cth), Australian Securities and Investments Commission Act 2001 (Cth) and Corporations Act 2001 Cth), Privacy Act 1988 (sets out minimum requirements in relation to collection, use and disclosure of personal information, data quality, access and data security through the National Privacy Principles (NPP), Telecommunications Act 1997 (Cth), which applies to some use of personal information, Telecommunications (Interception) Act 1979 (Cth) (prohibits interception of communications) and legislation passed by some States.[18]

SPAM

The Commonwealth Government has adopted a multi-layered strategy to address spam as recommended in

continued page 16...

The Challenge of Regulation cont...

the Final Report of the National Office for the Information Economy (NOIE) review of the spam problem and how it can be countered. This strategy involves the following elements designed to complement and reinforce each other:

* national legislation (the *Spam Act 2003* and the *Spam (Consequential Amendments) Act 2003*);
* international cooperation;
* information and awareness-raising;
* industry codes of practice; and
* technical solutions.

The Spam Act came into effect on 10 April 2004. It deals with 'commercial electronic messages' which means any form of electronic message including emails and SMS, but does not include fax, voice calls or standard telephone service. The Act prohibits the sending of commercial electronic messages for the purpose, or one of the purposes, of which is to advertise or offer goods, services, land, or business or investment opportunity, unless the recipient has consented to the receiving of the message. Consent may be either express or implied. Consent may be inferred from the circumstances or as a result of the business or other relationship between the sender and recipient.

Certain designated commercial electronic messages are permitted. These are defined as those that consist of no more than factual information. However, such messages must have the name and contact details of the sender and the sender's organisation. The message must contain the logo of the sender. Private law firm newsletter is an example of a designated commercial electronic message. Also included as exempt are messages from government bodies, charitable organisations, educational institutions that relate to goods/services provided by the body sending the message.

The Act has broad reach prohibiting spam sent from within Australia to a destination within or outside Australia. It also prohibits sending of spam from outside Australia to a recipient within Australia.

The Act requires also that all commercial messages must accurately identify the person or organisation who authorised the sending of the message. It must explain how the recipient can contact that person/organisation. The message must have a functional 'unsubscribe' facility. The Act prohibits the supply or use of address-harvesting software or supply or use of electronic address lists produced using such software.

Fines under the Act are severe: up to $A220,000 for companies and $44,000 for individuals. For subsequent breaches fines can go to $1.1 million (companies) and $220,000 (individuals). In addition the Federal Court can award compensation for any loss or damage caused by breach of the act or order the spammer to pay the amount of any financial benefit received.

Results so far suggest that the spam legislation is having some impact. Between April 10 and October 17 2004, the ACA received close to 60,000 complaints. The ACA has issued warnings to approx. 200 people. According to some, the number of major spammers in Australia has decreased significantly.[19]

Of course, for spam to be truly controlled, international cooperation is required. To that end, Australia, in cooperation with agencies in Korea, US, Japan, Mexico, Canada, Chile, Taiwan, Malaysia, Thailand and the Philippines, has signed a Seoul-Melbourne multi-lateral agreement to cooperate in the enforcement of laws against spam.[20]

BUSINESS-TO-BUSINESS B2B

While business to consumer (B2C) issues dominate the headlines, the fact is that B2B dominates Internet activity in terms of dollars. Many issues also arise from the development of B2B ventures such as supply chains. These include, for example:

Contract Issues

First there are the contract formation and performance issues. What is the legal architecture that must be in place to make sure the system works and that all the players understand their rights and responsibilities? What happens if a player in the chain fails to fulfil their role? Does the system live up to expectations? Does it work for all my suppliers, especially those in remote locations and with limited IT capability? Are the reporting capabilities sufficient?

Competition Law Issues

In formulating a B2B arrangement, it is best to examine the competition law implications at the outset. B2B arrangements are neither necessarily pro or anti-competitive. It depends upon the facts and circumstances of each case. Where they allow companies to reduce costs, gain efficiencies and allow smaller players to get a seat at the table, they are pro-competitive. Where they facilitate cooperation amongst competitors and provide incentives for collusive activity and monitoring compliance they can lead to violations of the Trade Practices Act.

1. Thought should be given to the nature of the market and whether the B2B network will have substantial market power. It should also be clear that there is a business efficiency case for the B2B arrangement. If the driver is more about controlling competition or keeping out competitors, then restrictive trade practices warning bells should be going off.
2. Are parties to the B2B arrangement 'competitors'? Do they involve competitor collaboration? If so, the arrangement will have to be careful, especially in relation to pricing matters. If the parties intend to purchase jointly, what will be the guidelines for that operation? Even where the joint buying arrangement enjoys protection from price fixing, it may still be illegal if it is likely to result in a substantial lessening of

competition in the market. In assessing the impact on competition the ACCC is likely to have regard to the size of the collective group and whether benefits are passed on to consumers.

3. Will the arrangement result in a lessening of competition in the market? The TPA prohibits contracts, arrangements and understandings that result in a substantial lessening of competition in a market. If so, are the anti-competitive aspects outweighed by pro-competitive benefits?
4. What about the impact on upstream and downstream markets? Arrangements that involve sharing of information regarding capacity, customer preferences and prices will also make it easier for the major players to enforce price 'discipline' upon all the players. This may have anti-competitive effects. What information 'firewalls' will be put into place to limit the legal and business risks of sharing information amongst competitors. It might not be a bad idea to structure the B2B so that it is controlled by an independent body. If not, it will be important to work out the governing rules for meetings, rules of operation and collection and sharing of data.
5. Does the B2B arrangement involve the exclusion or discrimination against other parties? Where such exclusions result in a substantial lessening of competition in the market, the TPA (s 45E, s 47, s 46) may come into play.
6. Where the B2B group is of significant size, it might be argued that it exercises monopsony power by buyers.
7. It might be found that the B2B arrangement has an anti-competitive effect on the competition for markets.
8. If parties to a B2B arrangement are concerned about the possible anti-competitive effects they should seek an authorisation from the ACCC. If they can show that the pro-competitive benefits outweigh any anti-competitive effects then the ACCC may grant an authorisation.
9. B2B participants who have a substantial degree of market power should be careful. Section 46 of the Trade Practices Act makes it illegal for them to use their market power to damage a competitor or keep them out of the market place.
10. In the area of resale price maintenance, B2B partners must be careful of s. 48 of the TPA.
11. Finally, competition issues are not one-off determinations. A B2B arrangement is not static. As it grows and develops, what was once a pro-competitive operation can become anti-competitive. So, as the B2B network expands, competition issues should be visited on a periodic basis to ensure that the arrangement complies with the TPA.

Other Legal Issues

In addition to competition law, there are other aspects of a B2B arrangement that should be checked out.

What are the tax implications? Surprisingly, many B2B schemes neglect this aspect. R&D credits may be impacted and in some cases there are also transfer pricing issues.

What about the rules of corporate governance?

What about the equity structure and rules governing shareholder arrangements?

Are there any licensing and technology rights/obligations issues?

What about intellectual property? Who owns the customer and other data that is being transferred across the supply chain? If the data involves personal details, then privacy legislation may also come into play.

What about risks of exposure to the laws of other jurisdictions? Supply chains structures can be inherently complex, and when they extend across numerous national boundaries, the activity may subject all those in the arrangement to the jurisdictions involved.

COMPUTERS IN THE WORKPLACE

Internet use policies, privacy, hacking, loss of intellectual property, fraud, use of computer to harass another employee, defamation by email, downloading of pornography and other illicit material, management of files, electronic signatures — these are just a few of the issues that arise from use of the Internet at work.

INTELLECTUAL PROPERTY

Intellectual Property is the 'gold' of the 21st Century and Information Age. Free Trade Agreements, use of copyright circumvention devices, circuit layout protection in computer games, battles between domain names and trade marks, the tension between competition and intellectual property laws, the emergence of a "Creative Commons" to rival the proprietary systems of IP[21], e-business method patents, recognition of Indigenous IP, represent just a few of the exciting issues. Information is increasingly becoming a 'commodity' and new issues will emerge regarding its use and abuse.[22]

M-COMMERCE

With the greater use and increasing power of mobile technology combined with global positioning systems, GIS, radio frequency identifiers and other technology, further legal issues will arise. For example, some are already calling for privacy laws that are technology specific.

LEGAL PROFESSIONALS

In today's environment technological literacy is no longer an 'option', but a vital part of the skills required of a lawyer. This includes the increasing use of mobile technology, modern notions of record management, marketing via the Internet and the delivery of legal services in new and innovative ways.[23]

ELECTRONIC COURTS AND EVIDENCE

Increasingly, electronic discovery, including laptops, is being requested in large cases. Note that even Bill

continued page 18...

The Challenge of Regulation cont...

Gates was caught out in the Microsoft anti-trust case where his emails told the real story about the motivation for dealing with Netscape. These developments have significant implications for knowledge management of all organisations, a part of which is managing the risks of litigation and record keeping requirements.

ENFORCEABILITY OF ONLINE CONTRACTS

While the Electronic Transactions legislation has provided the broad framework, many questions remain, especially in relation to the enforceability of contracts across jurisdictions. There are only about 14 reported cases dealing with click and browse-wrap agreements — none in Australia thus far.

E-GOVERNMENT

Australia was one of the earliest countries to recognise that government should lead the way in demonstrating the efficiencies, effectiveness and enhanced competitiveness that could result from smart adoption of technology. Australia has also played a leading role in the adoption of laws that provide the legal infrastructure to encourage and promote the use of technology. Privacy legislation, Electronic Transactions Act, Digital Copyright amendments, adoption of technology by courts,[24] Public Key Infrastructure (PKI), FedLink, digital records[25], e-procurement, government services online and so on, have all been part of this. The challenge will be to keep pace with developments elsewhere as borders between public and private, national and international become increasingly blurred. Significant developments are also ahead in relation to Government–to-Citizen and Citizen-to-Government relationships.[26]

Conclusion

Just after a decade after the World Wide Web became prominent, it is clear that its impact on government, business, the professions and individual lives has been profound. As we go into the second decade, important discussions are taking place regarding a major re-design of our cyber-infrastructure.[27] This will involve important decisions about tradeoffs between identity, accountability, anonymity and freedom of action. It will also involve choices about recognition or not of national, jurisdictional, institutional boundaries in the design. It is important that the Australian legal profession, government and citizens become informed about, and involved in, these discussions so that we may be successful participants in an Information Age. The lesson for lawyers is that just as the Industrial Age fundamentally shaped our thinking and ways of doing things, so too this new model of 'network' will increasingly shape and challenge what we do, how we do it, and with and for whom.

ENDNOTES

[3] Australian Government, Department of Communications, Information Technology and Arts, Information Economy Index 2004. Between 1998 and 2001 Australia experienced phenomenal growth in household connectivity so that by 2003, the percentage of households with Internet access increased to 58 percent

[4] See Griggs, L, Clark, EE, & Iredale, I (ed) (2003) Managers and the Law: A Guide for Decision Makers, Sydney, LBC Information Services

[5] See also AS 8000-2003 Corporate Governance and the recently drafted Australian Standard on ICT Governance

[6] www.srbi.com/pr13.htm

[7] Weber, Rolf H (2002) Regulatory Models for the Online World, The Hague, Kluwer Law International

[8] Weber at 32

[9] Ibid at 35

[10] Lessig, Lawrence (1999) Code and Other Laws of Cyberspace. New York: Basic Books.

[11] Ibid, at 94-95

[12] See Clark, EE and Puig, GV (published 2003) 'When Global Highways Intersect Local Laws: Defamation via the Internet –Dow Jones & Company v Gutnick [2002]HCA 56' Journal of Law and Information Science Vol 12(2) pp 271-281.

[13] See Hague Convention on Jurisdiction and the Recognition and enforcement of Foreign Judgments in Civil and Commercial Matters (http://www.hcch.net/e/workprog/judgm.html)

[14] Schenker, Jennifer L (2004/05) 'In Europe, Cellphone Profits Go Up as Clothes Come Off' International Herald Tribune, http://www.nytimes .com/2004/05technology/techspecial/04SHEN.html

[15] http://www.dcita.gov.au/ie/spyware/outcome_of_review

[16] See generally Clark, EE and Sainsbury, M (2002), Privacy and the Internet, Sydney, Thomson LawBook Co.

[17] While there are no stats specific to Australia one US study found that 90 percent of Internet connected computers have some forms of spyware: DCITA, 'Outcome of the Review of the Legislative Framework on Spyware, 1/05/05: www.dcita.gov.au /ie/spyware/outcome_of_review

[18] Criminal Law Consolidation Act 1935 (SA) which is the first state to legislate against identity theft. The act makes it an offence to possess personal identification information that enables a person to assume a false identity or to exercise a right of ownership that belongs to someone else, to funds, credit, information or other financial or non-financial benefit.

[19] Cramer, Gordon, The Australian Spam Act in Profile (parts I and 2), http://www.marketingprofs.com/: 1/05/05.

[20] See 'Asia-Pacific Cooperation on Spam, Media Release 042/054, http://www.minister.dcita.gov.au/media/media_releases/asia-pacific_cooperation_on_spam...

[21] See Lessig, L (2004) Free Culture: available through Creative Commons http://free-culture.org/freecontent/. See also, Lessig, L (2002) The Future of Ideas http://en.wikipedia.org/wiki/The_Future _of_Ideas

[22] See generally Putnis, P and Clark, E (2005) Copyright, media and innovation: Then and now', MIA: Media International Australia, No 114, February, pp 5-15.

[23] See generally Susskind, R (2000)

continued page 19...

feature

Pro Bono: on the national agenda

By John Corker, Director of the National Pro Bono Resource Centre

On 5 and 6 May 2005 about 40 practitioners from Alice Springs, Katherine, Darwin, Sydney and remote parts of the NT met over two days in Darwin to discuss unmet legal needs in the Territory and how the legal community could work better together to address those needs.

The National Pro Bono Resource Centre encourages practitioners based in the NT to support the initiative of the NT Legal Aid Commission and Law Society to facilitate more discussion about this issue, to strive for a more coordinated approach to the delivery of pro bono services and think about ways in which they may be able to help.

Nationally there are now over 25 law firms with pro bono coordinators and structured pro bono programs which involve everything from in-firm to outreach services and from secondment of lawyers into remote area communities to training programs for lawyers in those areas of legal practice where the unmet legal need is high.

There are Public Interest Law Clearing Houses in NSW, Queensland and Victoria and a pro bono clearing house started in the ACT in November 2004 run by the ACT Law Society. Other law societies and bar associations are involved in a range of individual and court based pro bono activities. There are Homeless Persons Legal Clinics staffed by pro bono lawyers in Melbourne, Brisbane and Sydney and new partnerships are developing between law firms who are willing and able to offer their services and remote communities very much in need of pro bono assistance.

Community organisations, and particularly Community Legal Centres (CLCs) are being encouraged to form partnerships and long term "multi-tiered" relationships with law firms. They are multi-tiered as they cover not only legal advice and representation but might also provide assistance with law reform and policy work, advice in relation to internal management issues, mentoring or co-counsel arrangements between law firm staff and solicitors at CLCs. They might also include non-legal assistance in the form of administrative services, accounting and bookkeeping services, access to law firm facilities and assistance with fund-raising events and conferences.

NT Legal Service Providers Forum

Innovative pro bono initiatives appear to be increasing but this trend is distinctly eastern seaboard. Encouraging the uptake of pro bono activity in less well-resourced areas is a major challenge for certain jurisdictions, including the Northern Territory.

On 5 and 6 May 2005 about 40 practitioners from Alice Springs, Katherine, Darwin, Sydney, Nhulunbuy and remote parts of the NT met over two days in Darwin to discuss unmet legal needs in the NT and how the legal community could work better together to address those needs. The conference was organised by Jenny Hardy from the NT Legal Aid Commission (NTLAC) and Barbara Bradshaw, CEO of the Law Society NT, and funded by the Law Society Northern Territory Public Purpose Trust. Lawyers from NTLAC regional offices, CLCs, Indigenous legal organisations, women's legal services and family violence prevention units explained the limitations and difficulties in providing adequate legal services to disadvantaged and marginalised people in the NT, particularly in remote areas.

A few local firms attended, as did Sydney-based pro bono coordinators from Clayton Utz, Blake Dawson Waldron (BDW) and Gilbert + Tobin. BDW have had two civil lawyers seconded to Katherine Regional Aboriginal Legal Aid Service, each for six months at a time. It was great to hear what a difference a person, who is fully supported by their firm and the local service, can make to the delivery of legal services. It was also great to hear of the contribution that is made by some local firms; but sadly few local firms were present at the conference.

A clearing house?

The NT Attorney-General, the Hon. Dr Peter Toyne, opened the forum by putting out the challenge to those present to see if a pro bono focal point could be established in the NT. The feeling of the meeting was that there was not enough capacity amongst NT-based firms to warrant a clearing house model. It was said that few NT-based firms are large enough to undertake a comprehensive pro bono program but noted that each firm was able to assist in its own way, perhaps by simply agreeing to file documents for a remote service, assisting with drafting law reform submissions, extending an

continued page 20...

The Challenge of Regulation cont...

Transforming The Law, (Oxford: Oxford University Press).

[24] See Hoyle, A and Clark, EE (2004, released in March 05) 'The Court of the Future and its Lessons' Australian Law Librarian Vol 12 (no 4), Summer, pp 45-58.

[25] Clark, EE (2004) 'Records Management in an Information Age: Law and Management Perspectives' Published Proceedings of the 21st International RMAA Convention, Canberra 12-15 September, pp 64-85.

[26] See Clark, EE (2003), 'Managing the Transformation to E-Government: An Australian Perspective Thunderbird International Business Review, Vol 45(4), July-August, p. 377-397, John Wiley & Sons, ISSN: 1096-4762; Online ISSN 1520-6874

[27] See eg, http/www.sdsc.edu/sbe