Communications LAW

B•U•L•L•E•T•I•N

THE OFFICIAL PUBLICATION OF THE COMMUNICATIONS AND MEDIA LAW ASSOCIATION INCORPORATED

Print Post Approved PP: 234093/00011 EDITED BY NIRANJAN ARASARATNAM Vol 19 No 2 2000

No Guts, No Vision: The Politics of Media Diversity in Australia

Peter Coroneos analyses some of the implications of the Government's approach to datacasting, digital TV and streaming on the Internet.

The digital television amendments to the *Broadcasting Services Act* passed by the Senate in late June spelt the kiss of death for the development of a multi-billion dollar datacasting[1] industry in Australia, and will do nothing to arrest the widening of the information divide both regionally and more generally. It also opened the door to extending the monopoly of the traditional broadcasters into the Internet space, through a review that could have seen streamed[2] audio and video content over the internet deemed broadcasting. Since no new broadcasting licenses will be issued until 2007 – some 40 internet years from now – the implications of such an outcome for industry are quite clear and quite chilling.

The good news is that our industrial strength lobbying in the two weeks after the legislation passed stemmed the haemorrage of business confidence by stimulating a rapidly convened Ministerial review, which was over in a matter of days, rather than the 18 months it could have taken. And thankfully the "review" found that streamed content available on the Net should *not* be considered broadcasting. But of course, we will continue to keep up the pressure until the necessary amendments turn the Minister's finding into law and so provide the industry with the certainty we so desperately need. Nothing less will do.

HOW DID WE GET HERE?

But let's go back and ask a couple of key questions about how and why we ever got into this ridiculous situation to begin with. Starting from first principles, Australians are entitled to ask: by what mandate the Government can use spectrum which belongs to all of us to favour the commercial interests of the free to air broadcasters ("**FTAs**") at the expense of everyone else?

Fairly spurious arguments were put by the Government that the FTAs needed some compensation for the investment they have to make to go digital. Interestingly, the same concessions were not made to other potential users of the digital spectrum who also have to invest millions in developing a broadcast capacity.

The Government further argued that FTAs have an obligation to broadcast Australian content, so somehow we are protecting content creators by protecting the FTA cartel. On close examination, this argument also fails. Firstly, the obligation exists only in relation to content for which there is market failure *eg.* drama and children's programming, not all content. Secondly, any content creator who wants to produce for television these days has to find overseas distribution backing before they even embark on production, because the ever diminishing licence fees that our local FTAs are paying will not alone cover the investment. Thirdly, datacasters would probably have been quite happy to agree to minimum content rules provided they could compete with the networks on an equal footing. So too would any fourth commercial TV broadcaster. The fact is, opening up the airwaves to competition is the best opportunity for stimulating the production of Australian content that we could ever have.

Of course, the more modes of content delivery there are, the less control governments have on what the public sees. This has not been lost on Asian observers who see Howard's agenda in more sinister terms, if not from our perspective, certainly from theirs. As Lim Say Boon of the South China Post wrote just days after the legislation passed:

> *...[t]his is Mr. More-Liberal-Than-Thou who not that long ago deigned to let his crisis-hit Asian neighbours in on the virtues of an open, competitive modern economy. This time around, there is little Mr. Howard can teach his neighbours about transiting [sic] to a New Economy that they couldn't learn from Beijing - circa 1989.*

INSIDE THIS ISSUE

CONTENTS

Worse, Mr. More-Liberal-Than-Thou is sending a frightening message to his Asian neighbours - with copies to every politically thin-skinned government in the region - about how even a liberal democracy like Australia can justify Internet censorship for commercial purposes, let alone for social and political reasons.

Internet Industry Association members have been outraged and in total disbelief of the cynicism underlying the policy. At the whim of Government, *"convergence"* has taken on a whole new meaning. It seems to describe the Government's vision of the future and the opportunity for competition in the new media. Both are now narrowing to the size of a small dot on a screen once the power is switched off.

Datacasting was the single biggest hope for reinventing Australia as a new economy - we could have leap-frogged the US in both penetration and advanced deployment of broadband services. We could have had almost the entire Australian population online within three years. That possibility is now about to evaporate.

The legislation has undoubtedly sent a negative signal to the international investment community. Pity the Australian dollar and the effect on interest rates. This Government had a choice - and it chose the old economy over the new. The only winners here will be the old economy television broadcasters – at least until we have the bandwidth to deliver similar and better content over the Net. But of course investment in bandwidth depends on a regulatory environment that supports confidence.

LOSERS: THE AUSTRALIAN COMMUNITY

Australians in regional areas have struggled with slow and expensive access. There is a widening gap between the information rich in the city and the information poor in the regions. People in the bush have every right to be very, very angry over the death of datacasting which could have provided alternatives to the closure of bank branches and the loss of other services in the bush. While technically they can still receive these, the business case for fast rollout of the enhanced technologies is now dead in the water. Now they will just have to wait until traditional broadband gets to them. Our members who are investing in satellite will help bridge the gap, but of course they will only keep investing as long as they know there will be no further restrictions on what they can transmit. And as long as FTAs contintue to dictate broadcasting and media policy in Australia, that uncertainty will remain.

Datacasting provided the chance to provide every Australian family with a television set with Internet access, through a backchannel built into a multifunctional box. Now they will just get TV - with a few more bells and whistles maybe - but still only TV. Data is the killer application of digital TV - this legislation has killed the "killer app".

A more open policy would have provided Australia with sufficient critical mass of online users to kick-start an e-commerce explosion which might otherwise take years to occur. Indeed, there was a strong commercial case for giving set-top boxes away just to get more of the market online. This legislation torpedoes the business case for such a play and condemns the majority of Australians to a slow and arduous climb up the data slope to the 21st century economy.

LOSERS: THE INTERNET INDUSTRY

On the industry side, the losers will be the startups and content developers who dreamed of unparalleled opportunities for pioneering developments, and those who saw the possibility of broadening the diversity of media control and delivery in Australia. We were about to become a test bed for the development of datacasting technologies for export into countries like India and China which, like Australia, have poor communications infrastructure in their remote areas. That opportunity will now probably be lost.

The patently artificial constraints on the type of content that can be datacast would emasculate the commercial case for investment in the new medium. Potential competitors to free-to-air broadcasters now have no incentive to invest in either broadband content development or delivery via spectrum. We have already seen all the main prospective datacasters abandon their planned trials. Theirs is a rational response to an irrational policy.

It gets worse. Not only can't you deliver most genres of video content over spectrum, but the Government has signalled the possibility of a ban on audio and video streaming over the traditional Internet. You don't have a review by the ABA on whether this might breach the spirit of the new law unless you want to leave open the opportunity of banning it. How the Government would ever implement this is hard to fathom, but the damage that could be done by even trying should be enough to worry every ISP in Australia and anyone else with aspirations to deliver broadband content over non-spectral media.

The breadth and intended effect of these policies are indefensible, even on the basis of preserving the Government's decision to not issue any further television licences. The measures are a hugely disproportionate imposition on the emerging media compared to the risk to the incumbents' businesses.

The Federal Opposition is not blameless in this debate, having supported the general thrust of the Government's legislation in 1998 which gave the FTAs free use of spectrum for eight years, while everyone else had to pay. And it was Labor's review amendment in the legislation which triggered fears that the datacasting restrictions would extend to Net based streaming, which does not use broadcast spectrum[3]. Labor has been silent lately hoping the Government will take all the heat on this issue. But we have not forgotten and at the appropriate time (read: in the lead up to the next election) we will be looking for iron clad commitments from the alternative government on exactly how committed they really are to the Internet revolution. Remember they also supported last year's content regulation legislation.

THE INFORMATION POOR STEALING FROM THE INFORMATION RICH

In truth, the best thing to really do with this highly corrupted piece of legislation, the *Broadcasting Services Act* is to throw it out entirely and start afresh. It has become so complex and full of compromises that its workability will be a real issue. Industry players in other leading information economies are not encumbered by the artificial barriers to entry we see here. Whichever way you look it, the legislation really just represents more impediments to competition, content development, investment and innovation.

In the online world we talk about old economy companies being "Amazoned" by new startups who can innovate, free of the legacy of offline investments. This principle operates on a national level too. This legislation tries to artificially limit technological convergence by regulatory means. This is not in the long term national interest, and will ultimately prove futile as everything moves to the Internet.

It need not be this way - but it will take some enlightened and courageous intervention to avoid the wreckage that otherwise lies ahead as technological convergence continues inexorably. From our side, the pressure will stay on until every last politician has committed to supporting the information revolution, or at the very least, doing no harm to it. So we are looking for vision and guts - not an unreasonable expectation for leadership one would have thought. Whether we get it depends on whether our decision makers can extricate themselves from the grip of the television moguls, and how soon our industry can assume the same degree of ballot box pull. Stay tuned.

1 'Datacasting' is broadly defined as the delivery of interactive digital content including internet content to television sets using broadcasting services band (BSB) spectrum.

2 'Streaming' refers to the delivery of packets of internet content in a way that the user experiences an uninterrupted flow of information. It is most commonly used for delivery audio and video content whether in real time or on demand.

3 Proposed section 216E requires the minister to "cause to be conducted a review of whether, in the context of converging media technologies, streamed audio and video content obtainable on the Internet should be regarded as a broadcasting service".

Peter Coroneos is the Executive Director of the Internet Industry Association.

The Communications and Media Law Association Incorporated (CAMLA)

ABN 46 002 651 005

Essay Prize

The Communcations and Media Law Association is holding an essay competition in 2000.

The purpose of the competition is -

- to encourage high quality work in communications and media law courses; and
- to improve links between those studying and practising in the area.

The prize will be given for -

- a previously unpublished essay which is the original work of the author;
- an essay completed by a student enrolled in an undergraduate or postgraduate course, possibly as part of that course;
- an essay on a subject relating to communications or media law;
- an essay of 1000 - 3000 words. The 3000 word limit (inclusive of all footnotes, annexures, attachments and bibliographies etc.) is not to be exceeded.

A prize of $1000 and a one year membership of CAMLA will be awarded to the winner.

The winning essay, edited in consultation with the author, will be published in the Communications Law Bulletin.

The winning entry, to be selected by a panel of experienced communications and media law practitioners, is likely to demonstrate original research, analysis or ideas. The panel will not necessarily be seeking detailed works of scholarship.

The award will be made at the annual CAMLA Christmas Function.

Only one essay per student may be submitted. Entries will be accepted by e-mail or by post. Entries WILL NOT be accepted by fax. Entries submitted by post should include 3 (three) copies of the entry typed well-spaced on A4 paper. The name, address, email, telephone and fax contacts and the tertiary institution and course in which the author is enrolled should be included on a separate, detachable sheet.

Entries submitted by e-mail should include the same details, in a separate e-mail from the entry.

The author's name should not appear on the pages of the essay.

Entries should be submitted to:

The Administrative Secretary, Communications and Media Law Association
PO Box 545 GLEBE NSW 2037 Australia

e-mail: rosie@bigpond.net.au

by 5 pm Monday 30 October 2000 *Late entries will not be accepted*

On line Payment Systems

Catherine Parr and Lewis Grimm explore some of the key issues relating to on line payment systems.

We are continuing to see the development of new on line payment systems or methods of facilitating payments on line. The developers of these systems in Australia will need carefully to consider the regulatory environment.

Payment systems and purchased payment or stored value facilities are regulated by the *Payment Systems (Regulation) Act 1998 (Cth)* ("**PSRA**"). That Act requires the operator of a purchased payment facility to be authorised or exempted by the Reserve Bank. However, where the provider is an authorised deposit taking institution ("**ADI**") it will be regulated by the Australian Prudential Regulation Authority ("**APRA**") and subject to capital and liquidity requirements.

There has been, therefore, the scope for some regulatory arbitrage between the prudential and regulatory regime imposed by APRA on ADIs and the prudential requirements imposed by the Reserve Bank.

In an attempt to eliminate this potential for arbitrage a new regulation was introduced on 15 June 2000. This article examines the legislation and the impact of this new regulation. It also highlights some other legal issues the providers of on line payment facilities will need to consider.

PAYMENT SYSTEMS REGULATION ACT

The PSRA was enacted to protect consumers and promote public confidence in *payment systems* and *purchased payment facilities* as these terms are defined under the PSRA (see below).

The PSRA proceeds on the basis that a system or facility cannot be both – it will be one or the other and will be regulated differently depending on which category it falls into.

Purchased Payment Facility

A *purchased payment facility* is defined as a facility (other than cash) in relation to which the following conditions are satisfied:

> *(a) the facility is purchased by a person from another person; and*
>
> *(b) the facility is able to be used as a means of making payments up to the amount that, from time to time, is available for use under the conditions applying to the facility; and*
>
> *(c) those payments are to be made by the provider of the facility or by a person acting under an arrangement with the provider (rather than by the user of the facility).*

In order for a facility to fall into this category, it is essential that the facility be *"purchased"*. The requirement for a purchase fits neatly with stored value cards and digital cash. Such categorisation may be more difficult where the facility offered is more in the nature of a conduit for transactions and a user is merely required to register for the service to be eligible. The term *"purchase"* also connotes some payment or consideration from the purchaser for the service supplied.

The explanatory memorandum which relates to the PSRA says that purchased payment facilities embody the unique characteristic that consumers pay for the facility using conventional means (the example given is cash, but credit cards would be equally applicable) and rely on the holder of the stored value backing that facility to subsequently redeem the value.

A provider of a purchased payment facility will need to be:

- an ADI;
- authorised under the PSRA;
- granted an exemption under the PSRA; or
- providing a facility declared for the purpose of the PSRA to be a facility to which the PSRA does not apply.

Payment System

A *payment system* is defined in the PSRA as

> *"a funds transfer system that facilitates the circulation of money, and includes any instruments and procedures that relate to the system".*

If the correct characterisation is as a payment system then the relevant part of the PSRA will be Part 3. That part permits the Reserve Bank to designate a payment system to undertake direct regulation of it.

Once a payment system is designated, the PSRA provides that it can be subject to the imposition of rules of access, the determination of standards, the arbitration of disputes and the giving of enforceable directions. A system which has not been designated is not required to be licensed or authorised in any way.

The explanatory memorandum for the PSRA says that *"it is expected that a sizeable proportion of payment systems will not be designated"* and that designation generally will occur *"only after substantial consultation with participants and after consideration of alternative regulatory approaches and voluntary arrangements have been exhausted"*.

THE NEW REGULATION

On 7 June 2000, the Commonwealth Government passed the *Banking Amendment Regulation 2000 (No. 1)* ("***Regulation***"), which regulates certain types of purchased payment facilities.

The Regulation says that the holder of stored value in relation to a purchased payment facility will be deemed to be carrying on a banking business (and

therefore brought under APRA's supervision) where:

- the facility is available for purchase and use on a wide basis; and
- all or part of the facility's unused value is repayable on demand in Australian currency.

This regulation acknowledges that holding stored value is similar to a deposit at a bank.

Store of value is a broad concept, and extends beyond smart cards.

APRA has yet to determine the meaning of *"available, on a wide basis"*.

APRA has indicated[1] that rather than determining "wideness" by reference to a set number of users or purchasers of the facility, it is likely it will be determined by reference to the circumstances and a combination of a number of different factors. For example a facility would be widely available if accepted at a number of geographically dispersed outlets (for example, supermarkets, newsagents or post offices). Another measure could be the size of the relevant float. A float of $100,000 probably would not qualify, whereas $100,000,000 probably would. In addition, APRA is likely to look at the size of individual transactions or float amounts.

It is likely that some transitional arrangements will be introduced for new businesses. Until a new facility is established and being used on a wide basis the Reserve Bank, if it grants an exemption from the PSRA, is likely to impose conditions on that exemption which will require reporting and contemplate a switch to ADI status at some point.

Once it has been determined that a purchased payment facility is a banking business, the holder of the stored value would be subject to the same authorisation criteria as for an ADI, although the capital adequacy requirements may not be the same, with $1,000,000 capital possibly being "a reasonable starting point" for a new business.[2] The holder of stored value would also be subject to risk management controls based on the recommendations of the Basle Committee on Banking Supervision's *"Risk Management for Electronic Banking and Electronic Money Activities"* (March 1998).

Because the PSRA is new legislation which does not appear to have been the subject of any judicial interpretation, and because it is obviously critical to remain on the right side of the regulators, the provider of a payment facility will need to reach an agreed position with the Reserve Bank on which part of the PSRA its system falls under and then, if the facility is a purchased payment facility, discuss with APRA whether the holder of the stored value is to be deemed to be carrying on a banking business.

OTHER ISSUES

There are a number of other issues to be considered in relation to a payment system which is to be offered to consumers including the following:

Financial Transaction Reports Act

Some of the speed and convenience of a facility intended to be provided entirely on line will be removed if the customer has to physically identify themselves and do a 100 point check. The structure needs careful consideration to see if this requirement can be avoided.

Financial Institutions Duty

With a Customer to Customer (C2C) or Customer to Business (C2B) system intended to be used for low value transactions an obligation to pay (and therefore a need to recover) financial institutions duty ("**FID**") will be a significant impediment. Although FID will disappear on 1 July 2001, careful consideration needs to be given in the meantime to the FID legislation and the situs of any relevant on line accounts.

EFT Code of Conduct

This is being expanded to cover all forms of consumer electronic funds transfer. It will almost certainly catch, in one way or another, any C2C or C2B online payment facility.

Perhaps the most problematic area of the new Code is the proposed regime for apportioning liability for unauthorised transactions.

CLERP 6

Changes to the Corporations Law will regulate the provision of facilities through which a person makes non-cash payments. The consequences of regulation will include the need to hold an Australian Financial Services Licence, obligations to give financial services guides and product disclosure statements and a number of other obligations. Some of the requirements are onerous and arguably totally unsuitable for a financial product which facilitates non-cash payments.

There is a lot to think about and the regulatory environment is continuing to evolve and change.

[1] Greg Brunner "Update: Regulation of Smart Cards in Australia"

[2] Greg Brunner "Update: Regulation of Smart Cards in Australia"

Catherine Parr is a partner and Lewis Grimm is a lawyer at the Sydney office of Allen Allen & Hemsley.

Internet Best Practice Model

Lewis Grimm summarises the recently released Best Practice Model for conduct on the Internet.

On 18 May 2000, the Minister for Financial Services & Regulation, Joe Hockey, released a code of conduct entitled *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business* ("**Best Practice Model**"). The aim of the code is to increase consumer confidence in business to consumer ("**B2C**") electronic commerce. However, many of the recommendations contained in it are equally applicable to business to business ("**B2B**") transactions.

Although it is proposed that the relevant industry associations and individual businesses adopt the Best Practice Model, there is no requirement that they do so. The code does not propose any remedies for its breach other than existing legal remedies for unfair business practices. Also, to the extent that the code is inconsistent with any existing laws, those laws prevail.

The code recommends that businesses:

- comply with laws relating to fair business practices and people with disabilities;
- deliver electronic goods and services without specialised software or hardware unless the customer has been clearly informed of the requirement for it in advance;
- obtain consent from the consumer's parent if the business believes that the consumer is under 16 years;
- only send commercial e-mails to existing customers and those who request them;
- clearly identify themselves and their contact details in online communications; and
- use secure payment methods and clearly inform customers about them.

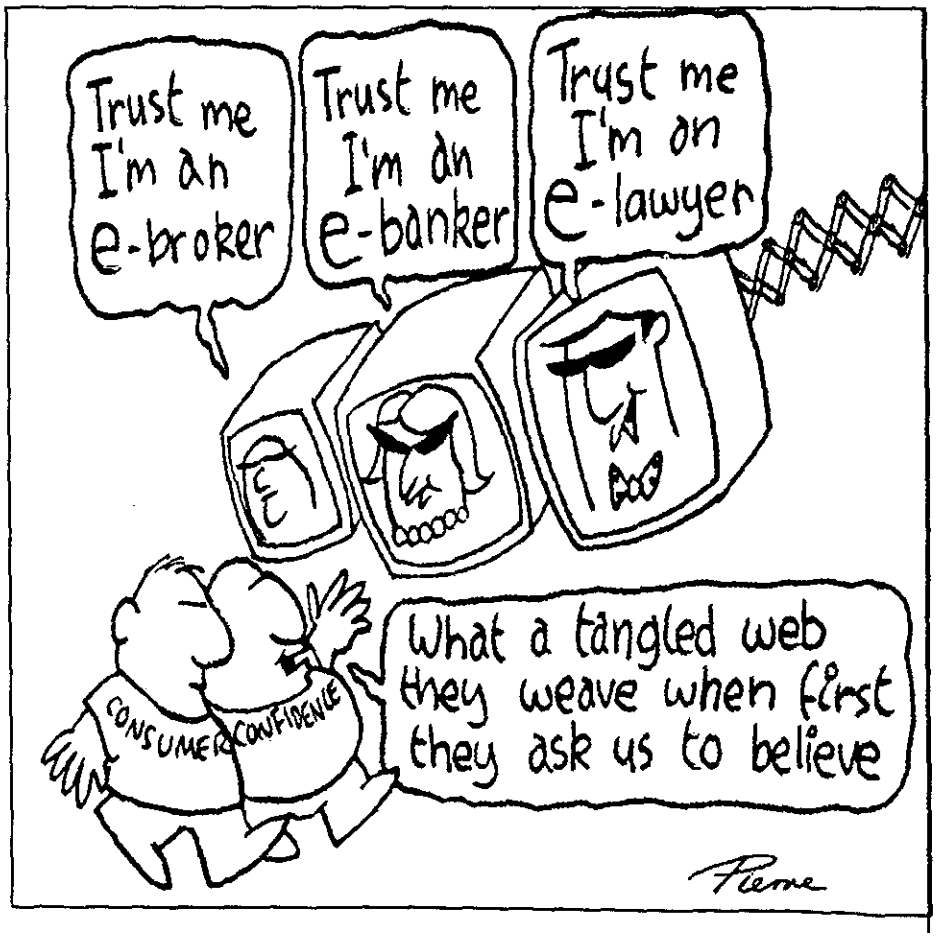
The code also makes a series of recommendations relating to the formation of the contract with the consumer as well as the resolution of disputes relating to the contract. It suggests that the business clearly provides customers with all relevant terms and conditions. However, it further proposes that the consumer should also be able to inform the business as to the purpose for which they require the product, and to modify the terms of the contract. Once the order has been received, the business should promptly acknowledge its receipt.

The contract should clearly display details of any external dispute resolution mechanism to which the business subscribes, but, in addition, the business should develop proper internal procedures to handle consumer complaints. The business should clearly display the jurisdiction where disputes must be determined at the earliest possible stages of the consumer's interaction with the business.

The code recommends that businesses must respect consumers' privacy when handling personal information, including adherence to the Privacy Commissioner's *National Principles for the Fair Handling of Personal Information*. This would also include the *Privacy Amendment (Private Sector) Bill 2000 (Cth)*, the specific terms of which are currently being negotiated in Parliament.

Provided this code is generally adopted, it has the potential to fulfil the stated aim of building Australia's reputation as a place to do business. However, it remains to be seen whether self-regulation will be effective in an area as fiercely anti-regulatory as the Internet, particularly given that businesses adopting the model outside the membership of an industry are required to notify the Department of Treasury.

Lewis Grimm is a lawyer at the Sydney office of Allen Allen & Hemsley.



Bright Lines in the Spectrum: Datacasting as a Case Study in Regulating Convergent Technology

Joanna Davidson examines the new legislative framework for datacasting.

Following the intense lobbying and negotiating effort which culminated in the last-minute passage of the *Broadcasting Services Amendment (Digital Television and Datacasting) Act 2000* (Cth) ("**Digital Act**") in the Senate on 29 June 2000, the Minister for Communications, Information Technology and the Arts commented in a media release

> *"Digital TV and datacasting must appeal to consumers if it is to succeed – ordinary Australians must be given a compelling reason to buy a new television set or a new set top box".*[1]

The final form of the Digital Act encapsulates the enduring challenges to government when regulating emergent, convergent, technologies. This article will examine the ramifications of the datacasting regime, addressing the question of whether Senator Alston's "compelling reason" to take up the new services has been legislated out of existence.

DATACASTING AND CONVERGENCE

Datacasting technology is an example of tertiary convergence: the further merging of the IT, media and telecommunications sectors and their broad extension into households, with the addition of external services such as retail and finance businesses, all happening on televisions, a virtually ubiquitous piece of consumer technology.[2] It therefore has *all* the attributes of a "services sector restructuring enabled by digitalisation", the definition of convergence adopted by the Department of Communications, Information Technology and the Arts.[3] It is potentially the definitive "sticky" environment.

This technology has significant advantages for the development and delivery of broadband content, utilising the potential of the broadcasting service bands to be the "big pipe" needed to redress the spectrum drought identified by the National Bandwidth Inquiry. Datacasting has the potential to eliminate the need for a physical connection to every home to deliver broadband services, posing a challenge to high-speed Internet carriage by cable or DSL; as well as increasing Internet penetration across the "digital divide".[4]

This is the blue sky picture, the sort of philosophy espoused in the UK, whose Minister for E-Commerce, Patricia Hewitt, has stated that:

> *"For us, the issue is how do we enable people to access the greatest richness of internet content at any time, using any device".*[5]

However, datacasting is itself a term largely unique to Australia, with similar services overseas still mostly confined to the status of "vapourware".

As this article will illustrate, the Digital Act has probably defined datacasting into dullness, destining it to fulfil the prophecy of being:

> ***"The first broadcasting technology that is in search of a business case, rather than responding to one".***[6]

DEFINITIONAL PROBLEMS

Datacasting was initially defined in the *Television Broadcasting Services (Digital Conversion) Act 1998* (Cth) ("**Digital Conversion Act**").[7] Essentially, the definition restricts a datacasting service to digital information transmitted in the broadcasting service bands that is *not* a broadcasting service. This distinction is a crucial one which informs the regulation of datacasting in the Digital Act, and is lumbered by what the Productivity Commission described as a:

> *"legacy of quid pro quos [which] has created a policy framework that is inward looking, anti-competitive and restrictive. As boundaries between media dissolve and the old concept of broadcasting becomes obsolete this regulatory framework is eroding or becoming circumvented."*[8]

DATACASTING LICENCES

Recognising the structural separation between service activities and underlying service delivery in convergent industries, the Digital Act sets out a regime for datacasting licences which is quite different from the current arrangements governing broadcasting licences.

Two different licences need to operate together in order for a datacasting service to function. The first is a datacasting transmission licence, which is the licence to operate the actual transmitter used to transmit the datacasting service, and is subject to the *Radiocommunications Act 1992* regulatory obligations in relation to the transmission. The second is a datacasting licence under the BSA, which authorises the actual transmission of content.

These licences may be held together, or by separate entities, in which case the transmission licence holder will need to apply to the ABA for a "nominated datacaster declaration" authorising the provision of the combined service by separate licence holders.[9]

CONVERSION TO A BROADCASTING LICENCE

The establishment of a bright-line distinction between a datacaster and a broadcaster for the purposes of protecting the franchise of free to air television broadcasters fosters uncertainty amongst potential datacasting licence holders.

This is manifested in the Digital Act's silence over the question of conversion of a datacasting licence to a broadcasting services licence when the moratorium on new commercial television licences ends on 31 December 2006 – a conversion which would be fraught with difficulties under the Digital Conversion Act.

The ABA has commented that without a datacasting channel being cleared and re-auctioned as a commercial television broadcasting service, the allocation of a commercial television broadcasting licence to a datacaster under parts three

and four of the *Broadcasting Services Act* ("**BSA**") would probably be impossible.[10]

MULTIPLE REVIEWS

Further uncertainty is engendered by the multiple reviews of the regime, including one of the entirety of the new BSA Schedule 6 by the end of 2002[11] a result of the end of definitional certainty which means that legislative restrictions on datacasting services may be circumvented by new technology within a few years.

The accrued rights of datacasters are also limited, the term of the licences being ten years with the expectation of a single renewal for five years only,[12] in contrast to the free to airs' expectations of renewal and standard 25 year licences for the telecommunications spectrum.

THE GENRE CONDITIONS: ENFORCING DIFFERENCE

Leaving aside the future use of datacasting spectrum, genre restrictions in the Digital Act designed to enforce the distinction between datacasting and broadcasting on the basis of the "look and feel" method severely constrain the genre and format of datacasting content.

Datacasters must not transmit the whole or an extract of a category A television program (including drama, sports, music, lifestyle, documentary, children's entertainment, quiz and comedy programs) unless the extract is ten minutes or less and cannot be combined with other extracts to create the whole or a majority of a category A program.[13]

Nor can they transmit a category B program or an extract from a category B program (including news, current affairs or weather bulletins and financial or business information) unless the extract is less than ten minutes long, couldn't be combined with other bulletins to form a longer bulletin and is not updated within 30 minutes. Further, a datacaster may not transmit any audio content which would amount to a commercial audio broadcast.[14]

These provisions effectively prohibit any content which might be seen as extracts in the form of either "segments" or "reports" with similar presentation or style, since together they might constitute a longer program.

Datacasters are left with exceptions to this regime to underpin their offerings: information only programs (strictly defined to exclude programs with a significant emphasis on dramatic impact or entertainment),[15] educational programs, parliamentary or court proceedings, interactive computer games, home shopping and, on the face of it, Internet carriage services. However, the carve-out of the genre conditions only applies to full individual point-to-point Internet access, not to content selected and copied from the Internet by the datacating licensee (the "walled garden" model).[16]

INTERNET OVER THE AIR?

Given that individual point-to-point "Turbo Internet" only allows a small number of users to be accommodated by the available bandwidth, it is certainly not a commercially viable model for popular web sites containing streaming video and multimedia material.[17]

The fact that the genre restrictions have been imposed on the "walled garden" model means that datacasters will have to constantly review the content of each web site they transmit and block access to any audio or video content which would offend the genre conditions. Anti-avoidance provisions prevent a datacaster from attempting to evade the conditions by placing their content on a web site and providing a link to that web site.[18]

Senate amendments to the Digital Act inserted an "exception" to the genre conditions for content copied from the Internet, provided that the ABA makes an exemption order on the basis that it is satisfied either that breaches of the genre conditions would be minor, infrequent or incidental; or that transmission of the material would not be contrary to the purpose of the genre conditions. The purpose of the genre conditions is, of course, to restrict broadcasting-style content of precisely the type over which datacasters are likely to seek exemption orders.[19]

This example of circular drafting means that it will be difficult to argue that rich multimedia content fits the exemption conditions. In addition, datacasters will presumably be required to present a case to the ABA for the exemption of each web site they wish to transmit – and they may wish to transmit several hundred sites. Both of these factors tend to the conclusion that the exception is unlikely to allow for very much more transmission of exactly the sort of content which would truly benefit from delivery over the bandwidth.

The way in which the clause giving the ABA power to make an exemption order for content copied from the Internet has been drafted also leaves open the possibility that a new request for exemption will have to be made each time the content of a site is updated. Subclause 27A(1) states that exemption orders may be made *"in relation to the transmission of the matter"*, but does not clarify the coverage of such an order or address the issue of change in the nature of the matter. The ABA's interpretation of the degree to which the matter must be altered before a new request to make an exemption order is required will be crucial to the amendment's effectiveness in achieving what its advocates described as a *"freer and looser"*[20] walled garden, and, ultimately, more viable datacasting services.

COMPETITION SENSITIVITIES

So far, this article has considered the legislative regime for datacasting alone. However, its incorporation into the BSA as part of the package of reforms associated with the conversion to digital television has significant implications for potential datacasters. Digital technology means that delivery mechanisms are an increasingly specious criteria to use when classifying content providers – in effect, the distinctions between datacasters, subscription and free to air broadcasters are being drawn by legislative rather than technological standards. Competition sensitivities, between these three types of content providers are, therefore, more and more a function of the drafting of their legislative frameworks.

Large potential areas for anti-competitive conduct are structured into the Digital Act. For example, the fact that free to air broadcasters will be allowed to broadcast electronic program guides ("**EPGs**") brings them into direct competition with datacasters offering such services. EPGs are the core menu presented to the viewer – therefore the controller of the EPG can control what is viewed, rendering them the pot of gold in digital TV terms.

EPGs are regulated under the Digital Act in an attempt to prevent exclusive alliances between FTAs and datacasters. The Act provides that datacasting licensees may transmit EPGs which contain either:

- information about their own programs; or
- information about television

programs transmitted by commercial or national broadcasters, *so long as* equivalent information is transmitted about its own programs and those of each other commercial or national broadcaster.[21]

However, commercial or national broadcasters must request the transmission of their information before this limitation comes into effect, meaning that common standards will not necessarily be applied in EPGs. A strict interpretation of the term "equivalent information" will also be crucial. Pay television services are not covered at all. This contrasts with the situation in the UK, where the Independent Television Commission created a *Code of Conduct on Electronic Programme Guides*, which not only ensures that there is no discrimination between free to air and pay television services, but also includes exact standards for size, ranking, colour and image of displays connected with broadcasters and restricts the terms of contracts between broadcasters and EPG providers.

Open standards and interoperability are common technical issues in telecommunications, but they are also a regulatory concern for convergent technologies such as datacasting.

Pancaking, otherwise referred to as "the pizza box syndrome", occurs when there is no common denominator between software used in set-top boxes. Under the Digital Act, domestic reception equipment must not be provided by the holder of either a commercial television or a datacasting licence, or a national broadcaster, unless it is also accessible by commercial and national broadcasters and each datacasting service.[22] The legislation also provides for regulations which may deal with technical standards, suggesting any relevant standards must ensure that as far as is practicable, conditional access systems and application program interfaces should be available to all providers of eligible datacasting services. Standards for pay television access are not included. Careful consideration of the content of standards in the regulations to accommodate convergence, and strict enforcement measures, will be required to avoid anticompetitive structures.

CONCLUSION

Given both the restrictive nature of the genre conditions on content which can actually be datacast, and the narrow exceptions allowed for content copied from the Internet, datacasting's appeal to consumers is likely to be limited. Regulating convergent technologies is a difficult task for government. However, attempting to impose strict legislative distinctions between different users of the broadcasting spectrum in order to protect existing businesses is not the best way of going about the regulatory task. The ABA's interpretation of the Digital Act's licensing provisions and exemptions will be determinative for the viability of the datacasting industry. If the industry fails, it may well be the fault of the legislation which enabled its creation.

1 Media Release, Senator The Hon Richard Alston, "Success of Digital TV Will Rely on Consumer Choice", 062/00, 30 June 2000.

2 Ninety nine per cent, or 6.5 million Australian households own a television set, compared to 50 per cent with personal computers, and 25 per cent with access to the Internet: ABS 8147.0, March 1 2000.

3 Department of Communications, Information Technology and the Arts ("DCITA"), Convergence Review, *Convergence Review Issues Paper*, November 1999.

4 Only 15 per cent of non-metropolitan Australians have Internet access at home: ABS 8147.0, March 1 2000.

5 Quoted in Tony Walker, "For giddy limits of datacasting, try a fudged policy", *Australian Financial Review*, 1 July 2000.

6 Tony Branigan, General Manager, Federation of Australian Commercial Television Stations, quoting a US broadcaster at the IBC "The Future of Television is Digital TV" Conference, Sydney, 29 May 2000.

7 The definition is now found in section 2 of Schedule 4 to the *Broadcasting Services Act 1992* (Cth) (to be referred to in this article as the "BSA").

8 Productivity Commission, *Broadcasting Inquiry Report*, Report No 11, 3 March 2000, p 5.

9 Digital Act, Schedule 1, items 14 and 140 (which inserts a new Schedule 6 – Datacasting Services into the BSA).

10 Giles Tanner, General Manager, ABA, "Turning Off Mt Barrow: The Regulatory Challenge of Digital Television", Gilbert & Tobin Digital Revolution Conference, Sydney, 14 June 2000. See the amendment to s 34 of the BSA, and the new s 102B of the *Radiocommunications Act 1992*.

11 Digital Act, Schedule 1, item 140 (Clause 61 of new Schedule 6 to the BSA).

12 Digital Act, Schedule 2, item 20.

13 Digital Act, Schedule 1, item 140 (Division 1 of Part 3 of new Schedule 6 to the BSA, clauses 13 and 14 (Category A) and 15 and 16 (Category B)).

14 *Ibid* (Division 2 of Part 3 of new Schedule 6 to the BSA).

15 *Ibid* (Part 1 of new Schedule 6 to the BSA, clause 4).

16 *Ibid* (Division 3 of Part 3 of the new Schedule 6 to the BSA).

17 At least one potential datacaster has suggested that in a 7MHz bandwidth, only 20 people could receive streaming video at the same time, eliminating the commercial viability of providing this service for the most popular web sites containing rich multimedia content.

18 Digital Act, Schedule 1, item 140 (Division 2A of Part 3 of the new Schedule 6 to the BSA).

19 *Ibid* (Division 4 of Part 4 of the new Schedule 6 to the BSA).

20 Doorstop interview, "Digital Television and Datacasting Legislation, ABC and SBS and Multichannelling", Stephen Smith, Shadow Minister for Communications, Parliament House, Canberra, 29 June 2000.

21 Digital Act, Schedule 1, item 140 (Division 1A of Part 3 of the new Schedule 6 to the BSA).

22 Digital Act, Schedule 1, item 125A (inserting new Part 3A of Schedule 4 to the BSA).

Joanna Davidson is a Research Assistant at the Sydney office of Allen Allen & Hemsley.

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.

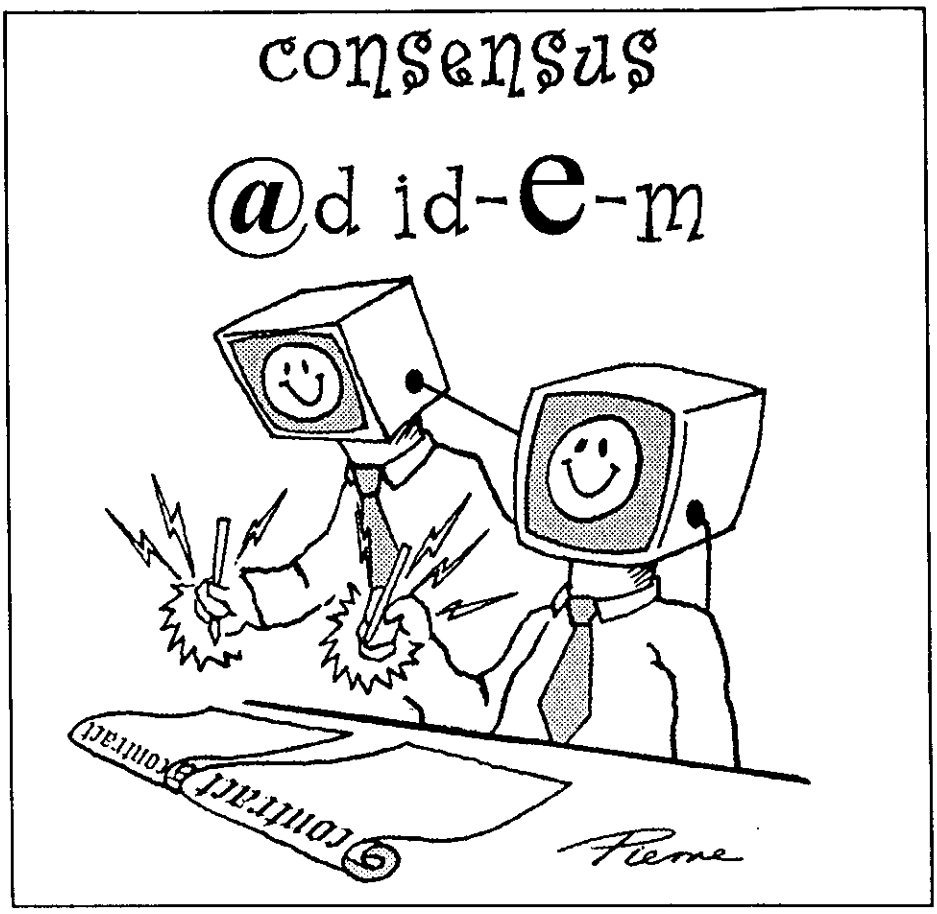
By just about all accounts, the pace of growth and take-up of the Internet is enormous, outstripping every other technological development in recent times. E-commerce is not only becoming an important part of retail business, but also business-to-business transactions. Alan Greenspan was stating the 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.

Cybertrading – Australian Regulatory Issues

Niranjan Arasaratnam discusses some of the key regulatory issues relating to cybertrading.

Internet technology is profoundly affecting the evolution of financial services activities. Issuers and financial services providers increasingly sell securities or provide financial services on the Internet. The power of the Internet to attract buyers and sellers without the constraints of geography and its efficiencies with respect to transparency of price, make the Internet an appealing medium for the financial services industry.

Australia has been no exception to the global trend. Online stock broking services have been phenomenally successful with Australian investors. By the end of last year, there were thirteen Internet brokers in Australia, with one listed on the Australian Stock Exchange ("ASX"). The number of registered online users is estimated to exceed 500,000, with the dollar value of Internet trading having grown from 0.05% in June 1998 to 1% by June 1999. Approximately 10% of all ASX trading is now conducted online, rising to 20% of retail trades.

The success of online brokers has led to the development of online financial service aggregators. These aggregators establish themselves initially as online broking providers and then, leveraging their existing client base, expand into insurance and a range of other financial services. This business model has led banks such as Westpac and Commonwealth Bank to roll out online broking services following the establishment of their online banks.

These developments are not without their regulatory risks. Cybertrading is increasingly attracting scrutiny from Australian regulators. This article discusses some of the issues and pitfalls of cybertrading in Australia.

FACILITATING ELECTRONIC TRANSACTIONS

A number of legislative changes to the *Corporations Law* have occurred in recent years to facilitate electronic communications. For example, the definition of terms such as "document", "writing" and "record" in the Corporations Law were widened in the early 1990s to encompass many types of electronic communication. More recently, the *Company Law Review Act 1998* (Cth) introduced reforms in order to facilitate electronic service of notice to members' and directors' meetings. One of the major goals of the *Corporate Law Economic Reform Program Act 1999* (Cth), which commenced in March this year, is to facilitate the more widespread use of electronic commerce.

However, the most significant step toward the promotion of electronic commerce occurred in December last year with the enactment of the *Electronic Transactions Act 1999* (Cth). This Act is facilitative rather than prescriptive in that it is only intended to enable rather than require electronic transactions. The Act is based on two key principles: functional equivalence and technological neutrality. Functional equivalence means that existing laws should apply equally to electronic and paper transactions. Technological neutrality ensures that no one particular technology is mandated by law, so that the law does not become redundant as technology develops.

Due to constitutional limitations, the Act only applies to Commonwealth laws. The States and Territories must enact mirror legislation to allow the application of the Act to State and Territory laws.

There are four key provisions of the Act:

- An electronic signature will be recognised as equivalent to a handwritten signature provided the electronic signature identifies the person, indicates the person's approval of the information communicated and was appropriately reliable for the purposes for which the information was communicated at the time the method was used.

- Where a Commonwealth law requires information to be given in writing, that requirement will be satisfied by the provision of an electronic communication where at the time the information was given it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference and the recipient of the information consents to the electronic form of communication.

- A person will satisfy the legal requirements for producing a document where the method of generating the electronic form of the document provided a reasonably reliable means of assuring the maintenance of the integrity of the information contained in the document, and it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference.

- The time that a person is deemed to have sent a document occurs when the communication enters a single information system outside the control of the originator. The time of receipt occurs when the communication enters the system designated by the

recipient as the address for receiving electronic communications. If no such address has been designated, receipt will occur when the communication comes to the addressee's attention. These deeming rules can be displaced by mutual agreement of the parties to the communication.

ONLINE SECURITIES MARKETS

As the market for online stock broking services increases, Australia is seeing the emergence of online exchanges for other financial products, such as bonds, foreign exchange and managed investment funds. All these exchanges use the Internet as a means to drive down transaction costs, facilitate cross-border transactions and avoid the need to conduct trades using intermediaries. They allow for direct retail participation in markets that were once the domain of institutions and intermediaries.

The establishment and operation of such exchanges requires a stock market licence under the Corporations Law. However, the licensing regime for stock markets has become increasingly redundant given the changing character of markets emerging from developments in information technology. The Australian Securities and Investments Commission ("ASIC") considers a number of factors when assessing an application for a stock exchange including the regulation of intermediaries; ensuring the adequacy, accuracy and availability of market information; support of an orderly and fair trading system; ensuring a speedy, economical and certain clearing and settlement system; the solvency of the market provider; and adequate market supervision arrangements.

Curiously, certain bulletin boards that regularly provide information about the prices of securities may be a "stock market" requiring licensing under the Corporations Law. This may be the case even if contracts for the sale and purchase of securities are not made directly on, or through, the bulletin board. If a bulletin board provides potential vendors and purchasers with a reasonable expectation that they can regularly execute orders at the prices quoted, by identifying people likely to deal at the quoted prices, the bulletin board will be regulated as a stock market. Bulletin boards are more likely to fall within the regulations where they facilitate the linking of buying and selling interests (for example by providing information over the telephone).

In response to proposals for an integrated framework for financial products, service providers and markets, the government has released draft provisions of a *Financial Services Reform Bill*, which would replace the part of the Corporations Law dealing with securities, exchanges and stock markets with a single licensing regime for financial products markets.

PROSPECTUSES

In Australia, the first prospectus distribution over the Internet (as well as in paper form) occurred in July 1996. More recently, ASIC granted relief to allow a completely online application process including the use of an electronic payment system.

ASIC permits the issue of electronic prospectuses provided the text-based information in the prospectus contains the same information as the paper-based prospectus. The electronic application form and prospectus can only differ from the paper application form and prospectus lodged with ASIC in the following limited ways:

- the different technological tools available to readers of electronic as distinct from paper documents (eg hypertext links and prompts);
- the difference between the paper and electronic environments (eg the absence in the electronic document of graphics and other decorative material); and
- investor protection mechanisms (eg the electronic prospectus must warn investors from passing on to another person the application form without a complete and unaltered form of the prospectus).

ASIC permits a fully electronic application process for securities subject to a number of conditions such as ensuring that the prospectus is provided at the same time as the application form. It has recently granted exemptions from the Corporations Law so that licensed dealers may personalise and issue application forms for securities, created either by themselves or issuers. This could allow for personalised and interactive application mechanisms.

In addition, ASIC permits Internet hosts to act as service providers and distribute electronic prospectuses through the Internet.

More recently, in December last year, ASIC released an issues paper discussing whether or not multimedia material should be included in prospectuses and other offer documents. One key policy concern that ASIC is currently grappling with is that multimedia prospectuses will disadvantage those who cannot access the electronic material. Another issue is consistency of the medium in which information is presented. The issue of electronic prospectuses cannot, however, be considered purely in an Australian context given the difficulties in placing jurisdictional limitations on securities offers.

FOREIGN SECURITIES OFFERS AND ADVICE

The Internet provides a quick and inexpensive distribution mechanism for offers, invitations and advertisements of securities. This raises the ability of overseas issuers and investment advisers to offer and advertise securities in Australia without any regulatory scrutiny or oversight. It also means that for those involved in making prospectuses available on the Internet, there is uncertainty about the application of the laws of the jurisdictions in which the offers or advertisements can be accessed.

ASIC considers that the Australian securities laws may apply to offers or invitations on an Internet site if that site is accessible from Australia, irrespective of where the offeror is located.

ASIC will not regulate offers, invitations or advertisements of securities that are accessible in Australia on the Internet if they:

- are not targeted at Australians;
- contain a meaningful jurisdictional disclaimer;
- have little or no impact on Australian investors, and
- there is no misconduct.

Foreign Internet investment advisers will be subject to Australian licensing requirements where they email investment advice to Australian investors. The investment advice licensing provision of the Corporations Law may also apply to investment advice provided on an Internet site (eg a home page outside Australia) that is accessible in Australia.

ASIC recognises that it can be difficult to enforce the Corporations Law fully in relation to investment advisers located outside Australia. To overcome this difficulty, ASIC intends to work closely with other, foreign, regulators and with IOSCO to ensure that the interests of Australian investors are protected and that confidence in the integrity of the Australian securities market is maintained.

FINANCIAL ADVICE ON THE INTERNET

As the Internet has become more accessible to the public, there has been an increase in the number of people providing investment advice on securities using the Internet. Internet advice may take a number of forms including investment advice on a homepage or investment advice sent by electronic mail.

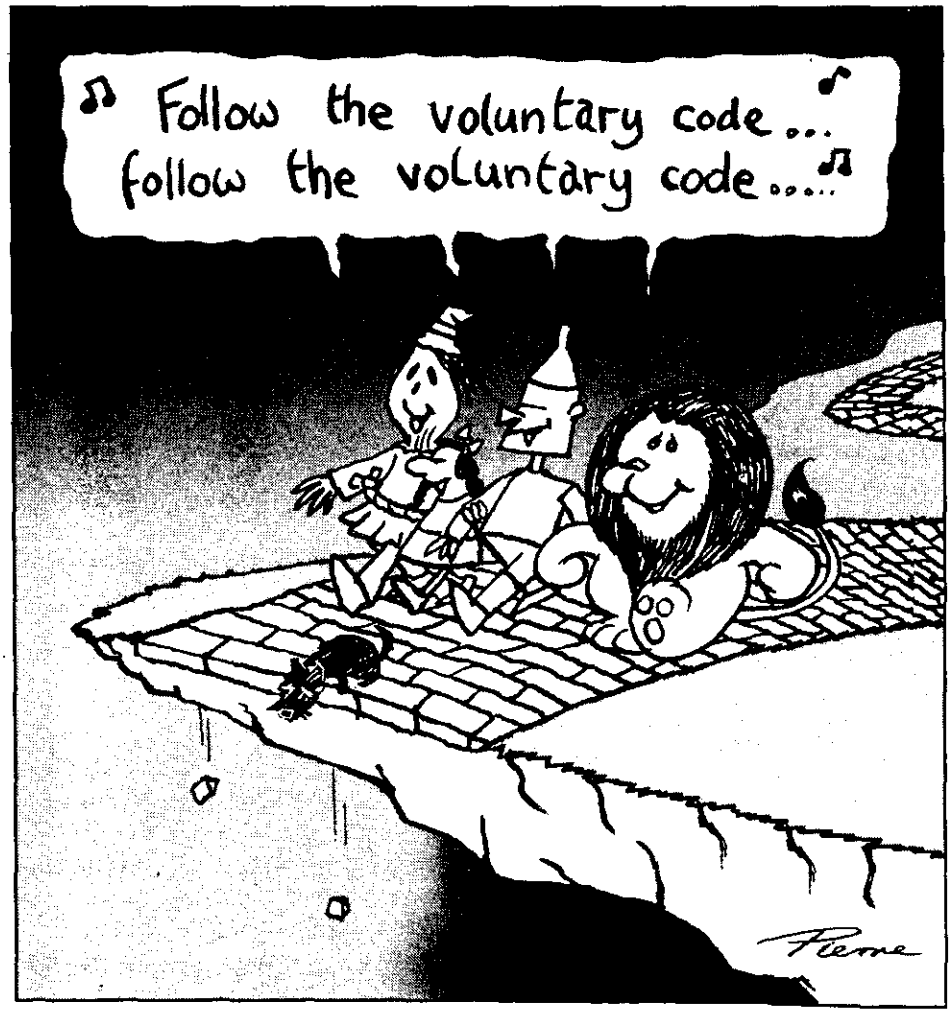
Providers of investment advice are required to be licensed under the Corporations Law. In addition, providers of investment advice or reports on the Internet may need a dealers licence instead of an investment advisers licence if the adviser receives commissions and other benefits from product providers for offering the advice.

ASIC takes the view that most of the licensing requirements apply to investment advice on the Internet in much the same way as they apply to investment advice in any other medium.

A person providing investment advice on the Internet requires a licence if they are in the business of providing direct or indirect securities recommendations, general securities advice or publishing analysis or reports on securities. Under the common law, in order to carry on a business, one needs to satisfy the requirements of system, continuity and repetition. The Corporations Law does not require that the business be carried on for a profit. Therefore, even if the Internet adviser does not get paid for giving the advice, the activity may still be a business if it is done with system, continuity and repetition. The investment advice may be provided as part of any other business. This means that any on-line service with a home page about securities or tips on securities will be subject to the licensing requirements of the Corporations Law.

However, it is possible to avoid the licensing regime if a web site provides purely factual information about securities on the Internet. In order for this to happen a web site must:

- not provide any direct or implicit advice or opinion on securities;
- provide warnings to the effect that the information is not suitable to be acted



on as investment advice and that it may be advisable to obtain investment advice before making decisions in reliance on the information.

Another exemption to the licensing requirements applies to "media advisers". Media advisers give investment advice on securities using the media such as newspapers, periodicals and information services that are generally available to the public. However, ASIC considers that it will generally be difficult for an Internet investment adviser to fall within the media adviser's exemption.

ASIC's regulatory scrutiny has extended to Internet hosts which publish prospectuses on their web sites. By publishing electronic prospectuses on a web site dedicated to providing that service an Internet host may be conducting an investment advice business. However, ASIC considers that there is no net regulatory benefit in requiring a person to be licensed as an investment adviser if they are acting purely as a service provider distributing electronic prospectuses via the Internet.

PRIVACY

Tailoring is crucial to offerings of online financial services, however privacy regulations in Australia, as well as a privacy-aware consumer base, are making it increasingly difficult to leverage customer data without obtaining specific customer consent.

On a spectrum of privacy regulation, Australia's privacy regime generally sits somewhere between the US and the European Union, with the private sector remaining largely self regulated. The *Privacy Act 1988* (Cth) is essentially limited to:

- information and handling practice of the Commonwealth and ACT agencies;
- those who hold and use tax file numbers;
- the activities of credit providers and credit reporting agencies in relation to consumer credit (ie information relating to a consumer's credit worthiness).

There is industry specific legislation which includes elements of privacy protection. However, this legislation is limited to particular competitors in the industry which is the subject of the legislation. For example, the *Telecommunications Act 1997* (Cth) imposes obligations on telecommunications carriers and carriage service providers (and their employees and contractors) to protect the confidentiality of information that relates to the contents of communications carried by their services.

The Privacy Commissioner, appointed by the Commonwealth as a privacy watchdog, tried to overcome the regulatory void by promulgating the *National Principles for the Fair Handling of Personal Information*. This code is a voluntary set of privacy guidelines modelled around the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

Some industries have also attempted to regulate data protection practices amongst their members. Codes of practice that contain provisions dealing with privacy include the Internet Industry Code of Practice, the Australian Communications Industry Forum Industry Code for the Protection of Personal Information of Customers of Telecommunications Providers and the Banking Code of Practice. However, as these codes are largely voluntary, their lack of compulsion diminishes their coverage. For example, only some 60 of the 700 odd ISPs in Australia subscribe to the IIA Code, notwithstanding that it complies with international standards and Australian Standard 4269-1995.

More recently, the Commonwealth government announced its intention to institute a light-handed legislative regime based on the Privacy Commissioner's *National Principles For the Fair Handling of Personal Information* and the OECD Guidelines. The intention is to ensure Australia complies with the data transfer provisions of the EU Data Protection Directive.

The proposed legislative scheme will enable business to develop codes which are consistent with the legislative standards and which can be approved by the Privacy Commissioner. The approval of a code by the Privacy Commissioner will be a disallowable instrument, subject to parliamentary scrutiny.

Codes may be developed by members of an industry body, a specific industry sector or interested organisations or individuals wanting a code to cover a particular type of information or activity. Where there is no approved code, the default legislative principles and complaint mechanism will apply.

The default legislative principles will be known as the National Privacy Principles ("**NPPs**"). The privacy rules in the industry codes, so called Code Privacy Principles ("**CPPs**"), must replicate or incorporate the NPPs, providing at least the same level of privacy protection. An organisation bound by a privacy code should not do an act or engage in a practice in breach of a CPP in that code, and if it does so, that will constitute an interference with privacy.

The legislative scheme aims to establish a "level playing field" for private sector organisations and individuals, regardless of whether an organisation is covered by a code or by default legislative provisions. If an individual feels that an organisation has breached privacy standards in relation to their personal information, they will have the right to make a complaint that their privacy has been breached.

The Commonwealth indicated in September last year that the draft legislation would be released in late 1999 with enactment in mid-2000. There would then be a one year moratorium on the enforcement of the legislation to give organisations an opportunity to institute appropriate practices to ensure compliance with the law. So far, the government has released a discussion paper in December last year setting out the key provisions of the proposed

legislation. The government's timetable appears to have stalled and the government is yet to clarify its position.

The key privacy principles under the proposed legislation include that personal information should be:

- kept secure;
- used or disclosed only in ways consistent with an individual's expectations or as required in the public interest;
- kept accurate and open to individuals to correct should it be inaccurate;
- only transferred to other organisations if it will be properly protected; and
- personal information must not be transferred to a jurisdiction that does not have comparable data protection laws.

In addition to regulatory sensitivity to privacy concerns, online payment systems have also recently attracted government attention.

EFT

The emergence of online trading of financial products has significantly encouraged online payment systems. However, even though Australians are enthusiastic adopters of new technology, privacy and security concerns inhibit the growth of online payments systems.

Until now most of the security concerns were dealt with by the EFT Code of Conduct. However, this code applied only to electronic funds transfer occurring by way of magnetic strip cards linked to an account and accessed by a PIN, using systems such as automatic teller machines and electronic point of sale facilities.

In April 1999, ASIC established a working party to examine the EFT Code in an effort to expand it to cover a broader set of electronic transactions made possible by the introduction of new technologies such as the Internet. The expanded code will substantially increase the consumer protection available to users of online payment systems, as it will introduce new provisions allocating liability for unauthorised transactions and system or equipment malfunctions. It also includes amended provisions on privacy and complaint handling.

It is proposed that the code will be divided into three parts. Part A will cover transactions which bring about funds transfers to or from or between accounts at institutions by remote access, such as internet and telephone banking, and credit card transactions not involving a physical signature. Part B will cover new electronic payment products which effect payment by the transfer of pre-paid value (such as stored value card balances or digital coins) but do not involve accounts at account institutions. Part C will apply to both types of transactions and sets down rules for electronic communication between transaction providers and users, including rules for privacy. It is hoped that the final version of the code will be completed by mid-year.

The key features of the Code are:

- Terms and conditions must be prepared by account institutions and must be clear and unambiguous, reflecting Code requirements. The terms and conditions must not provide for liabilities and responsibilities of users which exceed those set out in the Code and are to include a warranty that the requirements of the Code will be complied with. There are also requirements for the provision of terms and conditions and other information before an access method has been used for the first time.
- The code sets out requirements for records of EFT transactions, particular requirements for voice communications, as well as periodic statements and advice on security of access methods with account statements to be provided at least annually.
- An initial no-fault allocation of liability in all cases where a secret code is required to perform the unauthorised transaction. An account holder will be liable for a maximum of $150 unless the account institution can prove that the user contributed to the loss through unreasonably delaying notification, fraud, or contravening the requirements for protection of the security of their access method.
- Account institutions will be liable for loss caused by failure of their system or equipment to complete transactions accepted by that system in accordance with a user's instructions. The institution must not either implicitly or explicitly deny a user's right to make claims for consequential damage arising from system malfunction.
- Guidelines for interpretation of the National Privacy Principles in relation to EFT Transactions, including requirements for disclosure of surveillance device usage.

CONCLUSION

Australia is developing an increasingly specific regulatory environment for internet securities trading, and for online financial services generally. The government aims to achieve a more flexible and responsible financial system through its corporate law reform program, and new technology is rapidly being specifically addressed by various regulators under the strong influence of international developments. Much activity is likely over the next twelve months in this area, instituting some reforms of a significant scale with potential impact on legislative compliance costs.

Niranjan Arasaratnam is a senior associate of the Sydney office of Allen Allen & Hemsley.

The Communications Law Bulletin is the journal of the Communications and Media Law Association (CAMLA) which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

Contributions and Comments

are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in hard copy and on disk and comments should be forwarded to:

Niranjan Arasaratnam
c/- Allen Allen & Hemsley
Lv 23 The Chifley Tower
2 Chifley Square
SYDNEY NSW 2000
Tel: +612 9230 4280
Fax: +612 9230 5333
Email:
niranjan.arasaratnam
@allens.com.au

Communications and Media Law Association

The Communications and Media Law Association (**CAMLA**) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- defamation
- contempt
- broadcasting
- privacy
- copyright
- censorship
- advertising
- film law
- information technology
- telecommunications
- freedom of information
- the Internet & on-line services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

CAMLA Website

Visit the CAMLA website at www.gtlaw.com.au/camla for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

To: **The Secretary, CAMLA, Box 545, Glebe, NSW 2037**
Tel/Fax: +61 2 9660 1645

Name: .....

Address: .....

Telephone: .....Fax: ..... DX: .....

Principal areas of interest: .....

.....

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

- Ordinary membership $95.00 (includes subscription to CLB)
- Corporate membership $425.00
  (list names of individuals, maximum of 5)
- Student membership $35.00 (please provide photocopy of student card - full time undergraduate students only)
- Subscription without membership $95.00
  (library subscribers may obtain extra copies for $10.00 each)

Signature .....