Communications 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 AND SHANE BARBER Vol 20 No 2 2001

Electronic Transactions Update

Catherine Dickson revisits the Federal Government's Electronic Transactions Act, 1999 in light of its 1 July 2001 "changeover" date and also looks at the response of the States and Territories in the two years since the Act's commencement.

It has been eighteen months since the Federal Government enacted the *Electronic Transactions Act* (**ETA**) as its foundation for a framework for developing the information economy in Australia. This article looks at the certainty of the Australian legislative environment for e-business.

BACKGROUND

ETA was enacted by the Australian Federal Government in 1999 following an examination by the Electronic Commerce Expert Group (**ECEG**) of the suitability of Australian law to encourage and facilitate electronic commerce in Australia. Areas where the ECEG saw Australian law as being unclear or not facilitating electronic transactions were:

- uncertainty as to whether information, records and signatures in an electronic form should be given legal effect;
- a number of different form provisions requiring a document to be in writing where it was unlikely that an electronic document or signature would satisfy these requirements;
- no general provision allowing a data message to satisfy requirements of an original;
- no uniformity as to the admissibility and evidential weight of electronic documents;
- no uniform approach to retention and management of electronic documents; and
- uncertainty concerning the use and validity of data messages in contract formation.

The role of the ETA is largely to provide a framework for certainty and to ensure that electronic transactions have the functional equivalence of paper transactions.

PURPOSE OF THE LEGISLATION

ETA was enacted by the Federal Government as part of its strategic framework for developing the information economy in Australia. ETA creates a light handed regulatory regime for using electronic communications in transactions. It attempts to remove existing legal impediments that may prevent a person using electronic communications to satisfy legal obligations under Commonwealth law. The simplified outline of ETA[1] provides that for the purposes of a law of the Commonwealth a transaction is not invalid because it took place by means of one or more electronic communications. It also provides that the following requirements imposed under a law of the Commonwealth can be met by using electronic form:

- the requirement to give information in writing;
- the requirement to provide a signature;
- the requirement to produce a document;
- the requirement to record information; and

INSIDE THIS ISSUE

CONTENTS

- the requirement to retain a document.

For the purpose of a law of the Commonwealth, ETA provides criteria for determining the time and place of the dispatch and receipt of an electronic communication. It also provides that the purported originator of an electronic communication is bound by it for the purposes of a law of the Commonwealth only if the communication was sent by the purported originator or with the authority of the purported originator.

IMPLEMENTATION OF COMMONWEALTH LEGISLATION

ETA has a two-stage implementation. Before 1 July 2001 it will only apply to Commonwealth laws specified in the regulations. After 1 July 2001 it will apply to all Commonwealth laws unless they have been specifically exempted from application by the regulations. The *Electronic Transactions Amendment Regulations 2001 (No. 2)* sets out the extent to which ETA will not apply to particular Commonwealth Acts as from 1 July 2001.

Under the Electronics Regulations 2001 (No. 2) there is a list of 157 Commonwealth Acts and subordinated legislation that have been excluded (in whole or in part) from the operation of ETA from 1 July 2001. The list is more extensive than expected and includes legislation such as the Corporations Law (now known as *Corporations Act 2001*), *Evidence Act 1995*, superannuation legislation and insurance legislation. The extent of the list is disappointing given the Federal Government's objective of bringing all appropriate department and agency services online via the internet by 2001.

CONSENT

Commonwealth entities subject to ETA are required to accept electronic communications as long as it is reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference. However Commonwealth entities are entitled to impose conditions. Permissible conditions include those in relation to particular information technology requirements (including any particular electronic signature technology) that must be used, also any action a person must take to verify receipt of information. Under the Uniform Scheme, state entities will only be required to accept electronic communications if they have consented to such communications.

REQUIREMENT FOR A UNIFORM SCHEME

The Federal Government only has the constitutional power to legislate in specific areas, with the States and Territories having power to legislate in all other areas. To ensure that the principles contained in ETA apply to

all areas of Australian law, the Australian States and Territories have publicly committed to enacting uniform legislation Australia-wide modelled on ETA (Uniform Scheme).

As of June 2001, Queensland, Victoria and Tasmania have electronic transactions acts and the other States and Territories are in the process of legislating. The *Electronic Transactions Act* (NSW) was assented to on 3 May 2000 but has yet to be proclaimed. Until all States and Territories have legislated to give electronic communications functional equivalence to paper documents it will remain unclear as to whether and to what extent Australian law will enforce electronic contracts.

Even with the Uniform Scheme in place it looks like there will continue to be uncertainty under Australian law with respect to electronic contracts. Ascertaining the time and place of a communication is particularly important when the communication is the acceptance of an offer. The general principle is that acceptance of an offer must be communicated to the offeror for there to be a binding contract between the parties. However this is not the case where the postal acceptance rule applies.

Where the means of communication between the offeror and the offeree is instantaneous, such as in the case of telephone or facsimile communications, the formation of a contract is governed by the general rule that a contract is concluded at the time when, and the place where, acceptance of the offer is received by the offeror. However where acceptance by post is contemplated by the parties, acceptance is completed as soon as the letter of acceptance is properly posted.[2] There has been some discussion as to whether an internet communication is more closely aligned to an instantaneous means of communication or to a letter that is put in the postal system.

ETA and the Uniform Scheme deal with the uncertainty surrounding time and place of receipt of electronic information by providing that if an information system has been designated for the purpose of receiving electronic communications then the time of receipt is the time when the electronic communication enters that information system.[3] If there has been no designation of an information system then communication is taken to have been received when the electronic communication comes to the attention of the addressee.[4] Unless otherwise agreed, the place of receipt of an electronic communication is the place where the addressee has its place of business.[5] These provisions still leave uncertainty regarding electronic communications. They do not:

- deal with the uncertainty surrounding the application of the postal acceptance rule to the formation of online contracts. Having said this it is likely (although not yet determined by the Courts) that the postal acceptance rule would probably not be applied to data messages;[6]

- say anything regarding allocation of liability for the risk of non-delivery by an electronic system. If an information system is designated as a means of communication the sender/offeror takes the responsibility for non-delivery of the communications system up until the information enters a recipient's communication system;

  or

- entirely create certainty regarding receipt issues. If an information system is not designated by the parties then it remains unclear whether the words "comes to the attention of the addressee" means when the addressee has read the communication or has received a notification of mail.

ELECTRONIC SIGNATURES

The Government's legislative framework for e-business has not addressed the continuing uncertainty as to what will suffice as an electronic means of authentication for online contracts. The Federal Government and the ECEG for reasons such as flexibility, neutrality and avoiding enshrining in legislation what may prove to be incorrect guesses about best technology and business practices, made a decision to take a minimalist approach in giving legislative direction. However this light touch approach has resulted in uncertainty, particularly in relation to electronic signatures, that is not helpful to organisations doing e-business or looking to do e-business in Australia.

ETA and the Uniform Scheme provide that *if a signature of a person is required*, that requirement is taken to have been met in relation to an electronic communication if:

> *(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and*
>
> *(b) having regard to all the relevant circumstances when the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and*
>
> *(c) the person to whom the signature is required to be given consents to the requirement being met by using the method mentioned in paragraph (a)*[7]

It is likely that this provision does not extend to electronic signatures in electronic contracts as it is limited to where a signature is "required". The use of signatures for private transactions is a standard business practice to ensure that at the time of affixing the mark, the signatory has the necessary intention to be bound by the contents of the document. There is no legal *requirement* that a signature be affixed to a simple contract. In fact, oral contracts are enforceable. The purpose of a signature in a simple

contract goes more to the objective intention of the parties to be bound by a contract's terms and the integrity of the document. An original signature together with original initialled amendments demonstrates that the document has not been changed without obtaining the parties' express approval.

ENFORCEABILITY OF ELECTRONIC CONTRACTS

The integrity of a document is essential for it to be given weight as evidence by the Australian Courts. ETA and the Uniform Scheme do not directly deal with the enforceability of electronic contracts. The ECEG in its report to the Attorney General, considered that the Commonwealth and NSW Evidence Acts satisfy basic requirements for admissibility and the evidential weight of electronic documents as evidence. They considered that further law reform to deal with perceived problems with the admission of data messages was not the appropriate solution.[8] They recommended instead that the NSW and Commonwealth Evidence Acts be used as a model for a uniform approach to evidence in Australia.

It has been 3 years since the ECEG's recommendations were released and there is still no uniform approach to the admissibility of electronic evidence as evidence in Australia. The perceived problems listed by the ECEG in their report regarding electronic evidence[9] have not been uniformly addressed. Consequently, it does not appear that electronic transactions will have the functional equivalence of paper transactions at least for evidentiary purposes. One of the fundamental purposes of recording contractual arrangements and affixing signatures to such records is to ensure that such agreements are enforceable. So in this fundamental respect the validity of electronic signatures and consequently the legislative framework for enforceability of electronic contracts remains unsatisfactorily vague.

Nevertheless, under ETA there is a requirement for electronic documents that are produced (whether they are required to be produced or permitted to be produced) to have a level of integrity.[10] This raises the question of how the laws as to admissibility and evidential weight contained in Federal and State and Territory legislation will be read in conjunction with ETA and the Uniform Scheme. It would seem possible that if a document is admissible by a Court in paper form, then it may be produced by means of electronic communication if it complies with the production requirements in the Uniform Scheme. This raises the question whether production to a court is possible under the Uniform Scheme even if not permitted under the relevant Evidence Act.

Despite ETA, the announcement of the Uniform Scheme and the ground work the Federal Government has done in establishing a framework for electronic business, there are still uncertainties surrounding the enforceability of electronic transactions under Australian law. However, these are not necessarily insurmountable. Conducting business by digital means, and particularly over open systems such as the internet, affects some of the fundamental assumptions on which business has been traditionally based. These assumptions and the changes affecting them have to be analysed thoroughly and procedures have to be put into place to manage new risks before Australian businesses and consumers can rely with any certainty on electronic means as a way of conducting business.

1 s.4 Electronic Transactions Act 1999 (Cth)

2 *Mendelson – Zeller Co Inc v T & C Providores Pty Ltd* [1981] INSWLR 366

3 Section 14(3) Electronic Transactions Act 1999 (Cth)

4 Section 14(4)

5 Section 14(5)(b) Ibid

6 p63 Electronic Commerce: Building the Legal Framework Report of the Electronic Commerce Expert Group to the Attorney General, 31 March 1998

7 s.14 Electronic Transactions (Queensland) Act 2001

8 p39 Chapter 2 "Electronic Commerce: Building the Legal Framework Report of the Electronic Commerce Group to the Attorney General" 31 March 1998

9 see p35 ff Ibid

10 Section 11 Electronic Transactions Act (Cth)

The views expressed in this article are those of the author and not necessarily those of the firm or its clients.

Catherine Dickson is a Counsel in the Information Technology and Telecommunications practice at the Sydney Office of PricewaterhouseCoopers Legal.

Combating Cybercrime

The Federal Government has introduced new legislation to combat the problems of cybercrime, Niranjan Arasaratnam and Maree Flynn explain.

On 27 June, the Government took aim at hackers and website vandals with the introduction of the *Cybercrime Bill 2001* (**Bill**). The Bill significantly bolsters the range of computer offences by adding a new Part 10.7 to the *Criminal Code Act 1995* (**Criminal Code**). The computer offences are modelled on the *January 2001 Model Criminal Code Damage and Computer Report* developed through Commonwealth, State and Territory cooperation. The Bill repeals the existing offences in Part VIA of the *Crimes Act 1914* (**Crimes Act**) which were enacted in 1989 and are considered irrelevant to today's technology.

The Bill also significantly enhances the investigation powers of law enforcement authorities for searching and seizing electronically stored data by amending the Crimes Act and *Customs Act 1901* (**Customs Act**). These amendments build upon the existing provisions which were enacted in 1994 and take into account the draft Council of Europe Convention on Cybercrime. There are also consequential changes to the *Australian Security Intelligence Organisation Act 1979* (**ASIO Act**), *Education Services for Overseas Students Act 2000* (**ESOS Act**) and the *Telecommunications (Interception) Act 1997* (**TI Act**).

There are estimates that cybercrime is costing companies worldwide approximately $3 trillion a year. The growth in the Internet population and electronic commerce over the last decade means cybercrime is a realistic and substantial threat to the security and reliability of computer data. The Federal Minister for Justice and Customs, Senator Christopher Ellison, has stated that the Bill aims to strengthen business, government and community confidence in using new technologies:

> *The large amount of data that can be stored on computer drives and disks and the complex security measures, such as encryption and passwords, which can be used to protect that information present particular problems for investigators. The legislation will enable police powers to copy computer data and examine computer equipment and disks off-site, enabling them to obtain assistance from computer owners.*

The new offences contained in the Bill also cover using a computer to commit serious offences such as stalking, fraud or sabotage. The maximum penalty contained in the Bill is up to 10 years imprisonment.

COMPUTER OFFENCES

There are 7 new computer offences. These offences have extraterritorial jurisdiction recognising that computer crime often occurs outside the country. It will not matter where the conduct constituting an offence takes place, because if Australia is affected then prosecution can take place here. This means that an Australian citizen travelling to a country where hacking is not an offence, who then uses a laptop computer to hack into a computer in a third country, will be liable.

The Bill provides for concurrent operation of Commonwealth, State and Territory laws to avoid any gaps in jurisdiction and allow computer crimes to be prosecuted where it is most convenient. For example, the State and Territory computer offences would cover computer crime activities by employees using an internal computer network. The Commonwealth cannot regulate this conduct because computer crime on such networks does not use the telecommunications system.

The new offences apply to computers, computer data, or communications to or from a computer. The Government has left the term "computer" undefined so that the proposed computer offences embrace technological change. This complies with the discussions raised in the *Model Criminal Code Report* on computer offences that a restrictive definition may unduly limit the application of the proposed offences.

Summary of 7 new offences

The following is prohibited:

- Unauthorised access or modification of computer data or impairment of electronic communications to, or from, a computer. There must be an intention to commit a serious offence which is punishable by 5 or more years imprisonment. The penalty applying is the equivalent for the serious offence. So a hacker accessing credit details in a bank computer and intending to use them to steal money, would face the same 10-year-penalty imposed for a fraud offence.

- Unauthorised modification of data in a computer by a person who is reckless about whether data will be impaired. A maximum penalty of 10 years imprisonment applies. This offence is wideranging and can cover unauthorised access to a computer system and impairing data, or using a disk containing a computer virus to sabotage a computer.

- Unauthorised impairment of electronic communications to, or from, a computer. A maximum penalty of 10 years imprisonment applies. This offence aims to prevent "denial of service attacks" caused when a computer server crashes after a website is swamped with excessive amounts of unwanted messages. The high penalty recognises that such damage can be comprehensive and expensive.

- Unauthorised access to, or modification of, restricted data held in a computer. This only applies to accessing or modifying data protected by a password or other

security feature. A maximum penalty of 2 years imprisonment applies. People illegally entering protected computer systems to access or alter personal or commercial information are targeted.

- Unauthorised impairment of the reliability, security or operation of any data held on a Commonwealth computer disk, credit card, or other device. A maximum penalty of 2 years imprisonment applies. Examples of impairing data are destroying computer disks or using magnets to affect credit cards.

- Possession and supply of data or programs intended to be used to commit a computer offence are covered by two new offences. A maximum penalty of 3 years imprisonment applies. Traders of programs for hacking and inserting computer viruses would be caught by this provision.

Consequential Changes

The repeal of the existing computer offences would also mean that:

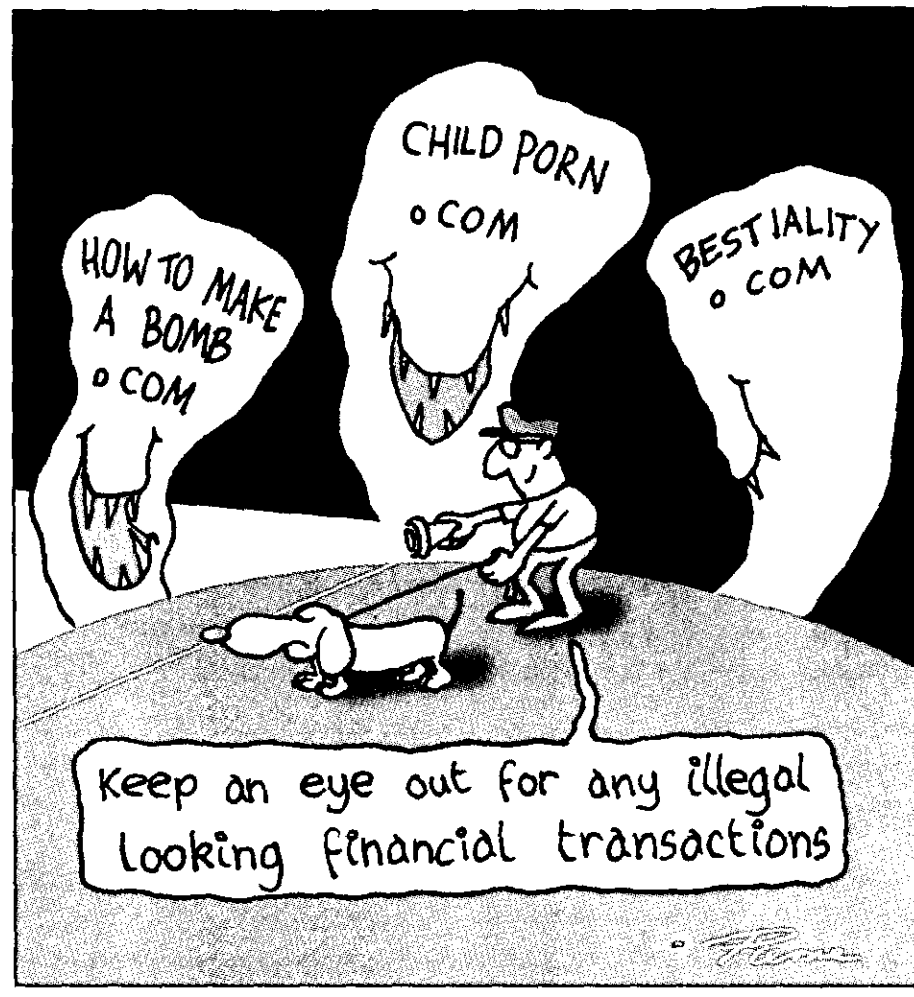
- Under the ASIO Act an ASIO officer accessing data stored in a computer under a computer access warrant will not commit an offence.

- Under the ESOS Act a person obtaining unauthorised access to information on a protected computer system receiving and storing information about students could be guilty of an offence.

- Under the TI Act a warrant can be obtained for the investigation of the proposed computer offences.

INVESTIGATION POWERS

The Bill also extends the criminal investigation powers in the Crimes Act and Customs Act for searching, seizing and copying electronically stored data. Law enforcement agencies are given further powers to detect and investigate crime involving computers. Under the existing law, investigators cannot receive assistance when accessing encrypted information from someone with knowledge of a relevant computer system.



This has left law enforcement agencies at a major disadvantage because large amounts of data are commonly stored on computer drives and disks which are protected.

Under the proposed amendments, a search warrant will allow law enforcement officers to search beyond computers located on search premises, to include material accessible from those computers but located elsewhere. This is particularly relevant because most businesses have networks to other computers and central storage computers.

Computer equipment and disks can also be examined offsite when this is significantly more practicable. This change acknowledges that large amounts of time are often required to circumvent today's complex security measures.

Officers will also be able to copy all data held on a computer hard drive or data storage device where some of the data is evidential material or if there are reasonable grounds to suspect this.

Finally, a magistrate may order a person with knowledge of a computer system to provide information or assistance so that an officer can access, copy or print data. Only necessary and reasonable assistance is required. Using such "insider knowledge" could be a major breakthrough in attempts to access encrypted information. This power is also contained in the draft Council of Europe Convention of Cybercrime.

Niranjan Arasaratnam is a Partner and Maree Flynn is a Research Assistant at the Sydney Office of Allens Arthur Robinson.

Cybersquatters and the Domain Name Game

Tracey Harrip, Lorien Beazley and Dominic van der Toorn urge trademark owners to act swiftly to prevent cybersquatters registering protected trademarks as domain names.

The introduction of the new .info and .biz top level domains means trademark owners need to act quickly to prevent cybersquatters from registering protected trademarks as domain names.

The Internet Corporation for Assigned Names and Numbers (**ICANN**) has finalised arrangements for two new additions to the internet domain name system. Since 1984 the only generic Top Level Domains (**TLD**) have been .com, .org and .net. General applications for the new top TLD's, .info and .biz, will be accepted within the next few months but, as discussed below, trademark owners have priority rights.

The new additions are likely to rival the existing TLD's in popularity and provide some much needed domain name space. A TLD identifies the most general part of the domain name in an Internet address. A TLD is either a generic top-level domain (**gTLD**) such as "com" for "commercial," or a country code top-level domain (**ccTLD**), such as "au" for Australia. As with the existing generic TLD's, both .info and .biz have global application. The .info domain is available to anyone whereas the .biz domain is restricted to business or commercial use.

ICANN has reached agreement with two organisations which will act as registrars of the new TLDs:

- NeuLevel (a joint venture between NeuStar, a North American company, and the Australian based Melbourne IT) will oversee the .biz registration; and
- Afilias (a consortium of 18 ICANN accredited registrars from around the world) will operate the registry for the .info TLD.

Five other new generic TLD's are also to be added, namely .name, .pro, .aero, .coop and .museum. Arrangements have not been finalised for registration of domain names under these more restricted TLD's.

The following is a summary of the application process and details of the special procedures trademark owners should utilise to protect their interests in particular domain names.

THE .BIZ REGISTRATION PROCESS

The first stage in the process of registering .biz domain names is the *Trademark Claim Period*. It began on 21 May 2001 and runs until 6 August 2001. During this time a trademark owner can submit a "trademark claim" (not an application for registration) to NeuLevel. The claim specifies the .biz domain names the trademark owner has an interest or "claim" in. Trademark claims can only be lodged during this period.

Unlike the .info registration process, submitting a trademark claim:

- is not an application for registration of that domain name; and
- does not guarantee the trademark owner will receive that domain name.

The claim simply notifies NeuLevel of the trademark owner's interest. NeuLevel keeps a record of the trademark claims. If an application is received that is identical to a trademark claim, NeuLevel puts the applicant on notice that there is a trademark claim over the relevant "claimed" domain name. The applicant must then inform NeuLevel whether it intends to proceed with the request for the "claimed" domain name. If the applicant decides not to respond to the notification, the application for the "claimed" domain will not be processed during the next stage. If the applicant proceeds with the request and is actually awarded the domain name, the trademark owner can seek to protect its rights using the STOP procedures discussed below.

The next stage is the *Domain Name Application Stage* which runs from 25 June 2001 to 25 September 2001. During this time applications for actual registration of a domain name (rather than a claim) are submitted. All trademark owners who lodge trademark claims should ensure an application for registration of the domain name is also lodged.

Between 26 – 30 September, 2001 is the *Name Selection Stage*. NeuLevel will process all .biz applications using a randomisation algorithm (a computerised lottery) into a single batch. The domain names will be awarded to applicants in the order that they appear in the randomised batch.

The random nature of the selection process could have important implications for the owners of major trade marks. The owner of a well known trademark registered in several countries could easily miss out on its requested domain name if the same trademark registered in another country is randomly selected first.

If, after the Name Selection period, a "claimed" domain is awarded to an applicant other than the trademark owner, NeuLevel:

- informs the trade mark owner who filed the claim; and
- "locks" the claimed domain for 30 days.

The trademark owner has 30 days to initiate proceedings to gain registration rights to the "claimed" domain name. One option is to use the Start-Up Trademark Opposition Policy (**STOP**) to resolve disputes.[1] Grounds for complaints based on STOP are that:

- the domain name is identical to a trademark in which the complainant has rights;
- the applicant is considered as having no rights or legitimate interests in respect of the domain name that is the subject of the complaint; and
- the domain name is considered as having been registered or used in bad faith.

Once a complaint is made under STOP the domain name is locked until proceedings are resolved.

The .biz registry will go live on 1 October 2001. After this time, applications will be processed on a "first come, first served" basis.

THE .INFO REGISTRATION PROCESS

On or about 20 June 2001[2] the rollout for registration of .info domain names will begin.

The first stage in the rollout process is the 30 day *Sunrise Period*. This initial window is designed to allow owners of trademarks to actually register a domain name in identical terms to their trademarks (rather than simply lay a "claim" to the name).

Only owners of valid, enforceable trademarks registered in any country and issued prior to 2 October 2000 are permitted to register a domain name in this Sunrise Period. In addition to the other information required to be lodged by all applicants for domain names, trademark owners must submit to Afilias:

- the characters (letters, symbols and logos) composing the trademark;
- the date the registration was issued;
- the country of registration and;
- the registration number of the trademark.

Registrations of domain names under the Sunrise Period are for a term of between 5 and 10 years. Once registered, the domain names cannot be transferred for 180 days. There are exceptions, for example, if a transfer is made as a result of a successful challenge, or a decision in UDRP (**Uniform Dispute Resolution Policy**) administrative proceedings or in compliance with an order of a court of competent jurisdiction.

Registrations during the Sunrise Period are not processed on a first come first served basis. Rather, applications will be randomly processed over 5 rounds. At the end of each round the domain names submitted will be randomised by a computer and processed for registration. If, during the Sunrise Period, two competing trademark owners submit a registration request for the same domain name, the first request to be selected at random will be awarded the specified domain name.

Parties can challenge a Sunrise Period registration under a dispute process exclusively provided by WIPO (**World Intellectual Property Organisation**). The grounds for challenge are:

- a registrant does not have a valid and enforceable trademark;
- the valid and enforceable trade mark does not have national effect (in the jurisdiction of registration);
- the domain name requested is not identical to the trademark; or
- the trademark registration did not issue prior to 2 October 2000.

The challenge must be issued within 120 days of the end of the Sunrise Period. Otherwise, complainants must use ICANN's UDRP or a court of competent jurisdiction.

Two weeks after the Sunrise Period ends, the *Start-Up Period* begins. In this period the general public (including those trade mark owners who did not apply in the Sunrise Period) may apply for .info domain names. Again, the registrations are not processed on a first come first served basis but over several randomised rounds. If a dispute arises during this period, parties are directed towards the UDRP or alternatively to an appropriate court.

Future TLD's that will free up domain name space for the majority of e-commerce on the Net:

- **sex**
- **smut**
- **porn**
- **seedy**
- **poontang**
- **grubbypreoccupations**

Pierre

The *Post Start Up Period* begins 2 days after the close of the Start-Up Period. This is a period of general registration where applications are processed on a "first come, first served" basis.

Registrations after the Sunrise Period are for a period of at least 2 years and there are no restrictions on transfer of the domain names. Disputes during this period are referred to the UDRP or the relevant courts.

Domain names registered during the Sunrise Period will become active 7 days after the beginning of the Start-Up Period. Domain names registered during the other periods can be used within 5 minutes of registration.

CONCLUSION

Trademark owners who wish to apply for .biz and .info domain names in terms of their trademarks need to act quickly to protect their rights.

1 Claimants can elect to use the specified dispute providers or can proceed through ICANNs UDRP (Uniform Dispute Resolution Policy) through litigation. However, STOP proceedings are said to be more time sensitive and less costly than the other alternatives.

2 The exact dates for the .info registration process are still to be confirmed. The dates seen here are estimates only.

Tracey Harrip is a Partner, Lorien Beazley is a Senior Associate and Dominic van der Toorn is an Articled Clerk in the Brisbane office of Allens Arthur Robinson.

The Interactive Gambling Act 2001 – Is It Needed, Will It Work?

Lisa Vanderwal revisits her earlier article on this contentious Act in light of recent Federal Government concessions regarding interactive gambling.

In a previous edition[1] we commented on the essential provisions of what was then the *Interactive Gambling (Moratorium) Bill 2000*, and some of the issues surrounding the Senate's initial rejection of what has now become the *Interactive Gambling (Moratorium) Act 2000*. This article looks briefly at the lead-up to the *Interactive Gambling Bill 2001*, the legislation following on from the *Interactive Gambling (Moratorium) Act 2000*, and outlines some of the controversy surrounding this Bill.

The proposed ban of interactive gambling has been the subject of considerable public debate over the past couple of years. In 1996 State and Territory Gaming Ministers agreed to develop a model code for interactive gambling that called for a strict licensing regime. In the following years, little action was taken with only the Northern Territory, Queensland and the ACT passing legislation[2]. In January 2000 the Commonwealth Government, appearing to lose patience with their inability to reach agreement and develop a code, foreshadowed the likelihood of banning interactive gambling altogether.

On 17 August 2000 the Government introduced the *Interactive Gambling (Moratorium) Bill 2000* which proposed imposing a 12 month moratorium on the development of the interactive gambling industry in Australia, beginning retrospectively on 19 May 2000 and ceasing at midnight on 18 May 2001. On 9 October 2000 the Bill was defeated in the Senate when the Government failed to obtain a majority by tied vote of 33:33.

On 8 November 2000 the Australian Casino Association released an updated and improved code of practice for on-line gambling, which was developed in conjunction with State and Territory regulators[3]. The code of practice aimed to achieve the highest levels of player protection standards and ensure the best and safest gambling environment. Amongst other measures, the code of practice ensured that players had to be identified with a PIN or password, minors were prevented from playing, security and privacy of players was to be strictly protected, gambling on credit was banned and information on gambling help lines and counselling services would be readily available. Despite the code of practice, and as a result of intense political manoeuvring, the *Interactive Gambling (Moratorium) Bill* was passed by both Houses in December 2000.

While the *Interactive Gambling (Moratorium) Act 2000* expired on 18 May 2001, the Government introduced the *Interactive Gambling Bill 2001* (**Bill**) which essentially made it an offence for an interactive gambling service to be provided to a person physically located in Australia, and established a complaints regime under which Australians could make complaints about interactive gambling services. The proposed legislation created as much controversy as the *Interactive Gambling (Moratorium) Act 2000* and invoked almost as much last minute manoeuvring in the Senate. The Bill was agreed by the Senate on 28 June 2001 and was approved by the Governor General on 11 July 2001. The purpose of this paper is to provide an overview of the Act and to examine some of the debate that has arisen.

INTERACTIVE GAMBLING ACT 2001

The stated policy of the Act is to limit and discourage Australians from gambling on-line, rather than to stop it altogether[4]. To this end, there are essentially three new offences created under the Act, along with a complaints process. The three new offences are providing an interactive gambling service to Australians, providing an Australian-based interactive gambling service to designated overseas countries, and publishing interactive gambling advertisements.

Providing an interactive gambling service to Australians

Section 15(1) of the Act makes it a criminal offence to intentionally provide to people who are physically present in Australia[5] interactive:

> *services for placing, making, receiving or acceptance of bets or wagers, or whose sole or dominant purpose is to facilitate the placement of bets;*
>
> *games of chance or mixed chance and skill played for anything of value where the player pays, directly or indirectly, to enter the game; or*
>
> *gambling services not covered by the above paragraphs*[6].

The above services must be provided in the course of a venture or concern in trade or commerce, whether or not conducted on a regular, repetitive or continuous basis[7]. The service must also be provided using:

- an internet carriage service;
- a datacasting service;
- a broadcasting service; or
- any other content or listed carriage service:[8]

Providing an Australian-based interactive gambling service to designated overseas countries

This second offence, contained in section 15A of the Act, was included as a last minute amendment in response to criticisms of the Act, which claimed it was being hypocritical. In particular, the Greens Senator Brown has commented that "we have an ethical consideration in this age of globalisation to people outside our borders as well as those inside. Welcoming the establishment of these facilities in our country through a regulatory system so that they can sell their wares externally while prohibiting that inside the country is hypocritical"[9]. The Australian Institute for Gambling Research echoed this point, claiming that "it is morally indefensible to imply that Australians should be protected from this form of gambling yet Australian operators can profit from the harm created in other countries"[10].

Section 15A of the Bill now provides that it is a criminal offence to intentionally provide interactive:

- services for placing, making, receiving or acceptance of bets or wagers, or whose sole or dominant purpose is to facilitate the placement of bets; lotteries or the supply of lottery tickets;
- games of chance or mixed chance and skill played for anything of value where the player pays, directly or indirectly, to enter the game; or
- gambling services not covered by the above paragraphs[11]

where those interactive services are provided:

- in the course of carrying on a business in Australia;
- where the central management and control of the service is in Australia;
- through an agent in Australia; or
- to customers where the relevant internet content is hosted in Australia[12].

In addition, in order for this to be an offence the service must be provided to customers who are physically present in a country declared by the Minister as being a "designated country"[13]. The Minister will only designate countries where those countries have legislation similar to the Act, and that country's government has requested the Minister to make the Declaration[14].

A fine of $1.1 million per day will apply to bodies corporate, and $220,000 per day to natural persons for a breach of the above provisions. However, it is not an offence if the provider of the service did not know, and could not have determined with reasonable diligence, that any of the customers of the interactive gambling service were physically present in Australia[15] or a designated country[16]. In determining whether a person could have known or ascertained that there was an Australian or designated country customer link, the following are to be taken into account:

- were prospective customers told that Australian law prohibits the provision of the service to customers physically present in Australia or a designated country;
- were customers required to enter into contracts that were subject to an express condition that the customer was not to use the service if he or she was physically present in Australia or a designated country;
- were customers required to provide personal details which would suggest that the customer was not physically present in either Australia or a designated country; or
- whether the person providing the services has network data that indicates the customer was physically located outside Australia or a designated country when the relevant account was opened and throughout the period the service is provided to the customer[17].

While the above sections appear to be quite broad, there are a number of specified excluded services under the Act. These include telephone betting, betting on horse races, harness races, greyhound races or other sporting events[18], provided such bets are not made once the event has begun[19]. In addition, the Act will not cover services provided in a public place, for example a shop, casino, bar or club[20]. There are also some exclusions in relation to broadcast and datacast services, and of course the Minister may determine that certain services are exempt services for the purposes of the Act[21].

Publication of interactive gambling advertisements

A new Part 7A, modelled on the *Tobacco Advertising Prohibition Act 1992 (Cth)*, has also been inserted into the Act as a result of the Senate amendments, under which a person is guilty of an offence if that person publishes an interactive gambling service advertisement in Australia[22]. This includes any promotion in writing, still or moving pictures, signs, symbols, visual images, audible messages or any combination of the above that publicises or promotes a particular interactive gambling service, interactive gambling services in general, the whole or part of a trademark in respect of an interactive gambling service, the domain name or URL that relates to an interactive

gambling service, or any words that are closely associated with an interactive gambling service[23].

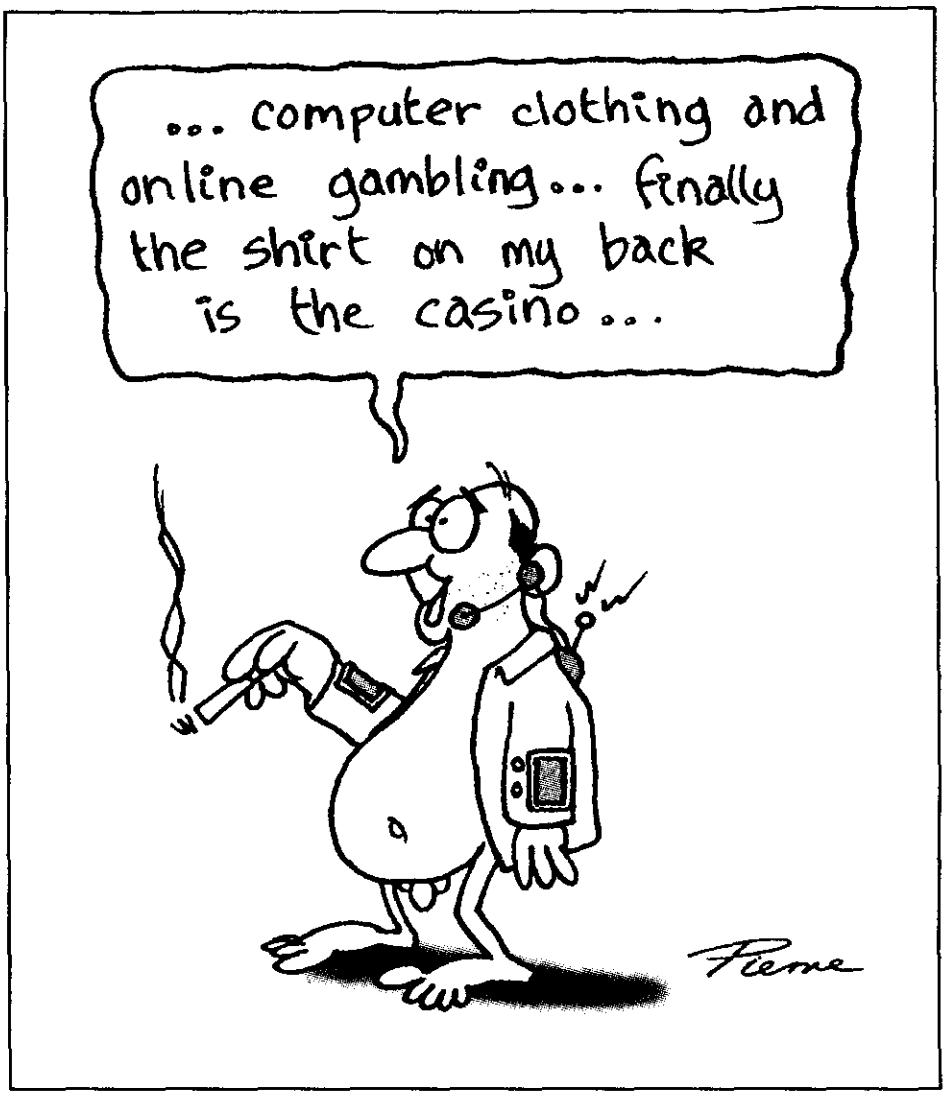
There are certain exceptions to this prohibition, which include advertising in periodicals distributed outside Australia[24] and advertising in relation to Australian sporting and cultural events of international significance[25]. Penalties of $13,200 apply to individuals and $66,000 to bodies corporate for contravention of these provisions. There are also similar prohibitions on the broadcasting or datacasting of interacting gambling service advertisements in Australia[26].

Complaints process

The Act provides that an Australian resident, a body corporate that carries on activities in Australia, or the Commonwealth, a State or Territory[27] may make a complaint to the Australian Broadcasting Authority (**ABA**) if they believe Australians can access a prohibited gambling service[28]. If the complaint relates to internet content hosted in Australia, the ABA may refer the matter to the police for investigation[29].

If the complaint relates to internet content hosted outside Australia, the ABA may issue a standard access prevention notice to the relevant internet service provider (**ISP**) directing the relevant ISP to take all reasonable steps to prevent Australians from accessing the content[30]. The ISP must comply with the notice by 6pm on the next business day after the notice was given to that ISP[31].

The Act does not specify any particular prevention mechanisms so as not to preclude any potential technological advances. Nonetheless, an ISP is not necessarily required to prevent Australians from accessing the content if it is not technically or commercially feasible to do so[32]. In addition, an ISP will not be required to comply with the standard access prevention notice in relation to a particular Australian user if access by that user is subject to a recognised alternative access prevention arrangement eg regularly updated content filtering software[33]. Any ISP who is obliged to comply with a standard access prevention notice and does not do so is guilty of an offence under the Act, punishable by a penalty of $5,500.



The Act also anticipates that an industry code and industry standard will be developed, and gives the ABA power to require an industry body to develop such codes or standards if the industry does not do so voluntarily[34]. Where any codes or standards exist, Australian residents, bodies corporate conducting business in Australia and the Commonwealth, a State or Territory may make complaints to the ABA in relation to breaches of those codes or standards, and any breaches will be dealt with in accordance with those codes or standards[35].

CRITICISMS

Criticism of the Act has been vociferous and from a wide range of sources. The Internet Industry Association (**IIA**) has labelled the Act as "a backward step for the safe internet usage in Australia that will not achieve any defensible public policy outcomes at all"[36]. It has said that Australia is flying in the face of world trends to introduce tough regulation of the industry, but not ban it all together, on the reasoning that strict local controls will better protect their citizens.

Indeed, the IIA claims that the approach that the Australian States and Territories have taken is widely regarded by overseas players as being without question the world's best practice[37], so much so that countries such as the UK and South Africa are likely to adopt standards similar to that proposed by the Australian Casino Association as outlined above. In addition, the IIA claims that by effectively banning the development of gambling-related technology such as encryption and security technologies which could have application in mainstream commerce on the internet will be lost as companies relocate from Australia, taking their skill base and intellectual property with them.

The Australian Labor Party was also critical of the Act, with Labor Senators

Mark Bishop and Kate Lundy pointing out perceived fundamental flaws in the policy approach behind the Act and finding fault with the implementation of the policy[38]. In particular, the Senators considered that the Act potentially exacerbates Australia's gambling problem by effectively removing a regulated service with in-built safeguards while still allowing access to unregulated and unlicensed off-shore sites (until such time as a complaint is made in respect of that particular service).

The Senators also noted that while investigations of potential offences were to be referred mainly to the Australian Federal Police (**AFP**) there is to be no additional funding, and the AFP is expected to fulfil this additional role from existing resources. The Labor senators consider that the AFP will be unable to effectively fulfil its role under the Act, thereby compromising implementation of the Act[39]. While the Government has allocated $10 million over 4 years for research and an education program into social problems associated with gambling[40], it will still not address the enforcement issues raised above.

The IIA, ALP and other opposers of the Act have also pointed out what appear to be glaring inconsistencies. While poker machines have created increasingly large problems as a result of their expansion, there is no complimentary legislation that could address this issue. In addition, while the Act attempts to prohibit most gambling services provided over the internet, it expressly excludes telephone betting. It is difficult to see the difference between placing a bet over the telephone, and placing a bet over the internet. This inconsistency is exacerbated by the exclusion of betting on horse, harness and greyhound races, and bets placed in public places. While this approach is consistent with the aim of the Act as set out earlier in this article, whether this artificial distinction is actually workable remains to be seen.

The removal of the requirement for an interactive gambling operator to have an Australian link may also create some difficulties for the Government. The removal was intended to be a strong deterrent to foreign operators soliciting Australian customers[41], but raises jurisdictional as well as enforcement issues – even if a country in which the interactive gambling organisation was operating, or in which the content is hosted, recognised Australia's right to enforce the legislation, the question remains as to how, or how effectively, Australia would recover the hefty fines under the Act.

CONCLUSION

The Government appears at first glance to be bravely attempting to address community concerns in relation to a number of on-line issues. While some of its initiatives which are clearly responding to community concern, such as the offensive internet content amendments set out in the *Broadcasting Services Amendment (Online Services) Act 1999*, appear to have been successful, others such as the *Electronic Transactions Act 1999* do not appear to have had much of an impact at all, despite the fanfare preceding that legislation.

However, the Government's legislative efforts tend to fail where it is responding to what appears to be blatant political and economic pressure and disguising it as a response to community concern.

This certainly does not bode well for this Act, which also appears to be a response to a political agenda, and which may not have been as well thought out as the Government would like to claim. Whether the Act will actually work, or will be the subject of a very public failure à la datacasting, remains to be seen. Still, like it or not, workable or not, Australia now leads the world in enacting legislation prohibiting on-line gambling.

1 Volume 19, No 3, 2000.

2 The Gaming Control Amendment Act 1998 (NT); the Interactive Gambling (Player Protection) Act (Qld); the Interactive Gambling Act 1998 (ACT); the Interactive Gaming (Player Protection) Bill 1999 (Vic).

3 See the media releases at aca.asn.au

4 Report of the Senate Environment, Communications, Information Technology and the Arts Legislation Committee on the Interactive Gambling Bill 2000, May 2001, page 33.

5 Section 8 of the Act

6 Section 4 of the Act, definition of "gambling service".

7 Section 4 of the Act, definition of "business".

8 Section 5(1)(b) of the Act.

9 23 May 2001, Senate Hansard: Interactive Gambling Bill 2001 - Report of Environment, Communications, Information Technology and the Arts Legislation Committee, page 05/23841

10 Report of the Senate Environment, Communications, Information Technology and the Arts Legislation Committee on the Interactive Gambling Bill 2000, May 2001, page 36.

11 Section 4 of the Act, definition of "gambling service".

12 Section 15A(7) of the Act.

13 Section 9B of the Act.

14 Section 9A of the Act.

15 Section 15(3) of the Act.

16 Section 15A(3) of the Act

17 Sections 15(4) and 15A(4) of the Act.

18 Section 8A(1) of the Act.

19 Section 8A(2) of the Act.

20 Section 8B of the Act.

21 Section 10 of the Act.

22 Section 61EA(1) of the Act.

23 Section 61BA(1) of the Act.

24 Section 61EB of the Act.

25 Section 61EC of the Act.

26 Section 61DA of the Act.

27 Section 19 of the Act.

28 Section 16 of the Act.

29 Section 20 of the Act.

30 Section 24(1) of the Act.

31 Section 28 of the Act.

32 Section 24(2) of the Act.

33 Section 24(4) of the Act.

34 Part 4 of the Act.

35 Section 17 of the Act.

36 Internet Industry Association News Release, 29 March 2001.

37 Report of the Senate Environment, Communications, Information Technology and the Arts Legislation Committee on the Interactive Gambling Bill 2000, May 2001, page 54.

38 Labor's Response to Interactive Gambling Bill, 23 May 2001.

39 23 May 2001, Senate Hansard: Interactive Gambling Bill 2001 - Report of Environment, Communications, Information Technology and the Arts Legislation Committee, page 05/23839

40 Media release, Senators Meg Lees, John Woodley and Lyn Allison, 28 June 2001.

41 Supplementary Explanatory Memorandum to the Interactive Gambling Bill 2001, Amendment (15).

Lisa Vanderwal is an Associate at the Sydney office of PricewaterhouseCoopers Legal

Pandora's Box Opened: Inquiry Into the Adequacy of Radio Services in Regional and Rural Australia

Carolyn Lidgerwood examines the activities of a bi-partisan parliamentary committee which has provided a lively forum for debate about the state and direction of the radio industry in regional and rural Australia.

In September 2000, the House of Representatives Committee on Communications, Transport and the Arts (**Committee**) accepted terms of reference for a broad ranging inquiry into the regional and rural radio industry (**Regional Radio Inquiry**).

Since that time, the Committee has been gathering evidence for the purpose of reporting on "the adequacy of radio services in regional and rural Australia and the extent to which there is a need for the Government to take action in relation to the quantity and quality of radio services in regional and rural Australia"[1]. The terms of reference direct the Committee to have particular regard to matters including:

- the social benefits and influence on the general public of radio broadcasting in non-metropolitan Australia in comparison to other media sectors;
- future trends in radio broadcasting in non-metropolitan Australia;
- the effect on individuals, families and small business in non-metropolitan Australia of networking of radio programming, particularly in relation to local news services, sport, community service announcements and other forms of local content; and
- the potential for new technologies such as digital radio to provide enhanced and more localised radio services in metropolitan, regional and rural areas.

Irrespective of the circumstances which led to the commencement of the Regional Radio Inquiry, it is clear that the Inquiry has generated a very large amount of interest among audiences and broadcasters alike.

The website of the Committee indicates that 275 written submissions have been received[2], and that public hearings have been heard across the country. Representatives of all sectors of the radio industry – national broadcasters, commercial broadcasters, community broadcasters and open narrowcasters - have given evidence to the Committee. The Committee has also heard from federal and state government departments and agencies (including the ABA), shire councils, infrastructure providers, aspirant broadcasters, peak industry associations, sporting associations and private individuals.

As the Chair of the Committee noted when introducing one of the public hearings, this

> *is an indication of the importance of radio to regional Australia, of the concern in the community about the current policies and practices revolving around radio networks and also, no doubt, of the concerns that some have about possible changes to those policies and practices*[3].

Submissions have focused on how the provision of radio services in non-metropolitan Australia, particularly by commercial radio broadcasters, has changed over the last decade. As the Federation of Australian Radio Broadcasters Limited (**FARB**) outlined in its first appearance before the Committee, "regional radio today is the product of a number of evolutionary factors. In a nutshell, these can be identified as the *Broadcasting Services Act* (**BSA**), prevailing market conditions and the impact of technology"[4].

As outlined in the terms of reference, the Committee is required to report on matters including "the extent to which there is a need for the Government to take action in relation to the quantity and quality of radio services in regional and rural Australia". In that context, some of the interesting issues raised by and before the Committee are summarised below[5].

SHOULD COVERAGE OF LOCAL ISSUES BY COMMERCIAL RADIO BE REGULATED?

The networking, syndication and automation of programming by regional radio broadcasters, particularly commercial radio broadcasters, has been discussed widely in the evidence presented to the Committee.

The use of new technologies, consolidation of ownership and commercial strategies in response to increased competition for advertising revenue has led to changes in how programming is provided in many non-metropolitan licence areas, and as some submissions have argued, the content of such programming[6]. The extent to which matters of local significance are covered by non-metropolitan radio, particularly commercial radio, is an issue which has dominated the evidence provided during the Committee's hearings. Certainly, the evidence presented to the Committee indicates that different approaches to the provision of local content are adopted throughout the regional and rural commercial radio industry[7].

Networking and localism

In its written submission, FARB argued that networking by commercial radio does

not compromise "localism", as networked and local radio programming is "interwoven to produce a comprehensive service"[8].

The Australian Broadcasting Association's (**ABA**) written submission noted that greater networking of regional radio services is "inevitable and not necessarily undesirable", but it expressed concern about whether the gains of greater networking have outweighed the "costs" – especially where networked programming has replaced locally produced material[9].

An important issue which is expected to be considered in the report by the Committee (**Committee's Report**) is how coverage of matters of local significance on commercial radio can be ensured in a competitive environment where networking, syndication or automation may be considered by some broadcasters to be commercial imperatives. Also, it will be interesting to consider what weight the Committee's Report places on the coverage of matters of local significance by non-commercial radio broadcasters in regional and rural Australia.

As the ABA has explained, commercial licensees are not required individually to ensure coverage of matters of local significance[10]. The relevant condition of licence in Schedule 2 of the BSA requires licensees to provide a service that, when considered together with other broadcasting services available in the licence area of the licence (including another service operated by the licensee), contributes to the provision of an adequate and comprehensive range of broadcasting services in that licence area[11]. While one of the objects of the BSA is to encourage "an appropriate coverage of matters of local significance"[12], this is not a condition of licence and is not currently a feature of codes of practice approved by the ABA under the BSA.

Suggested changes

Some commercial radio broadcasters have expressed a willingness to comply with local content conditions or standards if they were to be imposed. One suggestion put to the Committee was that local content standards should apply in the context of a moratorium on the issue of new licences in regional areas, and the abolition of the "two to a market rule"[13]. Another suggestion was that local content standards should be applied in markets where no additional competition had been introduced, but not in other markets, as the licensees in markets facing increased competition may struggle to meet such standards[14]. Unsuprisingly, the introduction of regulation in the form of local content conditions or standards (rather than self regulation) has not been advocated in FARB's submissions.

The ABA's written submission suggested that the current legislative framework (utilising industry codes, standards and conditions of licence) may be adequate to regulate the coverage of matters of local significance[15]. However, in its appearance before the Committee, the ABA also suggested that introduction of "tradeable credits" could be considered. This could involve each (presumably commercial and community) licensee being responsible for the provision of a certain number of minutes programming each day on local or community issues, but being able to contract with another station in the area to deliver that local programming on their behalf. As the Deputy Chairperson of the ABA explained:

> *Say you mandate 30 minutes a day, it may mean that you get one hour a day on a station rather than two 30 minute segments running in opposition to each other on two different stations. It may mean that they ... contract with the community radio station to produce and distribute it on their behalf. It lets the market forces as to who is the most efficient at producing that local content do so in a way that may enhance the actual spread of time that is devoted to community news in an area ...*[16]

The ABA acknowledged that it had not yet developed proposals about how this "tradeable credits" system may be implemented, but suggested it be considered by the Committee.

It is worth noting that some of the commercial radio broadcasters who appeared before the Committee were asked for their views about 3 yearly performance reviews, which would examine "the extent stations are connected with their communities and provide a comprehensive service"[17]. Mixed responses were received[18] - with some broadcasters conditionally favouring this approach, and others opposing it.

If the Committee accepts that changes are required to be made, it will be interesting to see whether the Committee's Report recommends changes within the existing legislative framework or whether it recommends that legislative changes be made.

SHOULD THE ABA'S LICENCE AREA PLANNING PROCESS BE CHANGED?

The Committee has heard a range of submissions about the impact of the ABA's licence area planning (**LAP**) process in regional markets. Some incumbent broadcasters have been critical of the issue of third and fourth licences in markets where the viability of such new licences was not established prior to their issue[19]. These are essentially criticisms of the existing legislative framework, rather than the ABA's application of that framework. The ABA's evidence explained how it had implemented the legislative framework by considering the "feasibility", rather than the "viability" of new services.[20]

The LAP process has seen a dramatic increase in the number of licences on issue in regional Australia. The Committee has noted the fact that this is to be contrasted with metropolitan areas. FARB's evidence was that in the past 9 years, commercial radio services to regional Australia have increased from 109 to 202, but these stations share only 35% of the radio industry's $680 million revenue[21]. The decline of regional radio's share of advertising revenue as a percentage of total advertising revenue is discussed in detail in a recent ABA report entitled *The Commercial Radio Industry 1978-79 to 1997-98*[22].

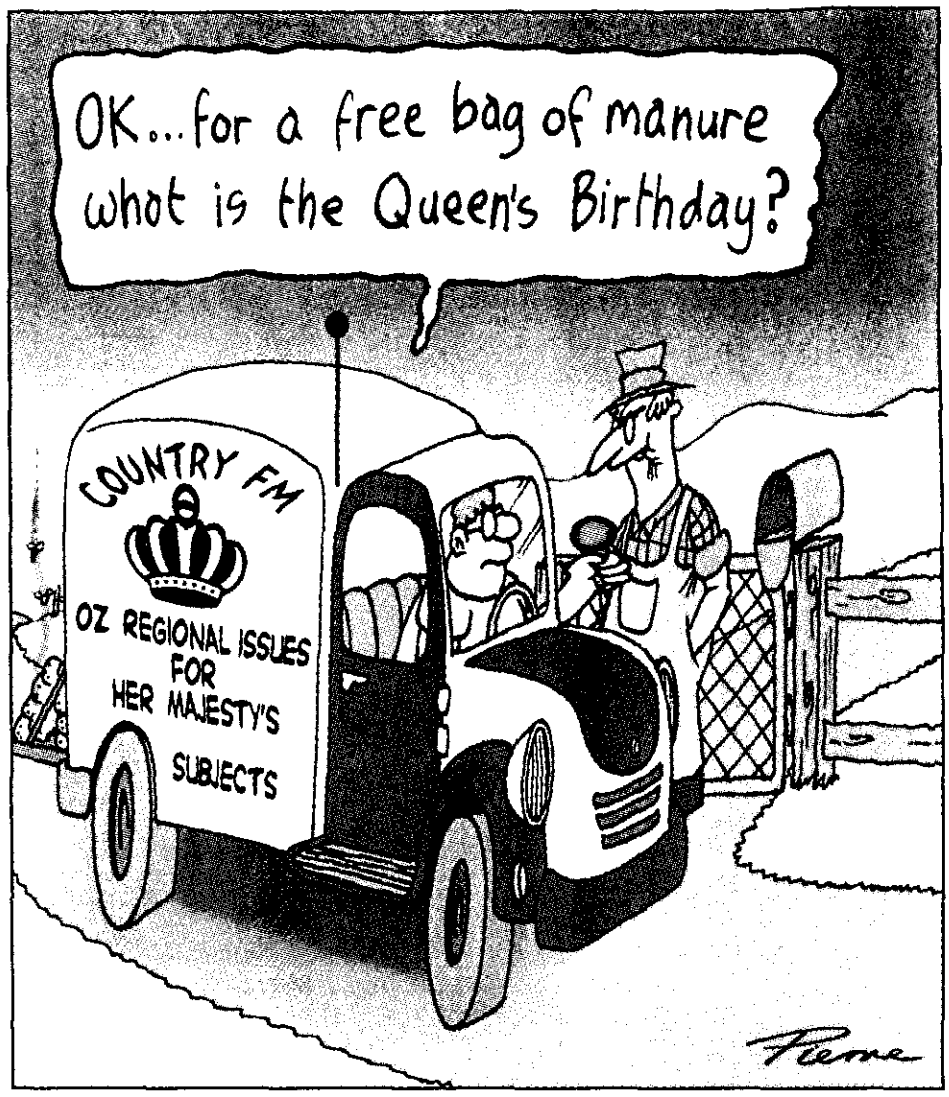
Evidence has been presented to the Committee that in markets where additional competition has been introduced, broadcasters are under pressure to balance economic viability

with the pressure of meeting community expectations about local coverage. FARB noted that "while these economics remain, it makes it almost impossible for regional commercial stations to sustain a totally local broadcasting operation in the old-fashioned way – that is, announcers sitting in studios whenever the station is on air"[23]. A theme of much of the evidence presented to the Committee has been that the issue of new licences following the LAP process has been directly linked to a decrease in localism.

One submission to the Committee was that if the LAP process continues, this will inevitably lead to further increases in networking and a further loss of localism. That submission argued that there should be a freeze on the issue of new commercial radio licences in regional Australia for the next 10 years – and that in return, incumbent regional broadcasters would be required to comply with minimum local content obligations[24]. FARB agreed that there should be a 10 year moratorium on the issue of new licences, but took a different view about when the moratorium should commence[25]. It is worth noting that in recognition of the cost of establishing new services, FARB also proposed that there should be 5 year moratorium on the payment of licence fees for all new services which are rolled out under the LAP process[26].

SHOULD RADIO BROADCASTERS BE SUBJECT TO COMMUNITY SERVICE OBLIGATIONS?

A range of evidence has been presented to the Committee about the relationship between networking and the ability to respond to national disasters. Emergency service organisations such as the Country Fire Authority, and government agencies such as the Bureau of Meteorology have made submissions to the Regional Radio Inquiry relating to their concerns about the impact of networking when emergency messages need to be delivered to particular communities[27]. Each of these organisations responded in the affirmative when asked whether the *Broadcasting Services Act* should be altered to insert community service obligations. It was indicated that this could involve a station having to demonstrate that it could broadcast a weather alert, for example, from its hub.



FARB gave evidence of its recent work with emergency bodies – and clearly favoured a self regulatory approach to the issue of emergency services, rather than a more prescriptive approach. The ABA indicated that it was working with FARB on this issue, and that the ABA's key objectives were to ensure that commercial radio is available to broadcast emergency announcements whenever needed in the regions, and that all broadcasters need to be aware of who to contact in the case of an emergency[28].

The Committee is expected to report in July-August 2001.

1 *Terms of Reference are set out in the Media* Alert issued by the Committee on 8 September 2000, available at http://www.aph.gov.au/house/committee/cta/irmed1.pdf. The Terms of Reference are also included in Official Committee Hansard at http://www.aph.gov.au/hansard/reps/committee/comrep.htm

2 http://www.aph.gov.au/house/committee/cta/irsub.htm

3 Official Committee Hansard, 30 January 2001, at 91.

Hansard is available from http://www.aph.gov.au/hansard/reps/committee/comrep.htm

4 Official Committee Hansard, 8 December 2001, at 18.

5 These are just some of the issues raised in evidence to the Committee. This paper does not address other important issues considered by the Committee, such as the role of national broadcasting in regional areas or digital radio policy, for example.

6 For example, see arguments about the reduction of quality of local radio (as a result of networking) in the Official Committee Hansard, 28 May 2001, at 810 (RG Capital Radio).

7 See, for example, Official Committee Hansard, 28 May 2001 at 774 (Ace Radio Broadcasters).

8 http://www.aph.gov.au/house/committee/cta/irsub.htm

9 http://www.aph.gov.au/house/committee/cta/irsub.htm

10 Official Committee Hansard, 29 May 2001, at 900.

11 Clause 8(2)(a), Schedule 2, BSA.

12 Section 3(g), BSA.

13 Official Committee Hansard, 2 February 2001,

at 337 (RG Capital Radio).

14 Official Committee Hansard, 19 February 2001, at 419 (Sun FM Stereo).

15 http://www.aph.gov.au/house/committee/cta/irsub.htm

16 Official Committee Hansard, 29 May 2001, at 909.

17 Official Committee Hansard, 28 May 2001 at 804.

18 See Official Committee Hansard, 28 May 2001, at 805, 812 and 831 (DMG, RG Capital Radio, Broadcast Operations Group).

19 See, for example, Official Committee Hansard, 12 March 2001 at 501 (Grant Broadcasters).

20 Official Committee Hansard, 29 May 2001, at 896.

21 Official Committee Hansard, 29 May 2001, at 849.

22 The report is available from the ABA website at: http://www.aba.gov.au/what/research/pdf/comrad79_98.pdf

23 Official Committee Hansard, 29 May 2001, at 849.

24 Official Committee Hansard, 28 May 2001, at 811 (RG Capital Radio). Note that the proposal was for the moratorium to exclude licence areas which do not have a FM commercial radio service.

25 Official Committee Hansard, 29 May 2001, at 863.

26 Official Committee Hansard, 29 May 2001, at 850. FARB outlined 9 recommendations during the last day of the Committee's hearings – see at 850-851.

27 Official Committee Hansard, 30 January 2001, at 113.

28 Official Committee Hansard, 29 May 2001, at 889.

The views expressed in this article are those of the author and not necessarily those of the firm or its clients.

Carolyn Lidgerwood is Special Counsel, Broadcasting, at Gilbert & Tobin in Sydney.

ACIF Code Compliance – Measuring Up

Brenton Yates and Liam Buckley examine the ACIF regime for telecommunications industry self regulation.

Self-regulation within the telecommunications industry is an ideal which by now most, if not all, industry participants have turned their attention to in some way or another. A significant portion of that attention has been directed to the activities of the Australian Communications Industry Forum (**ACIF**). ACIF is an industry owned, resourced and operated organisation which was established to implement and manage communications self-regulation within Australia. This article outlines some of the issues arising from, and benefits of complying with, the numerous ACIF Codes of Practice, as well as discussing those issues which stand in the way of a successful transition into industry self-regulation.

BACKGROUND TO THE AUSTRALIAN COMMUNICATIONS INDUSTRY FORUM

Embodied in the policy statement of the *Telecommunications Act 1997* (**Act**), is the fundamental object that:

> *... telecommunications be regulated in a manner that:*
>
> *a) promotes the greatest practicable use of industry self-regulation; and*
>
> *b) does not impose undue financial and administrative burdens on participants in the Australian telecommunications industry;*
>
> *but does not compromise the effectiveness of regulation in achieving the objectives mentioned [elsewhere in the Act].*[1]

ACIF was established in 1997 as the industry body representing sections of the telecommunications industry charged with the implementation and management of communications self-regulation within Australia. ACIF has a Board, Advisory Assembly, Reference panels, Task Specific Working Committees, Issues Specific Facilitation/Co-ordination Groups and a full time Executive. These positions are filled by delegates from carriers, service providers, industry associations and user groups, consumer organisations and individual members.

In accordance with Part 6 of the Act, ACIF's role is to develop and administer technical and operating arrangements that promote both long-term interests of end-users and efficiency and international competitiveness of the Australian communications industry. In fulfilling this role, ACIF oversees the development of codes and standards for the support of competition, the protection of consumers and to facilitate the co-operative resolution of strategic and operational industry issues. The success of this role however can only be guaranteed through widespread industry participation in developing, and compliance with, the codes and standards. ACIF is also responsible for additional publications including Industry Standards, Specifications, Guidelines and various other documents including Industry Statements, Reports, Overviews and Schemes.

Whilst all of the above publications are relevant to various industry participants, the ACIF Codes of Practice are of the most significance given that industry participants may be required and/or directed to comply with their provisions on a mandatory basis.

ACIF CODES OF PRACTICE

Under the Act, ACIF may deal with a wide range of matters through the implementation of Industry Codes and Standards. To date, ACIF has published numerous codes in the following three broad areas:

(i) Consumer Codes – "Rules" for the supplier-customer interface & interactions in a particular area;

(ii) Operations Codes – Primarily multi-lateral operating arrangements – ie

"Rules" for the supplier-supplier interface & interactions in a particular area (with supplier-customer interaction rules also included in some Codes); and

(iii) Network/Technical Codes – "Rules" for end-to-end network performance, the accuracy of call charging and billing systems or other design performance dimension as specified in Regulations.

The only limitation Part 6 of the Act places on ACIF with regards to the content of its Codes and Standards relates to issues of *design* and *performance requirements* of customer equipment, customer cabling, telecommunications networks or telecommunications facilities[2]. Such technical regulation is dealt with in Part 21 of the Act.

When ACIF publishes a Code, industry compliance with that Code is voluntary. In practice however most industry participants recognise the Codes as the establishment of "best practice" benchmarks and comply with them in any case. Nonetheless, mandatory compliance with a Code may be established by other means. Where an industry participant chooses to become a *signatory* to a particular Code, that participant undertakes to comply with that particular Code. Signing up to an ACIF Code takes place on a code by code basis. There are to date only two industry participants who have become signatories to ACIF Codes of Practice.

Mandatory compliance with an ACIF code may also occur once an ACIF code has been registered by the Australian Communications Authority (ACA). Once a code is registered by the ACA, the ACA may issue a direction to an industry participant to comply with a Code if that industry participant is clearly and continuously acting in breach of a particular Code. To date, no such directions have been issued.

CODE REGISTRATION BY THE ACA

All *ACIF Consumer Codes* are to be submitted to the ACA for registration (unless there is a specific reason for not doing so). Registration of *Operations and Network/Technical Codes* are to be assessed on a code by code basis, usually involving an assessment of the benefits of registration versus the cost/ disadvantages. In this regard, other assessment criteria may also include the:

- size of the sector(s) to which the Code applies;
- availability/cost effectiveness of alternative enforcement/compliance mechanisms;
- likely level of voluntary participation in the Code;
- effect on industry participants and the potential magnitude of a breach of the Code;
- degree of difficulty in identifying Code breaches; and
- likelihood of the Code requiring amendment over time.

Despite the above guidelines, ACIF has recently indicated its intention to submit *all* finalised/published Codes to the ACA for registration.

At the time of writing there are thirteen registered ACIF Codes of Practice which may at any time be enforced upon an industry participant at the direction of the ACA.

- ACIF C519 – End-to-End Network Performance
- ACIF C525 – Handling of Life Threatening and Unwelcome Calls
- ACIF C531 – Commercial Churn
- ACIF C515 – Pre-selection - Single Basket/Multi Service Deliverer
- ACIF C523 – Protection of Personal Information of Customers of Telecommunications Providers
- ACIF C522 – Calling Number Display
- ACIF C547 – Complaint Handling
- ACIF C521 – Customer Information on Prices, Terms and Conditions
- ACIF C542 - Billing
- ACIF C541 – Credit Management
- ACIF C518 –Call Charging and Billing Accuracy
- ACIF C546 – Customer Transfer
- ACIF C570 – Mobile Number Portability

There are a further six Published Codes which, whilst they have not been registered by the ACA, may at any time be registered and ultimately enforced upon a relevant industry participant:

- ACIF C504 – Customer Barring
- ACIF C513 – Customer and Network Fault Management
- ACIF C524 – External Communication Cable Networks
- ACIF C537 - Provision of Assistance to National Security, Enforcement and Government Agencies Industry Code
- ACIF C540 – Local Number Portability
- ACIF C555 – Integrated Public Number Database (IPND) Data

In keeping with the principle of self-regulation, Part 6 of the Act authorises the ACA to request industry participants and regulators to develop and register industry codes where the ACA may feel a particular issue remains unguarded. Where an industry code has been registered for more than 180 days and has failed to achieve the desired outcome or result, the ACA may develop and issue an *Industry Standard* which deals with the issue. Compliance with Industry Standards is mandatory for all industry participants.

THE BENEFITS OF BEING ACIF COMPLIANT

Proponents of the ACIF regime identify a number of benefits for a company committing itself to complying with the ACIF regime, specifically the ACIF Codes. These benefits include that industry participants who implement early mechanisms of compliance with the ACIF Codes will be in a better market position than participants who do not and may be faced at any time with a 'forced compliance' direction from the ACA which could be both inconvenient or

costly. Such 'forced compliance' may also include having increased disclosure to the ACA, being subject to regular reviews of activities and making undertakings regarding compliance to the ACA.

In addition, April 1998 saw ACIF become fully accredited as an *Australian Standards Development Organisation*, an accreditation awarded by the Standards Accreditation Board (**SAB**) which is an independent body reporting to the Council of Standards Australia. Participants who can demonstrate to their customers & clients that their business plan complies with ACIF Codes will also be able to make use of the SAB accreditation.

ACIF signatories are also able to utilise the ACIF code administration and compliance mechanisms, thereby leaving the involvement of government regulators (which can be costly and inconvenient) as an instrument of last resort.

PERCEIVED PROBLEMS WITH THE ACIF REGIME

Despite the obvious benefits, there have been criticisms of the ACIF regime and its overall effect on the industry, particularly from some smaller industry players. One of these criticisms is that the Working Committees responsible for the development of ACIF codes are usually comprised of representatives of major carriers and governmental authorities, the smaller players often not having the resources to commit to such an enterprise. As a result, it has been claimed that this style of industry self-regulation is merely 'codifying' the existing practices of these larger carriers and governmental authorities which may not lead to an easy adoption by the smaller carrier and service provider population.

This "big-end of the market" perspective is further reflected in the associated costs which may be incurred as a result of compliance. The cost issue in particular may have relevance for many, if not all, small industry participants.

As more and more codes and standards are developed, there may be a need to implement proper safeguards so as to ensure consistency with the Act, and its myriad of associated Acts, Regulations, Codes, Determinations and Standards. Given the propensity for telecommunications rules and regulations to out-date relatively quickly, the small industry participants may again feel the effects of the ACIF regime as they cope with interpretational issues and possible conflicting regulatory material.

In order to provide an idea of the issues relating to compliance with the Codes we have considered below a number of implementation issues which may arise out of *ACIF C518 - Call Charging and Billing Accuracy* (**ACIF C518**).

ACIF C518 was registered by the ACA on 27 April 2001 and applies to fixed and mobile carriers and carriage service providers (**CSP**) supplying telecommunication services intended primarily for the purpose of 'voice-telephony'. The Code defines the minimum required level of call charging and billing accuracy involving end-to-end network testing with a carrier or CSP, and testing of discrete segments, for example where more than one party is responsible for different billing accuracy perimeters of the end-to-end call charging and billing elements.

Compliance with this Code will involve testing of carriers and CSPs call charging and billing processes from the originating switch point to the terminating switch point for national calls within a carrier's or CSPs own network. Effects of customer equipment faults, fraudulent use of the telephone service or faults caused by atmospheric conditions in the access network are outside the scope of ACIF C518.

While most industry participants acknowledge the fundamental business requirement to ensure the accuracy of their billing processes, the development of formal test plans and compliance programs has traditionally been left to the largest carriers to implement. As set out above, however, ACIF's Codes of Practice seek compliance by all industry participants without reference to size. For smaller industry participants, management can find it difficult to justify the costs associated with compliance against the related business benefits.

The development of industry self-regulation was intended to develop codes of conduct which did not impose undue administrative and financial burdens. For smaller players, for this intention to be met they will need to take a wider view of the benefits of compliance. For example, developing test plans to ensure call charging and billing accuracy, may give management of smaller enterprises the opportunity to identify those areas where inaccuracies result in over-charging. Just as importantly from a business perspective, management may be given the opportunity to bill additional valid amounts to a customer for inaccuracies that resulted in under-charging. Development of robust and thorough test plans may assist management of industry participants in identifying additional revenues to compensate for the costs of implementing the plans, while at the same time increasing consumer confidence in the billing processes in place.

In light of the Codes generally, and ACIF C518 in particular, increased scrutiny will continue to be placed on the procedures adopted by industry participants for their billing and customer acquisition processes, particularly following recent failures of industry participants. Compliance with the Code may reduce the likelihood of negative comments by the media and consumer groups, and therefore, the intervention of regulators.

CHALLENGES OF IMPLEMENTING A COMPLIANCE PROGRAMS

It is not simply a question of telecommunications carriers and carriage service providers complying with all this new regulation and re-regulation in isolation to each other. The plethora of new codes requires these organisations to constantly re-adjust their compliance strategies and seek to modify them with their business objectives.

That is, after understanding the regulatory "universe" in which a carrier or CSP operates, management will need to perform a risk assessment of each of the regulatory requirements – and risk should be considered not only in relation to penalties for non-compliance, but also the impact of lost opportunities, changes in shareholder value and competitive advantage.

Only after understanding the regulatory requirements and the related risks can management begin to implement the required changes.

After implementing any required changes, there is also the requirement for regular monitoring and reporting processes to be established to identify any non-compliance, or new and emerging issues. Regular reviews are also required to ensure that the changing regulatory environment is understood in the context of changing business strategies.

Given the growing complexity of regulatory requirements, increasing consumer demands and the sensitivity of issues relating to carriers and CSPs, the board of directors and senior management of participants should ensure that there are adequate procedures within their organization to ensure that monitoring and reporting activities are undertaken. For some organizations, this requires regular sign off by operational management of the compliance with regulatory requirements, for others which are exposed to particular sensitivities either internal or external parties are asked to review compliance and report back to the board and/or senior management. The level of exposure that the board/senior management is prepared to accept will determine the procedures to be adopted.

By implementing formal regulatory management and compliance strategies, organisations may be able to demonstrate to the various stakeholders that they take a pro-active approach to regulatory management and link the operations to the delivery of the overall business strategy.

CONCLUSION

Whilst there are arguably a number of issues which prevent industry participants of all types from becoming ACIF signatories, it is clear that some benefits exist for those industry participants who do sign up, or at least put into practice compliance measures. Most importantly, by implementing formal regulatory management and compliance strategies, organisations will be able to demonstrate a pro-active approach to regulatory management, linking the operations to the delivery of the overall business strategy and creating value for their shareholders.

The question remains however, is all this new industry regulation really addressing the needs of the consumers and is it practical for industry participants, no matter how large or small, to comply with it? There remains a significant risk that the much heralded expansive competition in the telecommunications industry may well be adversely affected if potential participants are deterred from continuing to be players due to the sheer cost and technical difficulties of compliance.

1 *Telecommunications Act 1997* (Cth) Section 4
2 Section 15 of the Act

The views expressed in this article are those of the author and not necessarily those of the firm or its clients.

Brenton Yates is a Solicitor in the Information Technology and Telecommunications practice at the Sydney Office of PricewaterhouseCoopers Legal and Liam Buckley is a Director of business consulting firm PricewaterhouseCoopers.

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
Level 23 The Chifley Tower
2 Chifley Square
SYDNEY NSW 2000
Tel: +612 9230 4280
Fax: +612 9230 5333
Email:
niranjan.arasaratnam@aar.com.au
or
Shane Barber
c/-PricewaterhouseCoopers Legal
Level 10, Tower 2
Darling Park
201 Sussex Street
SYDNEY NSW 2000
Tel: +612 82666 787
Fax: +612 82666 999
email:
shane.barber@pwclegal.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
- privacy
- advertising
- telecommunications
- contempt
- copyright
- film law
- freedom of information
- broadcasting
- censorship
- information technology
- 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: ..... Email: .....

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 $110.00 (includes GST)
- Corporate membership $495.00 (includes GST)
  (list names of individuals, maximum of 5)
- Student membership $38.50 (includes GST)
  (please provide photocopy of student card - full time undergraduate students only)
- Subscription without membership $110.00 (includes GST)
  (library subscribers may obtain extra copies for $10.00 each plus GST and handling)

Signature .....