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 JASON MACARTHUR AND NIRANJAN ARASARATNAM Vol 18 No 2 1999

INTERNET CENSORSHIP: SEE NO EVIL, SPEAK NO EVIL, HEAR NO EVIL

New CLB Co-Editor Niranjan Arasaratnam analyses the pitfalls of, and myths surrounding, the Government's Censorship Act.

Talking about Internet censorship is like discussing abortion. It is impossible to have an informed debate because the protagonists end up talking about different issues. Each protagonist marks out its own territory based on an inflexible view of how the world should operate. Conservative groups preach family values, the Internet industry focuses on commercial issues and civil libertarians obsess about free speech.

The result? The *Broadcasting Services Amendment (Online Services) Act 1999* ("**Act**"), which is confused, ill-conceived and very difficult to implement in practice. The Act was passed by the Commonwealth Parliament on 30 June 1999 and awaits Royal Assent. In the meantime, the Internet industry is left wondering how the Act will be implemented and what its effect will be on e-commerce in Australia.

THE BILL

The Act amends the *Broadcasting Services Act 1992* ("**BSA**") to bring within its regulatory net the regulation of online services.

The Act establishes a complaints regime under which the ABA will investigate complaints from the public about *prohibited content* or *potentially prohibited content*.

There are two standards for prohibited content depending upon whether the content is hosted within or outside Australia. Internet content hosted within Australia is prohibited content if the content has been classified RC (Refused Classification) or X by the Classification Board, or the content has been classified R and access to the content is not subject to a restricted access system.

Internet content hosted outside Australia is prohibited content if the Internet content has been classified RC (Refused Classification) or X. R rated content from outside Australia is not prohibited and does not need to be subject to a restricted access system.

The rules apply to Internet content hosts ("**ICHs**") and Internet service providers ("**ISPs**"), with different standards applying to each. In summary, where there is prohibited content hosted within Australia, the ABA will issue a *final take-down notice* to the ICH directing it to remove the content from its site. Where the ABA identifies prohibited content hosted outside Australia, the ABA must notify the Australian police (if sufficiently serious) together with directing ISPs to carry out blocking measures in accordance with a specified industry code (a *standard access-prevention notice*). The ABA may issue *interim take-down notices* in relation to potentially prohibited content if it believes that the content is likely to be classified RC, X or R. Interim take-down notices apply pending classification.

If an industry code governing blocking content does not exist, ISPs must take reasonable steps to block the content. In determining what are reasonable steps, regard must be had to the *technical and commercial feasibility of taking the steps*. In addition, an ISP does not need to block overseas prohibited material if it has in place an ABA-approved *alternative access-prevention arrangement* that provides a reasonably effective means of preventing access to prohibited content. The Act provides examples of alternative access arrangements, including a service involving the use of Internet content filtering software or a *family-friendly* filtered Internet carriage service.

INSIDE THIS ISSUE

CONTENTS

The ABA may also issue *special take-down notices* or *special access-prevention notices* as an anti-avoidance measure which prohibits ICHs from hosting, and requires ISPs to block, the same, or substantially similar, content to any prohibited content identified in an interim or final take down notice, or a standard access-prevention notice.

ICHs and ISPs must take reasonable steps to develop industry codes (by 1 January 2000) which deal with procedures which ensure that online accounts are not provided to children without parental consent, give parents information and procedures to supervise access to Internet content, inform producers of content about their legal responsibilities, tell customers about their rights to make complaints and provide information on client-side filtering technologies and services. The Act also provides for the development by ISPs of codes on the steps to take to block access to overseas prohibited content and to provide client-side filtering technologies which will trump any direction by the ABA to block access to overseas content.

All notices must be complied with by no later than 6pm on the next business day after the notice was given to the ICH or ISP. The ABA may designate a scheme to deem service of a notice on all ICHs and ISPs.

EFFECTS ON INTERNET COMMERCE

The carriage of pornography on the Internet is good business. By some estimates, pornography accounts for up to 40% of Internet traffic. Internet censorship will fundamentally alter the economics of an ISP's business, particularly for the smaller ones.

Moreover, the implementation of blocking mechanisms is too expensive for smaller ISPs, nor do they have the technical skills to implement them. Smaller ISPs serve rural areas where many larger ISPs do not find it profitable to build points of presence. The Act serves to reduce Internet access and connectivity in precisely the areas the Government has identified are in need of more sophisticated communications.

Blocking technology is not 100% effective, with the result that legitimate sites will be blocked. Many companies use the Internet as the primary source of product information. The effective use of the World Wide Web depends on continuous availability of merchants' product information. The potential damage on legitimate Internet operators is enormous. It is analogous to discovering that your advertisement in the White/Yellow Pages has been deleted. For example, a search for an electrical component using Alta Vista and Iseek, the filtered engine search favoured by Senator Alston, returned 8545 entries on Alta Vista and a paltry 1591 on Iseek[1].

The Act will drive content outside Australia. The Internet is already a US-centric medium. The Act will add to the disproportionate amount of traffic from Australia to the US. As non-US ISPs have to pay for both ends of the transoceanic circuits that are required to connect to US backbones, it will increase the costs of Internet transmission for Australian ISPs.

DEFICIENCIES WITH THE ACT

E-mail exclusion

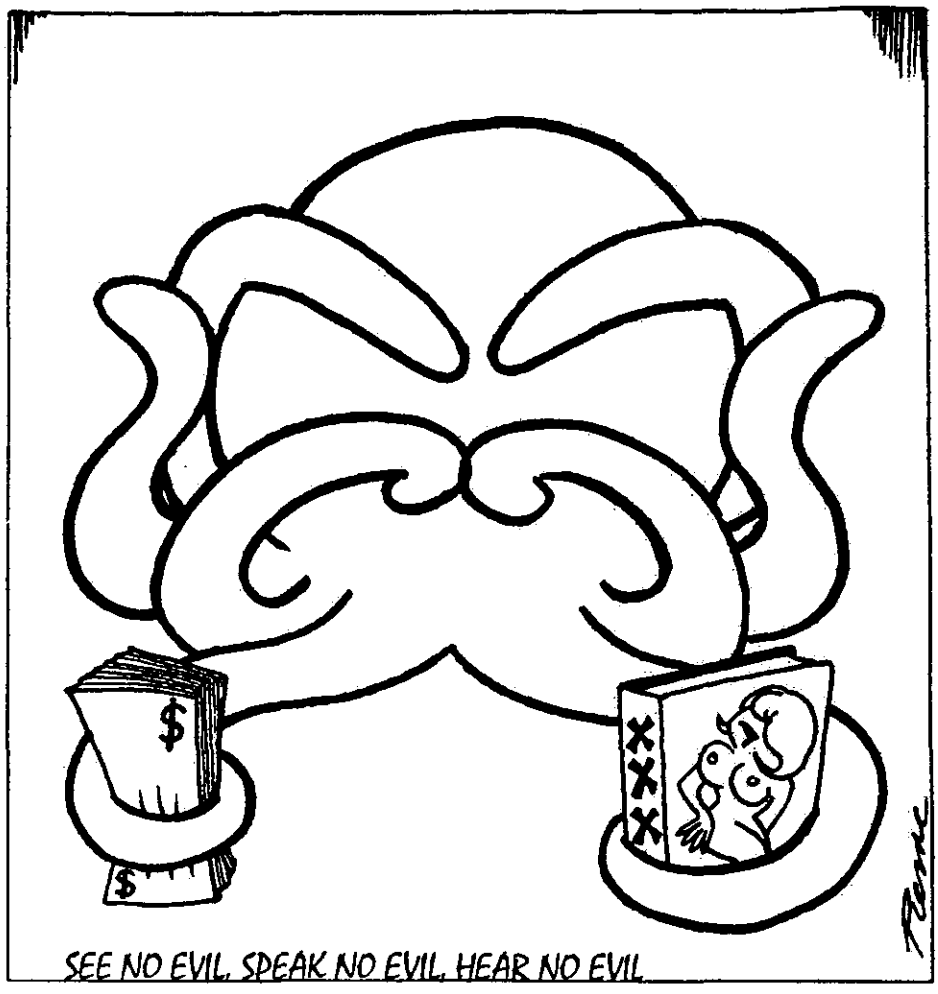
The Act excludes ordinary electronic email from the scope of Internet content which is to be regulated and limits its application to content accessed from a web site. It seems relatively easy for an ICH or ISP to buy IP addresses from other ISPs and send prohibited emails to users as a means of circumventing the Act. This practice does in fact occur resulting in a grov·ing market for solicited and unsolicited pornographic emails.

Definitional Problems

The Act applies to ISPs and ICHs. These terms (like many other technical Internet terms) are jargon without any settled meaning. ISP has been used to describe providers of Internet access only, resellers of other ISPs' Internet access, providers of Internet access together with email, newsgroups and chatrooms, providers of a gateway to a range of other linked sites and services, providers of a "walled garden" of password protected Internet sites and providers of wholesale IP connectivity to other ISPs and Internet access providers. The Act lumps all these entities into one with the assumption that each has the same responsibility over content and ability to control access to it. The Act assumes that these terms are static and immutable when in reality they are evolving together with the medium in which they operate.

Reliance on Codes

The Act relies heavily on industry codes. The Act requires associations or bodies that represent the ICH and ISP sections of the industry to develop codes on the various matters dealt with by the Act. It will be difficult to find such associations. The Internet Industry Association represents a small portion of the 600 odd ISPs in Australia, while it is unclear what body will represent ICHs. Industry codes assume some level of alignment of commercial interests amongst the industry players. This is sadly not the case. For example, for quite some time now the Internet industry has been developing a code of practice governing things such as billing practices, privacy and content rating. It has been near impossible to achieve consensus and the latest draft of the code remains a work in progress. The technical and commercial considerations of blocking will differ depending on the size of the ISP and where the ISP lies on the hierarchy of Internet networks.



In the absence of industry codes, ISPs must take reasonable steps to prevent prohibited overseas content from being accessed in Australia. The Act provides that in considering what are reasonable steps, the technical and commercial feasibility of taking the steps must be considered. As ISPs do not believe any form of blocking is technically nor commercially feasible, the test is extremely contentious. Technically, the use of proxy servers to block access is not feasible. Proxy servers slow network performance and can be circumvented. Commercially, it is not feasible to force onto users "clean" services that permit access to a set of permitted URLs only. That would severely limit the Internet universe and substantially diminish the utility of the Internet. The impact on Australia's position in the global e-commerce milieu would be enormous.

Anti-Avoidance Measures

The anti-avoidance measures, under which the ABA can direct ISPs to block content similar to prohibited material, are a real cause for concern. ISPs will become precisely what they do not want to be: editors of content carried over their networks. ISPs, by and large, do not view, let alone edit, content carried over their networks.

However, the new anti-avoidance measures will force ISPs and ICHs to scour their sites and networks each day to identify prohibited material. Once they discover any questionable material, ISPs and ICHs will have to decide whether the content is similar to prohibited content – a judgment on which significant penalties hang. Where is the old Government policy which made ISPs liable for content only if they knowingly created or provided that content[2]?

The revised draft of the Bill introduces the concept of recognised alternative access-prevention arrangements. Clearly, the Government was concerned with the practical implementation of its ISP

blocking regime and this amendment is a response to this concern. Essentially, ISPs will be able to trump a blocking notice if it offers client-side filtering services.

However, the filtering services must be approved by the ABA and its effectiveness will largely depend on the attitude of the ABA to client-side filtering services. The Act does not require the ABA to consider the technical and commercial feasibility of providing the filtering services (even though that is consistent with the Act's overall approach). Also, the Act provides an example of filtering services, being a *family-friendly* filtered Internet carriage service, which is neither a legal nor technical concept.

The take-down notices directing ICHs and ISPs to remove or block content may not be workable. The efficiency and fairness of the regime will depend upon how the take-down notices are framed. Not all web pages, nor all content on a web page, will be prohibited and take-down notices should reflect that reality. ICHs and ISPs will need to be given the specific offending web page, together with a precise description of what content is prohibited. ICHs should be told how the content can be modified to make it non-prohibited, or to move from one classification to another. Another problem will arise where take down notices are issued against ISPs who host content on behalf of their customers. Those ISPs will need to locate the content and delete it from their servers.

Complaint Flooding

The censorship regime established by the Act is open to abuse. The main scope for abuse is flooding. Any number of interested parties could flood the ABA with complaints against all manner of alleged prohibited content. All complainants have immunity from civil action in respect of any loss caused by a complaint. Armed with this immunity, an ISP could make a host of complaints against another ISP's content as part of a regulatory gaming strategy. Conservative groups are unlikely to limit complaints to hard core content. They will be concerned with any salacious content and may require the ABA to investigate all such content. Civil liberties groups may employ a complaints-bombardment technique as a spoiling tactic. Does the ABA and the Classification Board have the resources to respond to all such complaints?

Under the Act, the ABA's only way to filter (excuse the pun) complaints is by disregarding frivolous and vexatious complaints. It will be interesting to see how the ABA exercises this discretion.

MYTHS

It is not the drafting of the Act that is cause for concern, it is the entire Act itself. The Government has pushed through controversial legislation which raises fundamental civil liberty issues relying on a number of key myths. The number of myths relied on by the Government would make Homer proud.

MYTH 1: COMMUNITY CONCERN

The first myth is that the Act was precipitated by a groundswell of community concern over offensive material on the Internet. There was, however, no evidence before the inquiry that indicated the broader community was in favour of Internet content regulation. In fact, one participant in the select committee gave evidence of repeated requests of the Department of Communications, Information Technology and the Arts for evidence of such community outrage and its failure to provide a response.[3]

There are in fact a number of surveys and polls indicating an ambivalence towards Internet content regulation of the type proposed by the Act. The Australian Democrats described polls by the Age, www.consult, Roy Morgan (for the Eros Foundation) and an ABC phone-in as indicating overwhelming opposition to Internet content regulation, particularly any censorship of non-violent erotica.

If an ICH wishes to avoid an R rating, then , according to the Office of Film and Literature Classification Film and Video Guidelines, it would need to observe the following guidelines:

Language: course language may be used.

Sex: sexual activity may be implied.

Violence: generally, depictions of violence should not have a high impact.[4]

It is extremely doubtful that a majority of Australian adults would prefer to have their Internet limited by these guidelines.

MYTH 2: TECHNICAL AND COMMERCIAL FEASIBILITY

The second myth is that filtering is technically and commercially feasible. A cornerstone of the Act is the role of filtering technology. Under the Act, ICHs will be required to remove prohibited content (or substantially similar content). ISPs will be required to take reasonable steps to prevent end-users from accessing prohibited content (or substantially similar content) from outside Australia.

There are five factors which render the Act not technically or commercially feasible, all of which were identified by the Australian Democrats[5].

First, the use of proxies and router-based blocking technologies would reduce network performance and increase delays in Internet response times. Given the scarcity of bandwidth in Australia, this is a major concern.

Second, there are a number of techniques which can be used to circumvent blocking. Proxies which are based outside Australia can be used to rewrite queries and disguise responses so that they do not appear to originate from a blocked site. Encryption, protocol tunnelling, private networks and non-terrestrial communications also enable users to bypass blocking technologies. Web sites are already emerging which provide censorship avoiding strategies.[6]

Third, proxies are typically restricted to specific protocols on the Internet, such as the World Wide Web. Content can easily be shifted to FTP sites, mail servers and newsgroups.

Fourth, blocking involves the use of proxy servers which are expensive to purchase and it costs money and time to maintain.

Fifth, it was argued that filtering software is not 100% effective and that it invariably leads to the blocking of legitimate sites. For example, the German Government's attempts to block large amounts of content hosted in the Netherlands led to the entire server being unavailable to the significant disadvantage of other content

providers and users. In the United States, filter software resulted in breast cancer sufferers being unable to access Government-sponsored web sites. When a dictionary was put through Iseek, a filter engine, the words *alcohol*, *beer*, *bra* and *fist* were some of the words that were blocked.[7]

The Government accepted that blocking technology was not 100% effective. However, it was not convinced that problems with blocking technology was reason enough to scrap the proposed legislation. It argued that industry codes will set the standards for ISPs on how to block access to prohibited sites.

In the absence of industry codes, ISPs would be required to take reasonable steps to prevent access. The Act qualifies reasonable steps by having regard to the technical and commercial feasibility of the filtering measures. As discussed above, achieving consensus on industry codes and the feasibility of filtering is a significant challenge for the ABA and the industry.

MYTH 3: THE INTERNET IS A BROADCAST

The third myth peddled by the Government is that the Internet is a live broadcast medium and should be regulated as such.

Content regulation on the Internet raises fundamental questions as to the nature of the medium and the regulatory paradigms that ought to apply to such a medium. Is the Internet more analogous to a broadcast medium or a publication medium or a telephone medium?

The Government argued that the Internet is, or at least is moving towards, a broadcast medium due to its ease of access and higher bandwidths allowing real-time video streaming on the Internet. This was, in its view, justification for a regulatory scheme similar to that of a narrowcasting model.

The opponents of the Act claimed that broadcasting is a point to multi-point distribution medium while the Internet is a complex web of point to point communications. Accordingly, the regulation of Internet content would be as inimical as the regulation of telephone conversations. The corollary of this view is that Internet users should be responsible for the content they access and the extent to which children under their control should be monitored.

There is some judicial support to the opposition arguments. In *Reno v ACLU*, (which has now become part of Internet folklore, at least for the free speech advocates), the United States Supreme Court held that the Internet was not as invasive as radio or television and that pornographic material cannot be accessed accidentally.[8]

The Internet has aspects of both media: Internet services do broadcast content by allowing text, images and (poor quality) video to be provided by one person to many receivers (so called "push technologies"); while the interactivity of the Internet permits actual communications and the dissemination of information and ideas by any person similar to a telephone conversation.

It is misleading (and simplistic) to posit the Internet along broadcast versus telephone media lines. The broadcast/ telephone dichotomy has served the Internet industry well over the years in resisting government intervention in the development of the Internet industry. However, given the Government's position on content regulation, that dichotomy may be anachronistic and irrelevant. By disregarding the old paradigms, regulation which truly reflects the technical, commercial and social realities of the Internet may be formulated. May we please have a debate now?

1 See www.decisions-and-designs.com.au/thecensor.html.

2 Letter to The Australian newspaper by Attorney-General, Daryl Williams, QC, dated 17 November 1998.

3 "A Citizen's Comments on the Australian Government's Proposed Internet Censorship Legislation" by Dr David S Maddison dated 6 August 1997.

4 The OFLC web site can be found at www.oflc.gov.au.

5 Minority Report by Senator Stott Despoja.

6 See www.2600.org.au/censorship-evasion.htme.

7 See www.decisions-and-designs.com.au/thecensur.htme.

8 929 F. Supp. at 844.

Niranjan Arasaratnam is a Senior Associate with the Sydney office of Allen Allen & Hemsley

THE CENSORSHIP ACT: WHAT IT MEANS FOR ISPs

David Dodunski provides an industry perspective on some of the tools available to the Internet industry to comply with the Censorship Act.

So just how does the Internet industry technically comply with the *Broadcasting Services Amendment (Online Services) Act 1999* ("**Act**")?

This article examines the filtering and removal methods that are most likely to be implemented by Internet Service Providers ("**ISPs**") and Internet Content Hosts ("**ICHs**") following enactment of the Act. It also canvasses other types of client-side filtering technologies that would be better suited to the task at hand.

According to the Act, the Australian Broadcasting Authority ("**ABA**"), has the power to:

- Instruct Australian based ICHs to remove prohibited or potentially prohibited content from their server(s) that is classified RC or X, or classified R and is not subject to a restricted access system.
- Direct Australian ISPs to take all reasonable steps to prevent end-users from accessing prohibited content hosted outside Australia.
- Require Australian ICHs to remove, and Australian ISPs to block access to, content that is similar to prohibited content.

CONTENT REMOVAL

Let us assume that the ABA has instructed an ICH to remove offensive content from its servers. This is a fairly simple task for an ICH which hosts content on its own servers. However, the proposition changes where the "host" is an ISP, which by storing content is acting as an ICH. Removal of the offensive content will depend on whether the ISP can locate the content. This process in turn depends on whether the content is "live" and the precise location has been specified by the ABA. However, no amount of detail will assist an ISP if the owner of the content has moved the content. An ISP will play "cat and mouse" with an ICH chasing content on its servers. Meanwhile, the regulatory clock (one business day to comply) keeps ticking away.

CONTENT FILTERING - ACTIONS TAKEN BY ISPS

Of much more interest are the technologies involved in content filtering. ISPs will have to initiate an active and ongoing campaign to filter end user content to meet the ABA criteria to the best of their technical and commercial abilities.

In its current state, the Act is extremely broad and does not prescribe the exact software and equipment that will be required to be used by an ISP. However, it is likely that ISPs will utilise proxy server technology as their front line of defence.

A proxy server acts as a gateway between the end user and the Internet. Proxy servers are typically implemented by an ISP to speed up traffic flow and to act as a buffer between the Internet and its network. A proxy server can track and store Internet traffic. To explain how a proxy server works let us look at the difference between connecting to the Internet with and without a proxy server.

WHAT HAPPENS WHEN YOU ARE NOT USING A PROXY SERVER?

If you decided to go to Microsoft's homepage (www.microsoft.com) and your web browser was not configured to use a proxy server, here is the path the data would travel to get to and from your computer:

Request
your computer → Internet → www.microsoft.com

Response
www.microsoft.com → Internet → your computer

WHAT HAPPENS WHEN A PROXY SERVER IS INTRODUCED?

Things happen a little differently if your connection to the Internet travels via a proxy server. If the object requested is already in the proxy server's cache, then the proxy server sends a request to the web page to check if its local copy is current. If so, the proxy returns the page to the user (considerably quicker, because it is closer to the user). If the copy of the web page located in the proxy's cache is not current or does not exist, the proxy server fetches the page, caches it, and then gives it to you.

A cache is a database that stores the location and copies of all the web sites visited by users who connect to the Internet via that proxy server. The data path is as follows:

Request
your computer → proxy server → the Internet → www.microsoft.com

Response
www.microsoft.com → the Internet → proxy server → your computer

Essentially the proxy server separates the end user from the Internet, and carries out the end user's Internet requests on behalf of such end user.

PROXY SERVER USED AS A FILTER

As the proxy server contains a database of web pages, it has the power to act as a filter. The proxy server could forward (or refuse to forward) network traffic based upon its own internal rules. These rules could include blocking of sites deemed to be offensive and the blocking of certain text strings that contain offensive words.

By using the proxy server as a filter we are in effect adding another step to the process of viewing a web page. As

outlined above, the proxy currently asks two "Yes/No" questions before delivering a web page to an end user. The questions being, do I have a copy of the web page in my cache? If so, is it current? Filtering would add a third question, namely, is it allowed?

Whilst this does not seem like a big impact on performance, the problem is that, rather than caching complete web pages, a proxy server caches web objects such as text, frames, banners and animated pictures that together form the basis of a web page. The *ninemsn* web page, for example, consists of over 15 different objects. Requesting this page from a proxy server configured to filter content would result in the proxy server executing 15 extra queries. ISPs are justly concerned that filtering will slow down web traffic. For the ISP to bring the web back up to speed, huge capital outlays must be made to purchase faster proxy servers and more money spent on running this equipment. Filtering also places an administrative cost on the ISP to ensure that sites banned by the ABA are black listed on their proxy servers. As always, all these costs will be passed onto the consumer either in terms of slow access speeds or higher Internet charges.

What I have just described is how ISPs will use proxy servers to "filter" web browsing (www). However, the Act could also apply to news groups, Internet relay chat, FTP and other Internet services, both current and emerging.

Whatever the filtering solution adopted by ISPs it is unlikely to prove 100% effective. Recent tests conducted by the Electronic Frontiers Association using Internet filtering software have indicated that whilst these filters block many questionable sites, they also inadvertently block access to non-offensive sites.

CONTENT FILTERING – CLIENT-SIDE FILTERING

First generation filtering tools such as Net Nanny and CYBER PATROL work in a way similar to a proxy server installed at the client end to monitor traffic. These tools operate from a database containing good and bad sites that have been visited and rated. They essentially block access to the bad sites or allow the user to operate only within a defined "good zone".

Despite being limited to monitoring only web content, a major setback that these tools face is the ability to keep pace with the growth of the Internet. With a new site added every 18 seconds and an estimated 20% of Internet content devoted to pornography, it is unlikely that these first generation filters will continue to be effective.

Content Rating Services

The Recreational Software Advisory Council's RSACi rating is an association of webmasters who voluntarily rate their own Internet sites for classification. This rating functions within Microsoft Internet Explorer or Netscape Navigator.

There are two main setbacks with this rating system. First, though the system is two years old, fewer than 4% of web sites currently use the RSACi standard. As a consequence, software that relies entirely on the RSACi system makes 96% of the web either not available (if the software blocks unrated sites) or not freely available to the end user without some form of blocking.

Image Based Filtering

Previously, filtering technologies were either list dependent or relied on key word searches of HTML code to block access to a site. Now, recent advances in software technology have led to the development of Image Based Filtering.

Image based filtering is now available from such products as "Eyeguard".

Using sophisticated image analysis, Eyeguard checks the images being displayed for excessive skin tones, thereby protecting the user from pornographic images. Once installed, explicit images displayed on the screen from any source will automatically be blocked.

Unlike conventional web filters that can only eliminate known pornographic sites, Eyeguard protects against the actual site content. This affords the most complete security from any pornographic sites and will complement any existing Internet security program already in operation.

Until the specifics of the industry codes contemplated by the Act have been defined, we will not know for sure what technologies will need to be implemented by ISPs or the costs involved. What we can ascertain is that the most effective means of filtering will involve a mixture of ISP based filtering using proxy servers and client level complements such as Eyeguard image filtering.

If the objective of the Act is to protect a nation's citizens from exposure to perverted and immoral material trafficked via an electronic medium, then a cooperative relationship is needed between an ISP and its end users. Realising that each individual has a differing set of moral values and what may be technically and commercially feasible to one ISP may not be to another, this cooperation is unlikely to eventuate.

If you are concerned about the nature of the material present on the Internet, I advise you not to rely 100% on your ISP for protection; take additional action and implement your own end user filtering strategies. If all this seems too difficult then simply hang up on the Internet forever.

David Dodunski is a director of Eye-T Technology (Aus) Pty Limited.

PRODUCTIVITY COMMISSION INQUIRY: THE PBL VIEW

PBL gazes into the media crystal ball and finds outdated and anachronistic cross-media and foreign ownership rules.

Key features of the current regulatory regime for free television provide for high levels of sustainable competition in the industry, while also ensuring that the industry delivers programming which is relevant to, and valued by, Australians.

Free television has a unique and valued place in the lives of the Australian people. Australia's system of free television, which has developed over the last 40 years, is founded on a commitment from government and broadcasters to quality, diversity, responsiveness to audience needs and importantly, to Australian programmes. Australians have become accustomed to these high standards, and there is a public expectation that this service will continue.

Broadcasting legislation to date has recognised the important value given to free television by consumers, by limiting the number of available licences so that broadcasters can deliver the types of services consumers demand, including high levels of Australian content.

Free-to-air broadcasting faces serious challenges in the next decade. As it prepares for the expensive digital transition, it is also confronting a challenging and changing industry providing an expanded array of consumer services, such as pay television and on-line services, and proposed datacasting services. While these new services offer many benefits to those who have access to them, many Australians cannot afford new media. And most Australians would like to ensure that their free service is not compromised in any way.

The Productivity Commission should, in Publishing and Broadcasting Limited's ("**PBL's**") view, endorse those aspects of broadcasting regulation which preserve the current high quality, comprehensive, free television service with its benefits for Australian culture. In particular, the policy which limits the number of licences to three in any licence area should be recognised as providing extraordinary public benefit, in terms of culture, quality and diversity.

In a small economy like Australia, advertising revenue is limited. There is fierce competition between free-to-air broadcasters for advertising revenue. The television market is mature and its aggregate audience is stable. The minutes of advertising per hour are limited by regulation, so the aggregate supply of advertising audience minutes is also stable. A new network would simply fragment the available revenue, causing serious loss for all networks. If profit margins decreased, broadcasters would have no choice but to cut costs dramatically. Expensive programming such as drama, sport, current affairs and Australian content would be the first to be affected. Australians would be subject to a diet of low-cost imported programming.

Although free-to-air broadcasters are reviewing operations to take into account the new industry landscape, programming costs continue to rise. Local drama is appreciated by viewers, but can cost ten times the cost of its foreign equivalent. Broadcasters are also constrained by high regulatory costs, in the form of supertax licence fees and quota requirements. Pay television and on-line services are not subject to those burdens.

Both major political parties recently recognised these pressures, and

underlined their commitment to quality and local culture, when they legislated for a moratorium on new free-to-air broadcasting licences until 2007. This moratorium, and its effective enforcement (through appropriate limitations on proposed new datacasting services), is essential for the Australian broadcasting industry to maintain its current high standards.

THE BENEFITS OF DIGITAL BROADCASTING: A HIGH QUALITY FREE TELEVISION SERVICE

Free-to-air broadcasters are committed to introducing digital television, including high definition television, to Australian consumers. Preparations are underway for the transition, which will commence on 1 January 2001. Digital television will provide unsurpassed quality, and has the potential for many innovative new features. The legislation, including the moratorium on new licences, brings enormous public benefit, and is of central importance to the future of free television in Australia.

Free-to-air broadcasters should be encouraged to provide innovative features such as enhanced programming and high definition television, without regulatory limitations, so as to promote the speedy and smooth take-up of digital television. Pay television has been protected by restricting free-to-air broadcasters from providing multi-channelling and subscription services, unlike the USA where free-to-air broadcasters have complete flexibility. The transition from analogue to digital, with the added feature of high definition television, will be the most dramatic change for viewers since colour television, and will lay the foundation for free-to-air television for the next 50 years.

Datacasting services must be appropriately confined so that they do not amount to quasi-broadcasting services, in conflict with the moratorium on new broadcasting licences. Otherwise, audiences and revenue would be diverted from the free-to-air broadcasting industry, with adverse impact on Australian culture and quality.

ACHIEVING THE OBJECTIVES OF BROADCASTING REGULATION

Australia has the best broadcasting system in the world, with its balance of three commercial networks and two public broadcasters, all with national reach and commitment to Australian culture and quality. The services provided by free-to-air broadcasters to viewers are supplemented and complemented by scores of pay channels. The rules which limit the number of free-to-air broadcasters in each area, and some other policies, such as the anti-siphoning rules, which have ensured that consumers have the benefit of major sport on free television, are directed at preservation of the integrity and quality of this system in the public interest.

However, some other broadcasting policies require urgent re-evaluation as they have an adverse effect on consumer interest. These are: licence fee obligations imposed on free-to-air broadcasters; the system of Australian content regulation by way of inflexible "standards"; and pay television regulation.

CROSS MEDIA AND FOREIGN OWNERSHIP RULES

In recognition of a media landscape which has changed beyond description in the last few years, it is time for the cross media rules to be repealed, and along with them, the foreign ownership rules.

The cross-media rules are usually sought to be justified on the basis that the community needs access to a diverse range of information and viewpoints. This diversity is already assured through democratic principles, consumer demand, new technologies and services, and global participation.

The Australian consumer has access to a rich array of entertainment and information, with more services around the corner. The current range of media services providing news and information include commercial, public and community radio, national, regional and local newspapers, magazines, pay television, on-line services, data and information services and the five free-to-air television broadcasters. The availability of information sources will increase further when digital broadcasting is introduced. Datacasters base their business model on exploiting the conversion to digital broadcasting, which will enable them to gain access to the home through the TV set in order to deliver their digital services.

As is fitting for an advanced democracy, there is also a wide range of views, opinions and ideas, which are vigorously expressed in the media. Common ownership of different media forms, such as newspapers and television, would not affect this dynamic. Each media business would retain its own style, presentation and content, and views and opinions would be at least as varied and diverse as they are now. Commercial imperatives would guarantee this. The requirements of a newspaper audience, for example, are entirely different to the requirements of broadcast viewers. Consumers now have a wide range of choices open to them, and would exercise that choice negatively if there was a perception of media bias or blandness.

Free-to-air broadcasters, in particular, rely exclusively on differentiating their services on the basis of quality, such as accuracy and fairness in news and current affairs, and the provision of quality Australian programmes. Since broadcasters cannot differentiate their service on the basis of price, they can only gain audience loyalty by concentrating on quality. Any lapse in standards is rapidly penalised by viewers, who face zero switching costs in finding an alternative source of broadcast news.

Furthermore, independence of the media is a concept central to Australian democracy, and valued by journalists and producers of Australia's major media. Regulation, such as codes of practice, reflects high standards in broadcasting.

The advantages of cross-ownership do not lie in homogenising various media products, but in providing administrative and operational efficiencies, enabling both higher risk assumption and new investment and growth.

THE GLOBAL, CONVERGENT MEDIA INDUSTRY

The convergence of the media, computing and communications industries around the world has seen the emergence of new technologies and new media forms, and of huge transnational companies who have become active participants in globalised media businesses. These companies, such as AT&T, AOL, MCI Worldcom and Yahoo! have enormous capital bases, some with market capitalisation substantially in excess of

$100 billion. These companies are continuing to grow bigger and reach deeper into converged media and communications businesses. An example is the recent merger of the cable networks and media businesses of AT&T and TCI in the USA.

Within Australia, there is a similar pattern of convergence. Telstra and Cable & Wireless Optus are owners of, and active participants in, the television, Internet services and communications industries. Foreign transnational corporations have become substantially involved in Australian media businesses, for example, pay television (including News Corp, UIH, Time Warner, Sony, Disney), and Internet services (including AOL, Yahoo! and MCI Worldcom).

In this global information and entertainment landscape, and within Australia, Australian media companies are relatively tiny participants. The cross media rules are impeding the opportunity for Australian media companies to achieve the scale and capital base necessary to participate effectively in this global environment.

In particular, as the traditional boundaries between industries disappear, broadcasters will struggle to compete against the much bigger and better capitalised telecommunications companies. The telcos have crucial bottleneck control over the "last mile" access to homes and businesses. For example, in Australia, Telstra and Optus control all of the broadband HFC cable; Telstra controls all of the copper wire, which can deliver high-speed Internet access through xDSL technology; AAPT controls all of the available LMDS spectrum. These methods of high-bandwidth data delivery will enable the telcos to offer content that is directly substitutable for that of the free-to-air broadcasters. Yet there is nothing to stop the telcos making whatever investments they feel to be appropriate for their shareholders. In contrast, television, newspaper and radio proprietors are prevented by regulation from making what might be sensible investments.

FOREIGN OWNERSHIP LAWS INEFFECTIVE

In the past, PBL has supported foreign ownership laws, but in 1999, it is clear that these laws are not achieving their purpose. The rules apply unevenly and capriciously, and foreign participation in Australian media is a reality.

Foreign companies own substantial portions of the telecommunications, radio and newspaper industries and one free-to-air broadcasting network, and hold substantial investments in, or own outright, many of the operators in the pay television, online, and other media sectors. The justification of foreign ownership limitations based on levels of influence (as was intended to be the measuring stick) has become meaningless.

Further, even apart from questions of foreign ownership, consumers now have easy access to foreign sources of news. Online services deliver American newspapers, or British radio stations updated almost in real time. Pay television channels such as CNN are readily accessible. This means that the foreign ownership rules are not effective to prevent foreigners from exercising influence on the Australian populace.

REPEAL OF CROSS MEDIA RULES AND FOREIGN OWNERSHIP RULES WOULD CONFER ECONOMIC BENEFITS

Repeal of these rules would encourage efficiency by enabling local broadcasting companies scope to compete with "convergent" global media companies, both locally and on the world stage.

Local companies could build a stronger capital base for investment, and with it the leverage required for growth. Australian companies could trade their expertise and skills, and benefit from international relationships. Locally, infrastructure would improve, as would opportunities for development of content. There would also be increased export opportunities. The flow-on benefits for the economy of a competitive, efficient industry – creation of jobs, export opportunities, earnings - would be substantial.

Stronger media companies would have more capacity to meet public interest broadcasting objectives – high quality and innovative programming, diversity and Australian content. Community demand for services, competition in the provision of those services and competition regulation will ensure that Australians continue to receive media products of high quality, range and diversity.

However, the foreign ownership and control rules should not be repealed unless the cross-media rules are also simultaneously repealed.

PBL is prepared to compete with foreign companies within the changing Australian media sector, but it does not believe that it can do so on a genuinely competitive basis unless the cross-media rules are repealed and PBL can grow its capital base.

Repeal of the foreign ownership and control rules, without contemporaneous repeal of the cross-media rules, would produce the absurd result that foreign companies would be free to make further inroads into major Australian media sectors, while Australian media companies would be free only to look on.

AUDIENCE REACH RULES – OUTDATED AND INEFFECTIVE

The audience reach rule in the *Broadcasting Services Act 1992* is another outdated rule of no practical application that should be repealed.

The rule was part of the package of 1987 legislation ostensibly designed to protect diversity of information outlets in the Australian community. It has never had any practical effect, other than to create a second tier of commercial television broadcasting companies beneath the major networks.

Networking arrangements between major networks and their affiliates, pursuant to which most Australians receive all three network services, have long rendered the rule moribund.

This is an edited extract of the submission by Publishing and Broadcasting Limited to the Productivity Commission inquiry into Broadcasting Legislation.

CONVERGENCE - THE ARGUMENT OF CONVENIENCE?

The Productivity Commission is looking into the future of broadcasting legislation in Australia. Rachael Osman examines the industry push to get rid of the existing cross-media ownership restrictions.

The big news in media law is this - the not so secret password is "convergence". If you want to challenge cross media ownership restrictions, broadcasting licence restrictions, geographical restrictions, or almost any other type of restriction that currently exists regarding ownership of Australian media, begin your argument under the heading of "convergence".

THE CONVERGENCE ARGUMENT

"Convergence" is the word being used to sum up technological changes in the way media is or can be delivered to the public. It is a word that is featured heavily throughout the submissions received from big media players by the Productivity Commission's Inquiry into Broadcasting Legislation, which began in March.

The argument of convergence is basically this: because all existing communications are or can be digital, all existing communications have the capacity to be transported the same way, i.e. by satellite, cable, telephone and television. This means the existing divisions of media into the three pigeon holes of newspapers; television (analogue) and radio won't mean much because their digital equivalents will be travelling through the same tubes.

Submissions to the Productivity Commission's Inquiry into Broadcasting Legislation repeat this new wisdom as the reason why the Australian Government should consider current restrictions on media ownership as obsolete. Those in the "new media" camp (e.g. Ozemail and AOL) happily argue convergence. Those who are not in the established free to air broadcasters camp (e.g. Fairfax) also happily argue convergence. Packer's Publishing and Broadcasting Limited argues convergence up to a point, that point being the current moratorium on issuing any new commercial broadcasting licences and giving spectrum to people other than existing broadcasters. Foreign media proprietors who want a bigger share of Australian markets (i.e. News Limited) are more than happy to argue convergence.

The question is - will these arguments of convergence convince the Australian Government that media ownership rules need a fundamental overhaul?

THE PRODUCTIVITY COMMISSION'S VIEW?

Jock Given from the Communications Law Centre answered this question by stating:

> *"It is no secret that the Prime Minister would like to change cross-media ownership rules. This inquiry is a good vehicle to at least have a hard look at the existing media ownership rules."*

The inquiry has arisen from the requirement under the Competition Principles Agreement to review all legislation restricting competition. However, one look at the Issues Paper makes it clear that the Productivity Commission is fully convinced about the power of the convergence argument:

> *"The development of other services using telecommunications and Internet technologies is further blurring the bounds of broadcasting markets."*

"This is Australia's most comprehensive public inquiry into broadcasting ever," says Prof. Richard Snape, the Presiding Commissioner of the Productivity Commission. "Revolutionary technology is opening exciting new opportunities through the convergence of conventional television and radio with telecommunications and the Internet."

This convergence argument has got a lot of people excited. However, do these technological arguments justify the abandonment of existing restrictions on media ownership?

THE MOTIVATION BEHIND THE CONVERGENCE ARGUMENT

Jock Given maintains that the current arguments for convergence are really justifications for established media entities to increase their market dominance and for "new media" entrants to establish as much media dominance as they can in an environment that won't restrict them. "Arguments against cross-media ownership laws are being made by persons who would like to own more," he said.

Seen from this perspective, the basic premise of the arguments put forward by the big players appear very much as being primarily self interest as opposed to neutral arguments based on technological realities. An except from the submission by News Limited reads:

> *If we are to share in the benefits flowing from these opportunities we must be prepared to face the challenges thrown up along the way with enthusiasm and daring, not seek to hide behind walls of protectionist regulation. Otherwise we face the real danger of being left in a communications backwater....Cross-media and foreign ownership restrictions are inappropriate and irrelevant and should be removed....*
>
> *Convergence is not a theoretical issue: it is a reality which is blurring the lines between the delivery platforms of the media industry, making it counter-productive for government to attempt to create artificial barriers or distinctions between these traditional segments.*

Similarly the basic argument of the Fairfax submission reads:

> *We believe that media diversity, in an age of technological convergence, can be maintained and enhanced by competition policy and open markets and by the full and proper application of competition policy to these industries - rather than by regulation of media ownership.*

The submission by Publishing and Broadcasting Limited does a dog-leg by first advocating the need to continue "limiting the number of available licences so that broadcasters can deliver the types of services consumers demand, including high levels of Australian content". The

submission then advocates the desirability of abandoning cross media ownership restrictions by claiming "The advantages of cross-ownership do not lie in homogenising various media products, but in providing administrative and operational efficiencies...".

The message from the above excerpts is clear: because the world is changing we, the media proprietors, should be left to do as we please.

WHY THE RESTRICTIONS SHOULD REMAIN

What are the restrictions that they are trying to get rid of? The three kinds of limits placed on media ownership are: limits on ownership within a local area (i.e. the number of licences a person can hold in a defined licence area and restrictions on controlling more than one type of media), national limits (i.e. a person must not be able to control enough TV licences to reach over 75 percent of the Australian population) and foreign ownership limits. The basic idea behind these limits is that they encourage some sort of diversity in the media offered to the Australian public.

It is highly debatable whether the current media restrictions are doing a good job of providing diverse media in Australia. However, Jock Given is not of the opinion that our media ownership rules are ready for the scrap heap: "It is not a bad idea if major media is controlled by different people. While it is becoming more difficult to have legislation that deals with the different methods of delivering media, the current law is not obsolete yet," he said.

Convergence is a technical possibility. However, it remains to be seen whether the technical possibility becomes commercial reality. The media players are arguing that it will and that the only suitable type of regulation is general competition regulation under the *Trade Practices Act*. However, there is always the possibility that digital media might merely be an additional form of media, adding to consumer choice, the way analogue television did. As Jock Given puts it: "We need to be careful not to think that the world will end up with one media industry."

Rachael Osman is a postgraduate journalism student at UTS and a practising solicitor

THE UNIVERSAL SERVICE OBLIGATION RECENT EVENTS AND COMING ATTRACTIONS

Caroline Lovell examines recent developments in relation to the provision of the USO and outlines some future developments already on the horizon.

Part 7 of the *Telecommunications Act 1997* (Cth) ("Act") provides for the Minister for Communications, Information, Technology and the Arts to declare specified telecommunications carriers to be the universal or regional service providers in Australia. A universal service provider is required to fulfil the Universal Service Obligation ("USO"). This involves ensuring that all Australians, wherever they reside or carry on business, have reasonable access, on an equitable basis, to standard telephone services, pay telephones and prescribed carriage services[1].

Telstra is currently the sole universal service provider. Part 7 of the Act also contains a scheme for the assessment of the cost of providing the USO and for the collection, recovery and distribution of a universal service levy which shares amongst carriers the losses which result from the supply of services in the course of fulfilling the USO. The levy from each carrier is essentially a function of that carrier's proportion of the total revenue generated by carriers.

The assessment process takes place each financial year. The Australian Communications Authority ("ACA") is responsible for administering the process.

TELSTRA'S NET UNIVERSAL SERVICE COST CLAIM FOR 1997/8

In 1993/4, Telstra's cost claim was set at $230 million indexed to the CPI for the purposes of the 1994/5, 1995/6 and 1996/7 years as a result of a compromise between Telstra, Optus and Vodafone. For 1995/6 and 1996/7 Telstra's claims averaged about $250 million. For 1997/8 a new costing method was developed by Bellcore International Inc by agreement between Telstra, Optus and the ACA. On 25 September 1998, the ACA made the Net Universal Service Cost Avoidable Costs Determination 1998 which reflected the costing method developed by Bellcore.

Just a couple of days later, on 28 September 1998, Telstra filed its claim for the 1997/8 year with the ACA. The total of the claim was $1.8 billion. Not surprisingly, the magnitude of this claim caused an immediate reaction from the other carriers and the government because of its potentially negative impact on competition, investment and industry stability[2]. Without prior warning, the claim imposed a large liability on each carrier other than Telstra.

THE REACTION OF OTHER CARRIERS

Other carriers, for example Optus, immediately disputed Telstra's claim. Optus also made public statements that

if it were the universal service provider, it would be able to fulfil the USO for a tenth of the cost Telstra had claimed by using new and more efficient technologies than Telstra uses, for example wireless and satellite technologies. Optus claimed that Telstra's claim factored in costs for inefficient and aging networks and placed too much emphasis on the use of expensive copper network systems[3]. The other carriers also began lobbying the government for the opportunity to provide the USO.

This reaction is interesting, given that the services provided to fulfil the USO are loss-making, rather than profit generating. The interest of carriers other than Telstra in providing the USO seems to be the result of a number of factors, including:

- the belief that other carriers could fulfil the USO more cheaply than Telstra;
- the desire for control over the cost, as the current arrangements lead to commercial uncertainty. As the annual contribution cannot be known with certainty it has the potential to affect investment and other decisions to be made by carriers;
- the belief that providing the USO could facilitate a carrier's entry into new areas of Australia where it could then provide other services besides those required by the USO.

THE GOVERNMENT'S INITIAL REACTION

The government's initial reaction was to announce that unless agreement could be reached in relation to Telstra's claim for 1997/8 it would legislate to cap the claim. The size of Telstra's claim, particularly given the increase from the claims of previous years, meant that a negotiated agreement on the claim was always most unlikely. The *Telecommunications Laws Amendment (Universal Service Cap) Bill 1999* (**"Cap Bill"**) was introduced into Parliament on 23 March 1999 and passed on 26 May 1999. It is now only awaiting Royal Assent. Essentially, it caps Telstra's claim for 1997/8 at $253.32 million. This cap is also extended to the 1998/9 and 1999/2000 financial years[4].

Next, the Minister requested the ACA to provide a report on what the ACA considers:

- to be the real cost of providing the USO; and
- what might be appropriate arrangements for the future funding of the USO.

Prior to introducing the Cap Bill, the Minister also requested the ACA to review Telstra's claim for 1997/8. In order to do so, the ACA commissioned reports from industry consultants. In April 1999, Gibson Quai & Associates Pty Ltd and Ovum Pty Ltd provided the ACA with their report, entitled *"ACA USO Forward Looking Technologies Study"*. The Allen Consulting Group provided two reports, *"Telstra's Weighted Average Cost of Capital - Application to the USO"* and *"The Year 1 Cost Problem Application to the USO and Proposed Solution"*.

The report by Gibson Quai & Associates Pty Ltd and Ovum Pty Ltd advised on the technologies which would be appropriate to consider for the efficient provision of services in Potential Net Loss Areas identified by consultation with Telstra. The report also assessed the costs of providing the services using the technologies identified. A number of technologies, including LEO satellite services, were rejected because they were either not commercially available or failed to meet the study's performance requirements. The study identified a number of generic technologies as being worthy of further consideration and costing. These were CAN, Switching and Junctions. The lowest cost technology for providing the services varied between different Potential Net Loss Areas.

The first report by the Allen Consulting Group analysed the cost of capital which should be used to assess the magnitude of losses incurred in providing the USO for 1997/8 and 1998/99. The second Allen Consulting Group report considered the problem which arises in relation to depreciation used in calculating the cost of fulfilling the USO. Because the assets (infrastructure) used to fulfil the USO last, in general, more than one year, the report concluded that to return the first year depreciation in every year would over compensate the universal service provider.

On 29 April 1999 the ACA announced that it believed that the approach to the calculation of the cost of providing the USO set out in the report by Gibson Quai & Associates Pty Ltd and the first of the Allen Consulting Group's reports would lead to an annual cost/claim of around $600 million. If the recommendations contained in the second of the Allen Consulting Group's reports were also adopted, the cost could be reduced to about $425 million. As the Cap Bill has been passed, it was not ultimately necessary for the ACA to conclude its assessment of Telstra's claim for 1997/8 for the purpose of determining the contribution or levy to be provided by each of the other carriers. Nevertheless, the reports provided by the ACA's consultants have continuing relevance, because the result achieved by the Cap Bill cannot be, and was not intended to be, a long term solution. The ACA will also continue to assess Telstra's claim for 1997/8 in the context of its assessment of the cost of fulfilling the USO and future funding arrangements for the USO for its report to the Minister.

THE ACA'S ASSESSMENT OF THE COST OF FULFILLING THE USO AND FUTURE FUNDING ARRANGEMENTS

The ACA issued a Discussion Paper for the purposes of its report on 6 May 1999 entitled *"USO Costing and Assessment Arrangements"* and called for public comments by 28 May 1999. At the time of writing the ACA was expected to have provided its report to the Minister by 30 June 1999. It had received 4 submissions, from Telstra, Optus, Vodafone and SETEL (Small Enterprise Telecommunications Centre Limited), which had yet to be made publicly available. As the ACA's report is to be provided to the Minister, it will be up to the Minister to decide whether to release it publicly.

In light of the circumstances from which it has arisen, the ACA's report to the Minister is likely to recommend a change in the methodology used to calculate the net universal service cost. It also seems likely, as a result of the reports provided by Gibson Quai & Associates, Ovum Pty Ltd and the Allen Consulting Group, that the ACA will find that the cost of fulfilling the USO is substantially less than Telstra's claim for 1997/8, but

somewhat more than the amount at which it has now been capped for 3 years by legislation.

THE GOVERNMENT'S RECENT RESPONSE

On 6 April 1999, the Minister called for expressions of interest in tendering for the USO from carriers. The Department of Communications, Information, Technology and the Arts also issued a consultation paper calling for comments and expressions of interest by 28 May 1999.

At the time of writing, the Department had received 26 submissions or expressions of interest and was still taking submissions. The submissions already received are from a wide range of entities including carriers, the state governments and community groups. No arrangements have yet been made to make these available to the public and parts of them have been submitted on a "commercial in confidence" basis. The Department is not able to indicate a date by which it will respond to the submissions or expressions of interest as a result of the complexity of the issues it has to consider.

The consultation paper is careful to note that the call for expressions of interest "does not represent a commitment on the part of Government to establish a competitive selection process of any particular sort" and that an expression of interest will not be taken as a specific or binding offer by a carrier to be a universal service provider[5]. Nevertheless, the press release issued by the Minister on 6 April 1999 states that the government has formed the view that carriers other than Telstra may be able to deliver "a more competitive and efficient USO", for example by using satellite or wireless local loop technologies. Opening the USO up to competition may result in "more innovative services to regional, rural and remote Australia, improvements in service standards, and the introduction of new carriers and possibly new infrastructure with a resultant increase in price and service competition"[6].

The Minister's call for expressions of interest is a rare example of policy moving in advance of deployed technology. Although there is undoubtedly the potential for other technologies such as satellite technology or wireless local loop technologies to be utilised in relation to the USO, such technologies are not yet being used commercially by any carriers in Australia for the provision of services such as the standard telephone service or pay telephones (even if they are technically feasible).

Inevitably, then, there will be lag between any commitment by the government to tender the USO and the actual development and utilisation of alternative infrastructure to Telstra's existing networks. Query also, whether the current level of industry enthusiasm for the concept of providing the USO will subside when it is necessary for carriers interested in becoming a universal service provider to calculate how much it will actually cost them to fulfil the obligations of a universal service provider, for example, for the purpose of assessing how much to bid in the event that the USO is put out to tender by an auction process. As Telstra has never had to disclose the calculations it uses to determine its net universal service cost claims, carriers other than Telstra will find it very difficult to calculate the costs of fulfilling the USO, despite the studies undertaken by Gibson Quai & Associates Pty Ltd and Ovum Pty Ltd. The fact that the data provided by Telstra for these studies was provided in confidence means that these studies are not entirely transparent[7].

Whether the government moves forward with tendering the USO will no doubt depend on the quantity and quality of the expressions of interest received and on the degree of confidence they engender that the USO could be entrusted to a new universal service provider or providers.

The consultation paper issued by the Minister specifies the issues the government considers arise in relation to the competitive selection of universal service providers, including the following matters:

- what services should be included in the USO, given that tendering the USO will provide an opportunity to reconsider and perhaps increase the services to be provided?[8];
- how should service areas be determined? For example, should geographical areas be used or Telstra's existing exchange areas?;
- what service standards are appropriate and how can they be imposed?;
- what selection process should be used?;
- how should transitional arrangements be managed, for example, while functions such as maintenance are transferred from the existing universal service provider to a new universal service provider?;
- if a new universal service provider wishes to fulfil its obligations by using part or parts of Telstra's existing infrastructure, how will access be managed?;
- how long should a carrier remain a universal service provider?;
- what, if any price control arrangements should be imposed?; and
- what arrangements should be made to ensure that the USO is fulfilled and what "safety nets" can or should be developed in case a universal service provider is unable to fulfil its obligations.

1 The standard telephone service is a carriage service for the purpose of voice telephony or, in the case of a person with a disability, another form of communication of equivalent functionality which passes the connectivity test. The connectivity test is passed if an end-user supplied with the service is ordinarily able to communicate, by means of the service, with each other end-user who is supplied with the same service, whether or not the end-users are connected to the same network – *Telecommunications Act 1997 (Cth) s17*. A prescribed carriage service is one specified by regulation. No such services have been specified to date.

2 Australian Communications Authority Discussion Paper released 6 May 1999 – *"USO Costing and Assessment Agreements"*.

3 *Communications Day* 13 October 1998.

4 Clause 2 of the Bill is unusual and provides that the provisions capping the claim will be taken to have commenced on 30 June 1999 in the event that the Bill does not receive royal assent before that date.

5 Consultation Paper, page 4.

6 Press Release issued by the Minister on 6 April 1999.

7 On 24 November 1998 ATUG (the Australian Telecommunications Users Group) called for Telstra to disclose the costs it used to calculate its claim for 1997/8.

8 The government has also announced its intention to upgrade the USO to include a requirement that a universal service provider provide access on demand to high speed digital data services.

Caroline Lovell is a solicitor at Clayton Utz. The views expressed in this article are the author's own and not necessarily those of the firm or its clients.

STOPPING SIGNAL PIRACY

Signal piracy is a growing problem for television operators in Australia. Mark Bamford reports.

Among the legislative reforms being undertaken by the Government at the moment in the areas of copyright, broadcasting and electronic communications, one issue at risk of being overlooked is 'signal piracy'.

At present this issue looms largest for pay televisior operators. A pay television operator may deliver its service by means of satellite, cable or microwave multipoint distribution system. The program-carrying signal is encrypted by the operator using algorithms that alter the signal. A subscriber then gains access to the service by obtaining reception equipment which decodes the signal. In this way, the operator is able to track its signal and charge each customer periodical fees.

Unfortunately, it is possible for non-subscribers to intercept the program-carrying signal by purchasing unauthorised decoding equipment. In such a case, the operator is not paid the ongoing fees on which its business is dependent.

Free-to-air broadcasters may also be subject to signal theft, for instance where an encrypted satellite transmission to an area licensed for broadcast is intercepted and accessed outside the licensed area.

Currently, there is no effective legal recourse against such "signal piracy".

LACK OF REDRESS UNDER CURRENT LAW

There are no express provisions in the *Copyright Act 1968* ("**Act**") which directly address the unauthorised reception of encrypted transmissions.[1] To the extent that delivery of a television service constitutes a "broadcast" under the Act, the principal copyright in respect of the broadcast is to re-broadcast it. This means that the unauthorised *reception* of a broadcast does not amount to *infringement of copyright in the* broadcast.

To the extent that delivery of a television service does not constitute a broadcast (for example, where delivery is by cable which is, under the Act, a transmission to subscribers to a diffusion service) the Act affords no protection whatsoever.

Although a number of statutory provisions prohibit various acts in relation to telecommunications and radiocommunications, these do not directly and effectively prevent the unauthorised reception of encrypted transmissions.[2] A transmitter's only course of action is often to rely on trade practices or trade mark claims which are not suited to adequately deal with this issue.

WHAT IS NEEDED

Legislation should be introduced for the specific purpose of preventing the unauthorised reception of an encrypted transmission. Such legislation could incorporate the following elements:

- criminal sanctions against the unauthorised reception of an encrypted transmission;
- criminal sanctions against the commercial dealing in equipment which has the purpose of enabling unauthorised reception of an encrypted transmission;
- civil remedies in relation to the unauthorised reception of an encrypted transmission;
- civil remedies in relation to commercial dealing in equipment which has the purpose of enabling unauthorised reception of an encrypted transmission.

IS SIGNAL PIRACY A COPYRIGHT ISSUE?

The exposure draft of the *Copyright Amendment (Digital Agenda) Bill* ('**Bill**') introduces new enforcement measures:

- to provide criminal sanctions and civil remedies for the making of, and

commercial dealings in, devices for the circumvention of technological copyright protection measures;[3] and

- to provide criminal sanctions against the tampering with electronic rights management information.[4]

In the commentary on the exposure draft of the Bill, the introduction of remedies in relation to the unauthorised reception of encrypted broadcasts is specifically excluded on the basis that such unauthorised reception is not an infringement of copyright in the broadcast or underlying copyright material.[5]

This basis would seem somewhat inaccurate and inconsistent with other aspects of the exposure draft of the Bill. Such remedies are no less associated with copyright than are the proposed technological copyright protection measures and rights management information provisions introduced by the Bill.

The copyright affected by the unauthorised reception of an encrypted transmission may include copyright in the "broadcast" (as defined in the Act) and significantly, the underlying copyright material. Such material includes cinematograph films and the literary works, musical works and sound recordings adapted to create such films. A television operator will have acquired rights in such material for the purpose of its transmission.

The unauthorised reception of a television operator's transmission will not only diminish the value of the transmission but also the underlying copyright material.

The UK legislature has had no difficulty finding signal piracy an issue with respect to copyright, making it an offence under its copyright legislation to fraudulently receive programs, and to make, sell, import or let for hire an unauthorised decoder.[6] Similarly, legislative protection has subsisted in the New Zealand copyright legislation for some time.

Subsequent to the release of the exposure draft of the Bill, the House of Representatives Standing Committee on Legal and Constitutional Affairs invited submissions from the public in relation to the effective enforcement of copyright in Australia. The terms of reference for the Standing Committee's inquiry include the adequacy of criminal sanctions against copyright infringement and the adequacy of civil actions in protecting the interests of plaintiffs and defendants for copyright infringement.

If it is accepted that piracy is a copyright matter, then there would seem no better opportunity than at present to incorporate relevant provisions into the Act.

AMENDMENT TO OTHER LEGISLATION?

If the government is unwavering in its view of signal piracy as a non-copyright issue, then there is other legislation which could incorporate amendments to deal with the issue.

As far back as 1994, the Copyright Convergence Group recommended that criminal offences relating to the unauthorised use and reception of encrypted signals be introduced.[7] The difficulty with introducing measures against signal piracy into the *Crimes Act 1914* is that such legislation is not appropriate for civil sanctions.

Perhaps a better alternative is the *Broadcasting Services Act 1992*, being the legislation under which broadcasters and narrowcasters are licensed.

As signal piracy has been pressed with the government as an issue for some time, most important now is the "end" rather than the "means". The worst result would be for the issue to be deflected from one legislative initiative to another so that it is not dealt with substantively at all.

CONCLUSION

In 1997, pay television operators estimated that there were 2,500 – 5,000 recipients of pirated signals in Australia. Such figures are not, in absolute terms, astounding. They are, however, significant given the infancy of pay television in Australia.

In the US where pay television is more established, as far back as 1992 signal theft was estimated as resulting in US $4.7 billion in unrealised revenue annually.[8]

As pay television grows in Australia and new technology provides a greater choice of "subscription services" for consumers, the issue of signal piracy will become increasingly significant. The introduction of appropriately framed legislation to prevent the unauthorised reception of encrypted transmissions will provide benefits to copyright holders with no contrasting burden or adverse effect on the public.

1 Except where otherwise expressly provided, the word "transmission" is used in a generic sense to mean any broadcast, transmission to subscribers to a diffusion service or other communication.

2 Regulatory provisions prohibiting various related activity include the following: *Crimes Act 1914* (Cth) (Part VIIB); *Broadcasting Services Act 1992* (Cth); *Radiocommunications Act 1992* (Cth); *Telecommunications Interception Act 1979* (Cth).

3 Items 85, 87 and 88.

4 Items 9 and 87.

5 Exposure Draft – Commentary, paragraph 100.

6 See *Copyright, Designs and Patents Act 1988* ss 297-299.

7 'Highways to change, Copyright in the New Communication Environment', August 1994 p13.

8 Federal Communications Council report 97-053, 11 February 1997.

Mark Bamford is a Senior Associate in the Sydney office of Tress Cocks & Maddox

INFORMATION WARFARE: CHANGING TRADITIONAL NOTIONS OF AGGRESSION

Tanya Ross-Gadsden discusses the need for regulators to recognise the impact individuals have in cyberspace, and how individualised "cyberweapons" reshape traditional notions of aggression.

With the advent and proliferation of the Internet, information has become accessible to computer users of all descriptions. It is simple to interface with usergroups, exchange information and knowledge, or create individual Internet sites. This environment also reshapes the concepts of force, aggression, and warfare as the tools of war no longer belong to nation states. Technology has accelerated social interaction exponentially, yet municipal regulation and public international law have failed to keep pace. To some, cyberspace represents a new frontier akin to the wild American west of the early 1800's. In this environment, rule making will require a combination of law, regulation, education and training of users, as well as the cooperation of countries worldwide.

What authors do not mention is the way in which laws of the physical world must change in order to effectively operate within this new frontier. In this way, Information Warfare, as an exercise in information and systems control, threatens governments, groups and individuals.

This paper seeks to outline the challenges cyberspace and Information Warfare ("IW") pose to the traditional notion of force. First, the law of force, and its use by states, will be briefly outlined. Second, the pervasive and transnational nature of the electronic battlefield will be illustrated through definitions of IW. Finally, the public/private divide will be explored in an effort to test its strength and value on the electronic battlefield.

TRADITIONAL NOTIONS REVISITED

Since the *Treaty of Westphalia* in 1648, international law has been comprised of sovereign state actors who contract with one another through treaties of consensus. Sovereignty implies that a nation is not subject to the will of another, and that it is an independent actor in international relations.

Sovereign actors are prohibited from using force by the United Nations charter Article 2(4) qualified only by the right to self defence. In support of this prohibition, states' adversarial interaction is based on at least four assumptions. First, public international law is the law governing relations between states. Second, war, as regulated by public international law, is an adversarial exercise between states. Third, an actor engaging in war requires a strong national economy, industrial manufacturing capacity and a population from which to recruit a military force. Lastly, implicit in the first and third assumptions, non-state actors, groups, and individuals are not subject to public international law and are therefore not bound by its traditional notions.

In contrast, cyberspace is an electronic construct created by the interconnectivity of global communications systems and as such it has the power to overturn these fundamental assumptions. Through its multi-jurisdictional personality cyber-space facilitates the deconstruction of our highly structured and standardised society. Cyberspace can be differentiated from the international environment which constructed public international law because it lacks both boundaries and a physical presence and, as a result, cyber-citizens may maintain a sense of anonymity; reincarnating endlessly free of the confines of linear time. It is no longer necessary to measure aggression and military capability in arms and munitions. Cyberspace is responsible for introducing the individual to the

weaponry of information warfare through the personal computer.

WHAT IS INFORMATION WARFARE?

In order to understand the individualised nature of cyber-weaponry, it is necessary to understand what is meant by the term IW. Attempting to identify a comprehensive definition of IW, however, is not an easy task. Such a search may be in vain because of the ever changing nature and developing possibilities electronic interconnectivity present to society. In spite of this warning individuals, institutions and different branches of the United States military have created definitions of IW that reflect their own needs and perceptions. For example the Institute for the Advanced Study of Information Warfare ("**IASIW**") states that:

> *"Information warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries."*[1]

The advantage of the IASIW's definition is that it incorporates non-military interests as the subject of IW. It is the references to military or business adversaries that provide context for the words "offensive", "defensive" and "military", indicating that there might be an organisation behind IW activity. This is important since an organisational hierarchy would be able to provide operations, resources, and complex electronic systems through which to camouflage IW activities.

Alternatively, in more sweeping terms, IW has been said to be:

> *"The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/ restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives."*

This definition may be far too broad, and may also apply generally to social and political activity[2]. It also incorporates levels of organisation which could be labelled "strategic" or "tactical" which may not always be suitable when attempting to identify an information warrior. Perhaps a more fitting and inclusive notion of IW is the definition of Colonel Richard Szafranski USAF instructor at the American Airforce Air War College. Szafranski's definition illustrates the potential IW holds for individuals. He says:

> *"Information warfare is a form of conflict that attacks information systems directly as a means to attack adversary knowledge or beliefs. Information warfare can be prosecuted as a component of a larger and more comprehensive set of hostile activities –a netwar or cyberwar – or it can be undertaken as the sole form of hostile activity."*[3]

The Colonel has identified IW simply as a form of conflict which may or may not be an element of a larger tactical operation. He also demonstrates that IW is an umbrella term, incorporating *netwar* or *cyberwar* activities which may operate independently. Essentially, this definition does not explicitly apply to, nor does it exclude, an individual or group not aligned to any legitimate government or government agency. Evidence of this is the Colonel's examples of *netwar* and *cyberwar*. Although each involves a different use of technology and each aims to produce different outcomes, they are both defined in national or political terms.

Netwar has been defined as "information related conflict, at a grand level, between nations or societies"[4]. It involves disrupting what the target population knows or believes to know about the world. This includes psychological campaigns and propaganda, subversion and infiltration of electronic networks and databases, and efforts to promote dissident or opposition movements[5].

Cyberwar is less pervasive and focuses on supplementing military operations with information related to, and intended to facilitate, those operations[6]. The Gulf War, in much the same way as the current military operations in Kosovo, was an example of *Cyberwar*. Operations in the Gulf, including the destruction of Iraq's information systems and the application of information to reduce Allied consumption of capital and labour, were employed to immobilise Iraq's military leaders. Perhaps the greatest weakness of Szafranski's definition is its reliance on conflict. Conflict requires more than one party knowingly engaging in a struggle of opposing interests. In contrast, the demassification of society's information systems, brought about by cyberspace, negates the need for opposing parties.

Essentially, all of these definitions ignore the use of IW by individuals and groups as well as cyber-terrorists and cyber-extortionists. Even IW in the guise of *netwar* or *cyberwar* excludes the home office warrior. Clearly a new definition of IW is required that acknowledges the availability of IW weaponry to, and its use by, those individuals and groups not traditionally subject to international law.

BROADENING THE BATTLEFIELD

Cyber-terrorism is a creature of cyberspace and terrorists are currently active in extorting financial institutions. The cyber-terrorists use advanced techniques, often learned from the military, to threaten the integrity of banks and broking firms and demonstrate their ability to cause "computer meltdowns" to extort vast sums of money from the target institution. The funds demanded are transferred electronically into a remote account nominated by the terrorists only to be 'zapped' out moments later.

The weapons of IW have been described as "modern plagues" and include:

> *"The Logic Bomb"*: A coded device that may be detonated remotely. Once activated the "bomb" eats data and has the potential to destroy any electronic system including those systems that control rail, air, and road traffic.
>
> *"High emission radio frequency guns"*: This weapon "blows" an "electronic wind" through the target computer system.
>
> *"Viruses"*: the lowly virus has evolved to become ever more complex. They exist in many forms and may lay dormant depending upon their programme. A virus can be constructed with the capability to destroy an entire telephone communications system. Some virus bombs may be attached to an e-mail and, once inside the target system, begin writing over all disc application, data and communications files such as the recent Explore.zip and Melissa viruses.

Individuals are able to use this electronic arsenal against governments, governmental organisations, business, industry and other individuals. Hence, the meta-jurisdictional nature of

cyberspace and the nature of cyberweaponry merge physical theatres of war into one unique battlespace.

MERGING PUBLIC AND PRIVATE

Government and private agencies have considered the problems an electronic attack could present to an advanced information society. A hypothetical scenario included intermittent interruptions to the power grid, telephone line crashes, collisions of misinformed transporter trains, and "softwar" (the use of television broadcasting systems to publicise propaganda). Leaders in IW research were given fifty minutes to find a solution to the hypothetical havoc caused by the unidentified information warriors[7]. The value of this exercise is illustrated in the four main conclusions reached by the participants:

1. IW is inexpensive;
2. Cyberspace knows no geographic or theoretical boundaries such as national borders or the public / private divide;
3. Perception is easily manipulated in cyberspace and widely disseminated;
4. Cyberspace represents a battlefield with no discernible front line. Therefore analysts are not able to identify the origins of the attack.

An important message to come from this study is confirmation that cyberspace has circumvented international regulation and the rules of sovereignty.

To complicate matters, the 1995 G-7 conference generated eight core principles meant to guide the harmonisation and interoperability of information systems.[8]

These are:
- Promoting fair competition;
- Encouraging private investment;
- Defining an adaptable regulatory framework; and
- Providing open access to networks;

While:
- Ensuring universal provision of and access to services;
- Promoting equality of opportunity to the citizen;
- Promoting diversity of content, including cultural and linguistic diversity; and
- Recognising the necessity of worldwide cooperation with particular attention to less developed countries.

The means by which these principles are meant to apply to global information infrastructure are:

- Promotion of interconnectivity and interoperability;
- Developing global markets for networks, services and applications;
- Ensuring privacy and data security;
- Protecting intellectual property rights;
- Cooperating in R&D and in the development of new applications; and
- Monitoring the social and societal implications of the information society.

Conflict emerges when open networks and citizens' access are encouraged, yet intellectual property and privacy are protected by encryption or censorship, resulting in systems islands.

To facilitate interoperability at the governmental level municipal legislators may create regimes which include mandatory encryption or even demand that manufacturers include "trap doors" in their software enabling government agencies to observe electronic systems use. The difficulty arising from this exercise of governmental power is one of proportionality; is the loss of private rights, due to an exercise of parliamentary power, in proportion with legislative purpose? The borderless nature of cyberspace may exacerbate any imbalance by creating an unavoidable extraterritorial impact.

It is possible, however, that cyberspace may not be a common battlefield, but may be simply a conduit for the many forms of IW. Warring actors who are not operating under a common understanding of IW may never meet on a common battlefield. Assorted hacker attacks from various regions of cyberspace may rival terrorist attacks, but this activity may not necessarily be war if it lacks political motivation and purpose. Even so, hacker warfare is necessary, particularly if defensive, as it strengthens network security. In this way, non-public actors are held responsible for their own security and collectively create national security.

CONCLUSION

Cyberspace has, and continues to alter, the environment in which nation states communicate by making the means of international interactions available to individuals. While the Westphalian state-based system of international law remains preoccupied with sovereignty, individuals are creating a meta-jurisdictional electronic society. The difficulty exists in establishing a public international law regime which operates effectively in cyberspace. Although cyberspace may not necessarily be inimical to legal regulation, the absence of geopolitical boundaries and the lack of tangible manifestations of the information contained in cyberspace aid cybercitizens to elude detection and regulation. Further, the boundary-less nature of the Internet requires a new definition of what may constitute an act, or threat, of force.

Traditional notions of force, threats, and use of armed attacks, are defined with respect to physical manifestations, but in cyberspace the concern is the consequences of an attack rather than its nature. Traditionally minded members of the military do not believe warfare will become a video game without physical results, and any IW attacks without physical military backup may be only paper tigers. Even so, cyberspace remains a great equaliser through the deconstruction of social and legal boundaries. Inevitably, the redefinition of traditional notions of sovereignty and warfare will impose a new balance on the public/private divide. This new balance must include greater responsibility for individuals to participate in a growing electronic community. Failure to acknowledge individuals' access to cyberweaponry will inhibit the adoption of public international law rules in the electronic environment.

1 URL:http://www/pyscom.net/iwar.1.html

2 *Ibid*

3 "A Theory of Information Warfare: Preparing for 2020", URL: http/www/cdsar.af.mil/apj/szfran/html

4 J. Arquilla and D. Ronfeldt, "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict", URL: http://www.rand.org/publications/RRR/RRR/fall95.cyber/cyberwar.html

5 *Ibid*

6 *Ibid*

7 "Information Warfare: A Two Edged Sword" URL: http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html

8 "G-7 Ministerial Conference on the Information Society: Theme Paper" Brussels, 27 January 1995 URL: http://www.ispo.cec.be/g7/keydocs/themepap.html

Tanya Ross-Gadsden is an Associate at 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:

Jason Macarthur
c/- EMS Legal
61 Denison Street
BONDI JUNCTION 2022
Tel: +612 9387 2210
Fax: +612 9387 2230
Email:
jasonm.@ihug.com.au

OR

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 .....