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

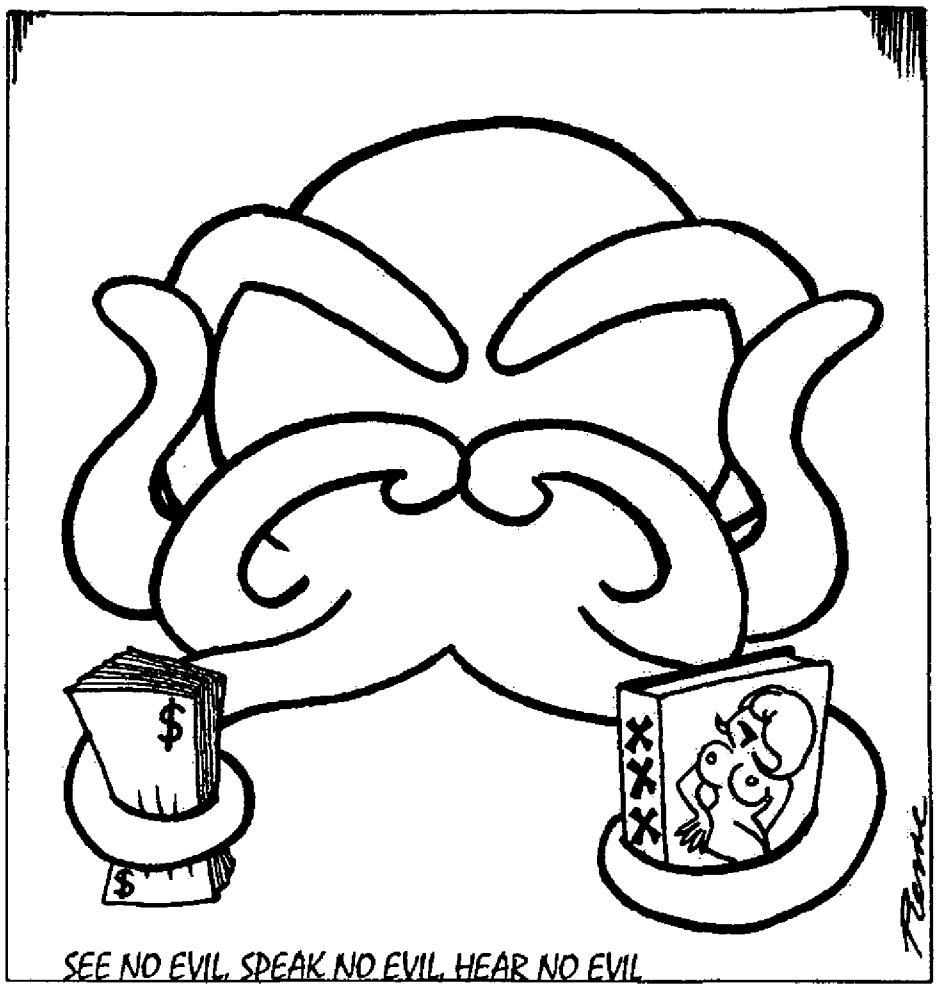
The Act excludes ordinary electronic email from the scope of Internet content which is to be regulated and limits its application to content accessed from a web site. It seems relatively easy for an ICH or ISP to buy IP addresses from other ISPs and send prohibited emails to users as a means of circumventing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