Communications LAW BULLETIN

THE OFFICIAL PUBLICATION OF THE COMMUNICATIONS AND MEDIA LAW ASSOCIATION INCORPORATED

Print Post Approved PP: 234093/00011 EDITED BY NIRANJAN ARASARATNAM Vol 19 No 1 2000

Internet Content Codes and the New Regime in Australia

The new millennium heralded the introduction of Internet censorship legislation in Australia. Peter Coroneous, Executive Director of the IIA, discusses the Internet Content Codes which will govern ISPs and content hosts.

On 16 December 1999, the Australian Broadcasting Authority ("**ABA**") approved three internet content codes of practice governing ISPs and internet content hosts[1]. These codes were developed by the Internet Industry Association ("**IIA**") as our response to the contentious *Broadcasting Services Amendment (Online Services) Act 1999* ("**Act**") passed in August 1999.[2]

For the purposes of context, the registered codes are in fact modules which will be incorporated into the more comprehensive IIA Internet Industry Code of Practice, which we are aiming to finalise in the first quarter of 2000. This broader code, draft 5.0 of which is accessible at www.iia.net.au/code.html, covers areas ranging from e-commerce, privacy, spamming, online sales and consumer protection, web development and other areas which the IIA has identified as priorities for a self regulatory industry response. In all cases, we have sought to set standards which reflect good corporate practice in the industry and to answer consumer concerns which appear to be impeding market growth.

Our objective generally is to ensure that workable self regulatory solutions will increase consumer confidence and help accelerate the use of e-commerce in Australia, but also stave off more heavy handed regulation by government. An assessment of our response to the present legislation, and an analysis of the likely effect on industry will probably show that in spite of the difficult circumstances we found ourselves in during mid-1999, the outcome is a good one for both industry and end users, and certainly the best available in the climate in which it was developed.

CONTENT CODES

To return to the content "codes" specifically, the Act provided for up to three codes to be developed, one for content hosts and two for ISPs. It also provided for the ABA, to make default standards for the industry where codes were not in place by 31 December 1999. Given the choice, we believed we were in a better position than the ABA to devise codes which would meet the tests of technical and commercial feasibility and also acceptance by industry, so we undertook to cover the field in the four short months that were available to us. The codes are not mandatory,[3] however the ABA can direct ISPs and internet content hosts to comply under threat of fines.[4] In this regard, they are not unlike the telecommunications codes which industry is developing, or the privacy codes which we expect to be developed once the relevant legislation passes this year.[5]

The new legislation was prescriptive in regard to some matters with which the codes had to deal, for example the provision of information to end users and minimum age limits for access account holders.[6] In other respects, we had latitude to be more creative owing to amendments to the legislation which we negotiated just prior to its Senate passage. We were, therefore, able to come up with solutions that we believe will advance the general objective of protecting children online, but without the risk of substantial damage to the ISP sector, which in some cases is quite fragile.[7]

ISP CODES

While space precludes an exhaustive analysis in this article, the approach within our **ISP codes** amounted to facilitating the empowerment of end users, who in turn could take more control

INSIDE THIS ISSUE

CONTENTS

over what was accessed, and at the point where control is best exercised – in the home. This in our view was a more workable approach to the default statutory alternative which would have applied without our intervention, namely the ABA requiring ISPs to take "reasonable steps" to prevent access by end users to prohibited content hosted overseas.[8] Accordingly, the second ISP code, mandates the provision of approved filter software to end users, other than exempted classes, and proscribes (as required by the Act) the issuing of access accounts to minors without parental consent. This squarely puts the onus back onto those responsible for children to ensure they do not have unrestricted access, and provides them with tools which they can activate, *if they so choose*, to block certain sites, or certain classes of internet sites.[9] ISPs are not required to absorb the cost of provision of filter software, but are instead at liberty to charge, or to give it away, as part of their marketing approach.

To date we have seen both options emerge, though competition in the market, both among ISPs and also suppliers of filter products, will keep prices to a minimum. Where a charge is levied at all, it is typically under $20 which is modest compared to access charges over a year. Except where a subscriber already has an approved filter installed or is a commercial customer behind an adequate network-level content firewall, ISPs are required to provide a filter "for use". While end users are not required to deploy it, we expect that most families will choose to do so. AOL reports that in the US, over 70% of their users choose to activate "parental controls" (which is essentially a user configurable content filter resident within the AOL browser and regularly updated by a content rating agency).

Under the IIA system, the suppliers of the approved filters,[10] and not the ISPs who merely distribute them, are required as a condition of approval, to accept updates from the ABA in respect of sites which the ABA has deemed prohibited as a result of complaints it has received. We expect that the installed user base will receive live updates transparently and on a regular basis, in the same way as anti-virus software updates are implemented. This ensures that the ABA is not acting in a vacuum, but is feeding into the process by which families are taking control.

The IIA solution, at least as far as ISPs are concerned, has removed any externally imposed form of censorship or obligation to monitor content, and replaced it with optional, but generally effective solutions which respect the right of Australians to determine for themselves what their families access online. As far as protecting adults from material which they might find offensive, the same solutions will be equally applicable. For them, it now becomes a case of "if thine eye offends thee, install a filter".

CONTENT HOSTING CODE

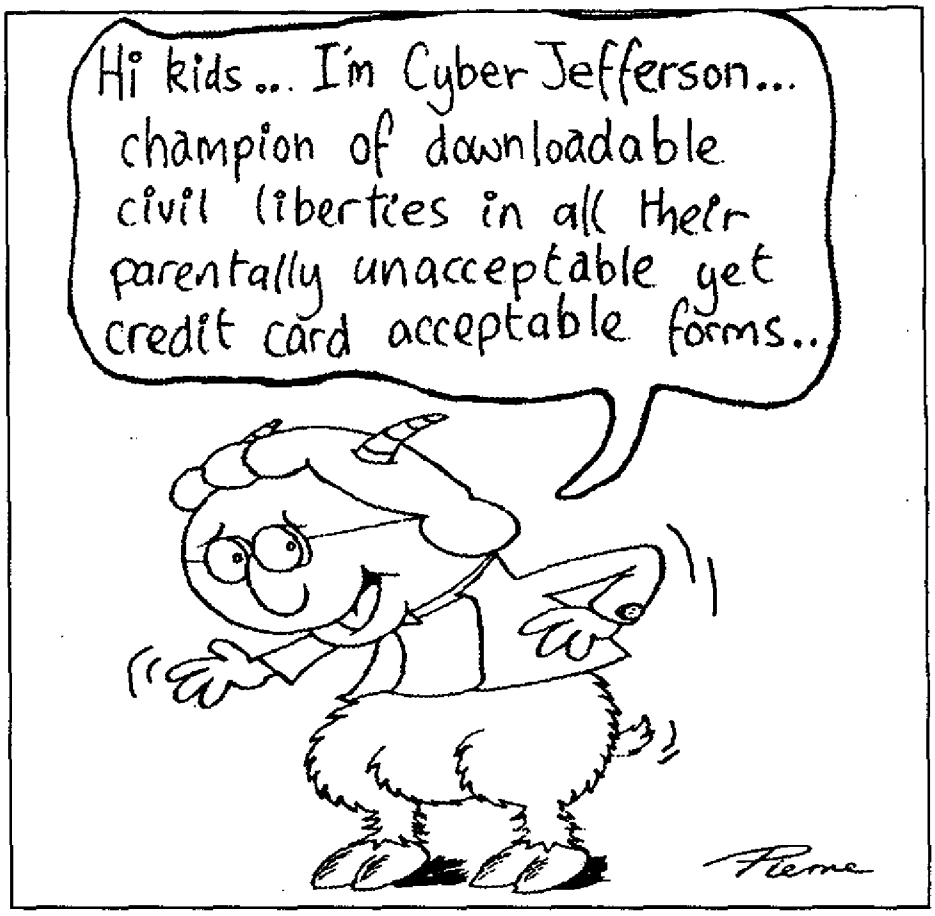
The content hosting code was subject to a requirement in the Act that content hosts remove prohibited or potential prohibited content which the ABA determined was hosted within Australia. Hosts are required to act by 6.00pm on the business day following the day in which the notice was issued. While the number of complaints which the ABA has received has been low, as we predicted it

would be, it has nevertheless issued several takedown notices, all of which have been complied with. While some sites have simply relocated offshore, again as we predicted, we anticipate that the level of takedown notices will remain low, partly because less than one percent of internet content hosted here is likely to be the subject of the regime, and partly because most commercial operators have now relocated their adult content to constitutionally protected US sites. In spite of this, we do not consider that moving all internet content to the US is warranted particularly since hosts are not expected to take pre-emptive action here, so that no liability arises unless and until formal notice is given. The ABA will, as a matter of course, detail the content in question and also provide the URL. Compliance for hosts is therefore likely to be a relatively easy task.

CONCLUSION

Some commentators have suggested that the continued presence of and accessibility to pornography on the internet is evidence that the new regime has failed. That would be a reasonable conclusion if the view were that the legislation was designed to eradicate access to all content which might be deemed offensive. But I doubt that even the Government believed that was the case, even though that was how the media portrayed the push. Certainly we all share the concern about what children might access on the internet, but it was never going to be the case that legislation in isolation was capable of reversing the risk. Nor will it solve problem gambling, bomb recipes, hate speech or whatever social evil the internet is blamed for in tomorrow's press.

Co-regulatory solutions are relatively new in global internet governance terms and Australia can rightly be said to be leading the field. Ironically perhaps, the legislation forced us to rethink our own strategies and the result may in fact be optimal, at least given present technologies. The content regulation debate has been characterised by highly charged and usually inaccurate assertions about the effect on free speech, network performance and industry survival. Many of those concerns may have been valid in a worst case scenario, and we were all justified in our protests against heavy handed solutions. However, we believe the alternative system now in place, when combined with education, remains the best way through this moving field of moving targets - the twenty first century communications environment.



1 See www.iia.net.au/code.html 'Version 6.0'

2 The Act amends the *Broadcasting Services Act 1992* (Cth).

3 IIA members in subscribing to the entire code once it is finalised, will of course be binding themselves to all relevant parts.

4 The legislation provides for court orders to suspend operations (clause 85 of Schedule 1 of the amending legislation), but is not envisaged that a situation would ever emerge where that would be invoked. It is nevertheless a draconian sanction and one which we believe is unwarranted.

5 The combination of industry developed rules underpinned by enforcement by an independent statutory authority has come to be known as 'co-regulation', and is in our view a model well suited to internet governance.

6 See clause 60 of Schedule 1 of the Act which lists the matters with which industry codes must deal.

7 Competition in the sector has reduced some ISPs to quite marginal economic operations. In our view the consolidation which has already occurred will accelerate, but we did not want the legislation, or indeed our intervention, to hasten the demise of numerous small Australian businesses.

8 "Prohibited content" domestically refers to content which is rated R (where there is no age verification for access), X or Refused Classification (RC). For content hosted overseas, R rated content is permissible whether or not behind an age barrier. "Potential prohibited content" is content that would likely be deemed prohibited if the material were so classified by the Office of Film and Literature Classification ("OFLC"). Directions from the ABA in respect of this category are generally interim under the regime, pending classification of the content.

9 The Act catches web based content and content stored within newsgroups, but not ordinary email or material which is streamed live over the internet.

10 The Schedule to the present content codes lists 16 approved filters. The list is intended to expand over time as more options are developed and presented to the IIA for inclusion. The initial "batch" were included as a result of an examination of available options by the CSIRO in November 1999. The new community advisory body, NetAlert, which has funding for education and to operate a parent information helpline will presumably resource future evaluations of software filters. It should also be noted that some approved filters are server level filters, designed for optional provision to those end users who lack the skills or confidence to install client end filters at home.

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