Particularly Children: A Qualitative Evaluation of the Effectiveness of Australia's Internet Censorship Regulations

Orren Prunckun[†]

Abstract

This study evaluates the Australian *Broadcasting Services Amendment (Online Services) Act, 1999 (Cth)* — its intent, its purpose and its practical implementation — as to how effective it is in protecting children. Background data was collected from published Government reports and qualitative data was collected through interviews with a number of Internet Service Providers and Internet Content Hosts. The findings suggest that the legislation is not effective in controlling online content. Industry opinion confirmed that the Act was passive and only had an active component when a complaint was made. Further, the interviewees corroborated the view of some Internet security analysts that the World Wide Web is dynamic and continually changing. If correct, the ramifications of such rapid changes are that a more effective, long-term solution could lie in educating children and their parents about the Internet, and not relying purely on a technical or legislative response.

Context and Intention of the Legislation

The purpose of the *Broadcasting Services Amendment (Online Services) Act, 1999 (Cth)* (BSA) is to provide a mechanism for controlling access to material on the Internet. The BSA was intended to protect society's vulnerable from accessing offensive material that appears regularly online. It was the view of the Federal Parliament that children are less likely to be able to make decisions about what is appropriate Internet content without external guidance. As Rod Nockles, corporate spokesman for the Commonwealth Government's NetAlert recently said: "…the most worrying issue with internet safety at present is students accessing inappropriate content — written or visual." (Gravis, 2006: 27) Whether that access is accidental or willful, the Act was brought about in the interest of protecting minors.

According to Senator The Hon Helen Coonan, Minister for Telecommunications, Information Technology and the Arts, in her National

[†] Address for correspondence: Orren Prunckun, BA, LLB, Adelaide, South Australia, E-mail: orrenp@hotmail.com

Press Club address of 14 June 2006, the BSA was intended "…to help protect Australian families. [T]he Government has committed to doing everything reasonably possible to ensure that all Australians — particularly children — are safe on the Internet." (Coonan, 2006) The amendments were intended "…to provide a means for addressing complaints about certain Internet content; and to restrict access to certain Internet content that is likely to cause offence to a reasonable adult; and to protect children from exposure to Internet content that is unsuitable for children." (CoA, 1999: 3(1)(k),(l),(m))

Although Internet regulation in Australia can be traced back over a decade, it recently culminated with campaigns by the likes of Tasmanian Liberal Senator, Guy Barnett. Senator Barnett pushed hard for censorship of the Internet in November 2005. (Barnett, 2005; Refused Classification, 2006; and The Age, 2005) The result of such campaigns was that legislation has been enacted.

Focus of the Research

This study explores the question of whether Australian Internet censorship regulations are effective. It looks specifically at the Commonwealth Government's attempt to censor Internet material that is deemed "unsuitable for children." (CoA, 1999: 3(1)(k),(l),(m)) through the *Broadcasting Services Amendment (Online Services) Act, 1999 (Cth)*.

Modus Operandi of the Legislation

The BSA, and the complementary *Classification (Publications, Films and Computer Games) Act, 1995 (Cth)* (CoA, 1995), are the two most relevant statutes for Internet regulation in Australia. The BSA is not concerned with the actions of Internet users (i.e. consumers) or content creators.[1] Under Schedule 5, the BSA places this burden on Internet Content Hosts (ICHs) and Internet Service Providers (ISPs). The BSA allows the Australian Communications and Media Authority[2] (ACMA) to examine Internet material but only on a complaints basis. It attempts to censor refused and restricted classification online material which has been defined so under the guidelines for film and video — the *Classification Act*. Both Acts are administered through regulatory agencies.

These guidelines state that if content is hosted in Australia, the ACMA is empowered to issue a "takedown notice" requiring the prohibited material to be removed from the web site (in the case of an ICH) or block users from accessing the content (in the case of an ISP). If the criticised web site is hosted outside of Australia, the site is added to a list of banned sites. This list is then added to commercially produced filtering software, which must be offered to all consumers by their ISPs. (ABA, 2006: 43)

But how effective is this legislation? Does it achieve the outcome the Parliament intended? Specifically, does it "…ensure that all Australians — particularly children — are safe on the Internet." (Coonan, 2006)

Research Question

In order to gauge the effectiveness of Australia's Internet censorship regulations, the provisions of the *Broadcasting Services Amendment (Online Services) Act, 1999 (Cth)* will be considered through industry opinion as to whether the legislation achieved its goal of removing sites that have been criticised, and to what extent these actions protected children.

Method of Collection

Although the ACMA did not released an annual report for 2005–06 at the time of this study, the statistical data was collected from the annual report of the Australian Broadcasting Authority (ABA) for 2004–05 (ABA is now part of the ACMA) to set the background for the qualitative exploration that followed.[3] The study then gathered qualitative data from practitioners in the field of Internet service provision and content hosting. Several ISPs and ICHs were interviewed to provide rich contextual information in order to investigate these socio-legal phenomena. In doing this, a non-probability sampling frame was selected for two reasons: 1) the conclusions being drawn would not represent a particular population; and, 2) no statistical test of significance would be used. (Monette, et al., 1990: 150–152) However, this approach was particularly attractive as it allowed the variables to be examined in the natural setting in which they occur. Therefore, a convenient sample of ISPs/ICHs was used. (Vito, et al., 1988: 125)

The researcher contacted twenty-four South Australian and interstate ISPs/ICHs with a series of questions designed to gauge their views on the effectiveness of the legislation. Of this number, four agreed to be interviewed, one declined, and the remaining nineteen did not respond at all. Although the sample of four could be seen as limited, there are compelling reasons to note these responses, in particular, because these ISPs/ICHs represented an important market share of Australian Internet users and/or hosted many high-profile, well trafficked commercial web sites. In addition, the fact that there were so many non-responses, in the end, proved insightful in itself as the ISPs/ICHs which consented to interview offered their interpretation of why their colleagues might not have participated in the research. This added further depth to these practitioners' perceptions of these dynamic phenomena.

Findings

The Australian Broadcasting Authority's Perspective

According to the ABA *Annual Report*, the legislation is "output" based rather than "outcome" based. The *Annual Report* stated that there was no measure of censorship effectiveness. In other words, the report provides only statistics of actions taken by the regulator. There was no "impact review" which demonstrated the effectiveness of the online content scheme. (ABA, 2006: 67)

Nevertheless, the ABA charted the number of notices of complaint, investigations and takedown notices for questionable Internet content. In 2004–05, there were 1,145 complaints and 814 investigations (43 from the previous year and 23 carried through to 2005–06). Some of those investigations included multiple web sites, which constituted more alleged prohibited content. There were 149 invalid claims, 212 terminated claims (based on lack of information), and 905 items prohibited. Forty-eight take down notices were issued for Australian ICH and 875 of the 905 items were referred to manufactures of software filtering for sites hosted outside Australia. (ABA, 2006: 56–57)

The report only discussed takedown notices and referrals. The statistics did not account for the vast amount of prohibited online material that had not been brought to the Authority's attention. That is to say, just because a complaint was not lodged does not mean there was no inappropriate material. As only a fraction of complaints have resulted in takedown notices — this could indicate either reluctance or a disinterest in pursuing enforcement by the public.

Not only did the ABA initiate investigations and issue takedown notices, it implemented a code of practice for ISPs and ICHs. For instance, ICHs were banned from hosting pedophilic material. (ABA, 2006: 43) The code required ISPs to have "Internet safety" pages available to users. (ABA, 2006: 2) The code also called for education initiatives such Cybersmart Kids (Cybersmart Kids Online, 2006) and Net Detectives (Alston, 2003) aimed at school students to teach Internet safety. The ABA stated in its *Annual Report* that it intended to enforce compliance with the code of practice. Only 20 percent of the ISPs and ICHs that were audited were reported to have failed the audit (but as a result of the audit, they subsequently made the necessary changes). (ABA, 2006: 58) This indicates a very high rate of compliance with the code.

Because the ABA only measures efficiency (i.e. output) not effectiveness (i.e. outcome), it appears the figures published in the *Annual Report* can only demonstrate that the agency was *efficient* in how it went about protecting children. However, in terms of *effectiveness*, there was no way it could demonstrate this. Hence the research here: Does the law actually provide Internet protection — particularly to children?

From the Perspective of ISPs and ICHs

The ISPs and ICHs interviewed stated that they were not required to implement any specific counter-measures under the Act. This is consistent with the legislation's intent — a complaint based system. In fact, one ICH said that prior to their interview with the researcher, they were not aware of the existence of the Act, nor what its purpose was. Having said this, they took the commonsense stance that they would not host inappropriate material anyway. Preventing unsavory material from being hosted was part of being a good corporate citizen, they said. Their hosting guidelines were purely internal and were driven by business policy rather than legislation. According to all of the interviewees, the Act did not change their commercial practices.

One ICH said it hosted a site which has some material (i.e. text but not graphics) which might be interpreted as being unsuitable for children. In an abundance of caution, the site owner installed a "pop up box" that carries a warning about the content in order to protect young people prior to viewing. This interviewee said these types of safeguards were the most sensible approach that ICHs could take. Implementing these kinds of safeguards have no doubt gone a long way towards saving those interviewed from receiving complaints, or being issued with a takedown notice.

One interviewee said that content could be added (i.e. uploaded) by Internet users without restraint. However, this host routinely moderated all new additions within 24 hours of it appearing on the web site. This practice allowed for the possibility that some uploads could be unsuitable, and if so, would be removed by the ISP (no negotiation would be entered into with the person posting the material as this was a condition of use set by the host). The interviewee explained that if content was moderated *prior* to posting, or needed *prior* approval, no content would be added and they would rapidly lose business. They said they had to play a balancing game in this regard.

The interviewees claimed that the requirements of the legislation were ineffective because the regulating agency (i.e. ABA/ACMA) had failed to notify them of the Act's obligations. They thought the legislative changes should have been posted as public notices similar to when road rules change. They were unanimous in saying that none had received information about their obligations regarding unsolicited messages called "spam." (Wikipedia, 2006)

The interviewees claimed that prohibited content is still accessible despite the legislation being enacted and the filtering of sites. They said that the legislation could be seen as "political window dressing" in that content is simply shifted to web servers offshore.

The interviewees all said monitoring user's activities was not guaranteed. Although filtering software such as NetNanny® (NetNanny, 2006) is offered to consumers, they are not required to install it. According to a report by McCrea, et al. (1998: 40–41) of Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO), for filtering to work, it needs to start at the ISP level by banning sites with a "blanket" approach. Relying on consumers is not effective they said. Also, filtering software is discretionary, which means users will self-select what they view.

Therefore, filtering software is not a realistic solution and cannot control content, especially if content is hosted outside Australia. As the legislation only applies to Australian ISPs and ICHs, hosting a server in another country provides a safe haven from the reach of Australian laws. This raises jurisdictional problems for any investigation and prohibits prosecution. In order to bring about effective censorship of offensive material it would need identical laws across *all* jurisdictions *worldwide*. Not a likely occurrence. (McCrea, et al., 1998: 41)

Interviewees said that there was no realistic technical solution besides the ones advanced by McCrea, et al. (1998) in their publication *Blocking Content on the Internet: A Technical Perspective*. This report states that censorship is possible, but not effective in blocking content hosted outside of Australia. McCrea, et al. (1998) explain that this can be done by two methods — packet-level blocking and application-level blocking. Nevertheless, the CSIRO report was of the view that a web site owner could work out ways around these counter-measures as quickly as they are implemented. (McCrea, et al., 1998: 40)

The authors of the report said that parents often use filtering software as their *only* approach to Internet safety, when they should be involving themselves through supervision. Children need some form of guidance as their youth prevents them from making sound judgments on their own (as well as teenagers and some young adults). But the dilemma is that it is not possible to supervise their activities all the time, therefore it is difficult to guarantee that children will not access inappropriate Internet content. Ultimately, such software may give parents a false sense of security.

One interviewee discussed *Shockwave* (Adobe, 2006) media viewing software as a specific example. They said that the software only detects text. If, however, the text message is written into an image file it will evade detection. Moreover, "streaming" audio and video media is able to bypass most conventional methods of censoring. The ability to censor this media needs to

be highly sophisticated. The interviewees were not aware of any products on the market that could do this.

All interviewees suggested practical behavioral measures as the most effective counter-measure — such as education in conjunction with a technology-based censorship regime. They said that censorship alone will not moderate content — the only way was in combination with education, or education in the guise of "entertainment" (which is better received by children). They suggested a two-pronged approach — target school-aged children and their parents (/grandparents). Parents need to be provided with information on how the Internet works and what their responsibilities are toward their children.

Of the businesses that declined to respond to the researcher's request, or did not respond at all, three explanations were presented by the interviewees: 1) the lack of response could be due to an excessive workload with the businesses placing the researcher's request in the low priority tray (after all, there was no business prospect coming from the query); 2) their non-response may suggest that the ISPs were unaware of the Act, or they had business interests they wanted to protect. Perhaps they did not want to bring further attention to their businesses, which in turn, may have brought unwarranted audits or media attention; and, 3) it could simply be that these ISPs and ICHs were complying with the legislation. However, if this latter explanation was the case, it would have been thought that they would have replied as such.

Discussion and Conclusions

The responses of these ISPs/ICHs lead one to conclude that the legislation is not very effective. It can also be concluded that neither are other methods of Internet censorship. As an illustration, it is virtually impossible to confiscate web-based material due to nature of medium and the construction of the Internet. An infinite amount of copies can be made of content, with minimal cost for onward distribution. (Lim, 2002: 45) In addition, digital media does not degrade like analogue or print material and it can last "forever" and re-emerge on a web site(s) years hence.

Some restrictions placed on children are effective in the physical world but are useless in cyber space. For example, alcohol, cigarette, and gambling laws seem to be effective. Yet the Internet can be bypassed and there is little or no mechanism to check who is accessing information, and little ability to enforce breaches (if they can be detected).

Insofar as the regulations may have been intended to protect children, industry opinion suggests that this has been a failure — only a small fraction of

complaints have resulted in takedown notices. Material can easily be shunted offshore if and when a complaint is made. If the web site is added to a list of banned sites through filtering software, there is no provision that requires users to install the programs (or use them if installed), or oblige in self-censorship. This system makes censoring material online difficult if not impossible.

Finally, an unintended consequence of the legislation is that it inhibits freedom of expression and borders on outright censorship. (ALIA, 2006; Jones, 2000) Even so, it seems that laws such as the BSA attempt to strike a balance between preserving freedom of speech and censoring undesirable material that is likely to harm to people in society who are yet to be able to make judgments as to its intellectual worth. In these cases, it would be hard to argue that levelheaded censoring would be detrimental to society. Surely, the important community goal is to protect children rather than on un-vetted speech. It is a "balancing game," as one ISP put it, between enforcement and the real issue: children's psychological health and well-being. However, the legislation appears to provide moderation in terms of censorship to preserve free speech and is efficient in censoring criticised content. But it is also acknowledged that it fails to effect *complete* protection for children.

Endnotes

1. A content provider is someone that provides content to an Internet Content Host.
2. The Australian Broadcasting Authority and the Australian Communications Authority combined to form the Australian Communications Media Authority (ACMA).
3. The Australian Communications Media Authority's annual report for 2005–2006 had not been published at the time of this writing.

References

Adobe (2006). *Shockwave Player*. Available at: http://www.adobe.com/products/shockwaveplayer/ Accessed 13 February 2007.

Australian Broadcasting Authority (2006). *Annual Report 2004–2005*. Canberra: Australian Broadcasting Authority.

Australian Library and Information Association (2006). *Analysis of the Broadcasting Services Amendment (Online Services) Act 1999*. Available at: http://archive.alia.org.au/publishing/bsa/legislation.html Accessed 13 February 2007.

Commonwealth of Australia (1999). *Broadcasting Services Amendment (Online Services) Act 1999 (Cth)*. Canberra: Commonwealth Government Printer.

Commonwealth of Australia (1995). *Classification (Publications, Films and Computer Games) Act, 1995 (Cth)*. Canberra: Commonwealth Government Printer.

Coonan, The Hon Helen (2006). *Protecting Families Online: Address to the National Press Club 14 June 2006*. Available at: http://www.iia.net.au/index.php?option=com_content&task=view&id=480&Itemid=32 Accessed 13 February 2007.

McCrea, Philip; Smart, Bob; and Andrews, Mark (1998). *Blocking Content on the Internet: A Technical Perspective.* Sydney: CSIRO Mathematical and Information Sciences, June

Cybersmart Kids Online (2006). *Smart Net Surfing for Kids and Their Grownups*. Available at http://www.cybersmartkids.com.au/ Accessed 13 February 2007.

Monette, Duane; Sullivan, Thomas; and DeJong, Cornell (1990). *Applied Social Research: Tool for the Social Services, second edition*. Fort Worth: Holt, Rinehart and Winston, Inc.

Garvis, Sarah, reporter (2006). "Safety Net" in *Advertiser*. Adelaide, 17 October.

Vito, Gennaro; Latessa, Edward; and Wilson, Deborah (1988). *Introduction to Criminal Justice Research*. Springfield, Illinois: Charles C Thomas.

Jones, Melinda (2000). "Free Speech and the 'Village Idiot'" *University of New South Wales Law Journal Forum* Volume 6, Number 1. Available at: http://www.austlii.edu.au/au/journals/UNSWLJ/2000/11.html Accessed 15 February 2007.

Alston, Richard (2003). *Speech by Senator the Hon Richard Alston, Minister for Communications, Information Technology and the Arts, Launch of Net Detectives, Thursday 25 September 2003, International Grammar School, Ultimo, Sydney*. Available at http://www.dcita.gov.au/Article/0,,0_4-2_4008-4_116887,00.html Access ed 13 February 2007

NetNanny (2006). *Keeping Your Kids Safe on the Internet*. Available at: http://www.netnanny.com/ Accessed 13 February 2007.

Refused Classification (2006). *Internet Censorship in Australia: January – December 2005* Available at: http://www.refused-classification.com/internet_05-01to12.htm Accessed 13 February 2007.

Barnett, Senator Guy (2005). *Ban Access to Porn and Extreme Violence on the Internet*. Australian Christian Lobby. Available at: http://www.acl.org.au/national/browse.stw?article_id=6422. Accessed 13 February 2007.

The Age (2005). "Keeping Kids from Nasties on the Net," in *The Age* Avaiable at:

http://www.theage.com.au/articles/2005/12/07/1133829659783.html?from=top5 Accessed 13 February 2007.

Lim, Yee Fen (2007). *Cyberspace Law: Commentaries and Materials, second edition*. New York: Oxford University Press.

Wikipedia (2006). *E-mail Spam.* Available at: http://en.wikipedia.org/wiki/Spam_%28email%29 Accessed 13 February 2007.