



Submission to the Review of Schedule 5 to the Broadcasting Services Act

Convergent Communications Research Group¹

November 8, 2002

Introduction

This submission responds to a request from the DCITA for comment on a review of the operation of Schedule 5 to the Broadcasting Services Act 1992. It adopts the format and headers from the issues paper provided by DCITA in September 2002.

The Convergent Communications Research Group (CCRG) at the University of Adelaide can offer a distinctive view on these matters. The Group brings together academics and industry experts from telecommunications, media, legal and economic backgrounds to deal with the regulatory and commercial challenges which arise with convergence of the communications and content industries. Our group provides the broad perspective we see as essential in responding to this review.

General

Internet regulation is a relatively recent initiative. The rapid evolution of Internet communications has meant that few could foresee its impact and even fewer have accurately predicted its trends. It is not surprising that existing regulation could not address Internet communications, nor that measures hastily put in place to address the regulatory gap continue to show signs of strain.

It is safe to assume that regulatory schemes adopted now, unless cognisant of what is coming, will be no more effective in a few years' time than past regulatory schemes are today.

¹ Contacts for correspondence:

Mr Peter Ramsey, Senior Adviser, Regulation. pramsey@eleceng.adelaide.edu.au

Mr Robert Chalmers, Senior Adviser, Law. robert.chalmers@adelaide.edu.au

Submission to the Review of Schedule 5 of the Broadcasting Services Act

Any new Internet regulatory scheme must be able to respond flexibly and rapidly to future developments or risk being stranded amongst the shoals of irrelevance. This requires that a convergence perspective be adopted so that possible regulatory regimes can be tested against conceivable future developments.

A study of communications convergence is really an exercise in future-thinking. Convergence is driven in large part by the universal technology inherent in digitisation. It immediately opens new vistas for the integration and delivery of content, the coming together of many art forms, and the necessity to extend consistent regulatory coverage over what have traditionally been viewed as separate activities (telecommunications, radio broadcasting, TV broadcasting, cinema, datacasting, internet)

In framing our response, we draw in part on the two recent works on the topic of Internet Regulation by our members. These are Robert Chalmers' "Regulating the Net in Australia: firing blanks or silver bullets" [1] and Dr Paul Chapman et al's "Media Streaming and Broadband in Australia" [2] which was commissioned by the Australian Broadcasting Authority at the beginning of 2002.

As a general comment, we agree with the principle that some form of regulation is in order and we are happy to support aspects of the legislation where appropriate. Where we cannot, we have tried to be constructive in our criticism while offering concrete suggestions.

However, we recognise that any method of regulation based on particular technical solution is bound to become ineffective as it is overtaken by further advances. This implies that regulation must be built on a technology-neutral foundation to provide any lasting solution. We therefore fully support those initiatives which are based on consumer education and assisting those whose responsibility it is to guard the interests of the most vulnerable.

Discussion

Comment is sought on the complaints process and outcomes, and the referrals of 'sufficiently serious' content to the relevant police authorities.

It is clear that the vast majority of complaints relate to material that is hosted off shore. This content is outside the jurisdiction of Australian authorities and there is no possible response other than referral to police and inclusion in filter lists – there is no ability to directly "take down" offensive material hosted offshore. This is a fundamental weakness in the regulatory regime, especially as some content providers deliberately move off shore to supply such material.

In our view, the only logical response is to attempt to coordinate the activities of regulators and interest groups across a number of countries. But, as with most international cooperation and coordination, progress is generally slow. As with all global treaties, a number of countries must champion the issue and Australia could play such a role. We would anticipate that support would come from many OECD countries and, particularly, from China as well.

Submission to the Review of Schedule 5 of the Broadcasting Services Act

Comment is sought generally on the performance of the complaints process.

It seems clear that the complaints process has not resulted in any diminution of offensive material on the Internet. It relies on the vigilance of users to recognise unsuitable content, and follow through with a complaint for each and every instance. In comparison, film censorship is more effective because it is dealing with a much more limited distribution and screening system which is vastly easier to control.

In the case of Internet there is no clearinghouse between the producers of content and its mass distribution. Therefore the censorship function must be placed squarely in the hands of the users - which fundamentally means the parents and guardians of children. They must be easily able to access the tools to take immediate action to handle unsuitable content as they see fit, and this points to the need for education and public awareness campaigns.

Comment is sought on the scope of Internet content that is addressed under Schedule 5. Note that this request for comment is not intended to encompass the issues addressed by the OFLC's guidelines review.

We see particular difficulty in the scope of controlled content including R rated material where access is not protected by an effective adult verification mechanism.

Firstly, the inclusion of R rated material is highly problematic because R ratings may be assigned for reasons other than covering potentially inherently offensive material such as pornography. It may also include material that has been so classified because it deals with "adult themes" (ie including non sexual material such as suicide, crime, corruption, marital problems, emotional trauma, drug and alcohol dependency, death and serious illness, racism and religious issues). This raises significant difficulties for "legitimate" content providers whose material deals with such issues.

Being a research group, the CCRG also has concerns about restricted access to material for legitimate purposes such as research and education. One of our members teaches a multi-media course but is unable to include study of important pornographic sites because of these restrictions.

Secondly, there is at present no sound means of adult verification. If such a system relies on credit card numbers then it is easily defeated once such numbers are obtained (either "legitimately" or using numbers available from the Internet). Similarly the other measures mentioned in the Restricted Access Systems Declaration 1999 (No. 1) are can be defeated by means of false ID or digital signature, or through acquisition of inadequately secured PIN code details. This is just one instance of a broader systemic problem that potentially affects any e-commerce system – lack of trusted infrastructure and identification/authentication measures. These are complicated problems that will be extremely difficult to resolve in the short to medium term. [3]

Submission to the Review of Schedule 5 of the Broadcasting Services Act

Comment is sought on the operation of the codes, in particular the ‘designated notification scheme’ under code 2, the scheduled filters and the designated alternative access-prevention arrangements.

The designated notification scheme relies on the ABA notifying ISPs and filter suppliers in relation to prohibited or potentially prohibited content. The responsibility of the ISP is to offer filter software and the filter software supplier to include relevant filtering in their latest offering.

Filters can be both over and under inclusive, as has been amply demonstrated by numerous enquiries locally and internationally [4]. Filtering is a very difficult task. It is not simply a matter of raw computation but often requires value judgements and in practice is aimed as much at banner advertising as offensive conduct². Filters can also be easily bypassed. However, they are a self help measure, and as such do provide some assistance to those who are grappling with content exclusion at the coal-face.

It is worth noting that while most businesses and many consumer users of the Internet consider virus filtering to be an essential part of the on-line toolkit, web content filtering is much less widespread.

Comment is sought on the level of responsibility taken by industry under the Schedule 5.

The IIA and related industry players have co-operated with the co-regulatory approach despite reservations, and this has occurred at significant cost. The cost of filter provision and compliance has a major impact particularly on smaller ISPs and has been blamed (in part) for driving industry rationalisation.

However, we support the emphasis in this case on co-regulation – that is the task is not driven by black letter law but rather by the industry attempting to meet the legitimate interests of the legislators in providing a workable system of regulation.

Comments are sought generally on the co-regulatory approach established by Schedule 5 to the Act, including the Internet industry codes of practice and whether the registered codes have operated to provide adequate community safeguards.

Clearly it has not been possible to provide “adequate community safeguards” if by that it is intended that there be robust screening of Internet material for offensive content. However we recognise that this is an exceedingly difficult task with the present regulatory stance only partially successful.

² For example, the University of Adelaide’s standard web filter disallows access to part of the Australian Broadcasting Authority’s web site <http://www.aba.gov.au/tv/content/codes/commercial/index.htm> on the basis of the word “commercial” in the address.

Submission to the Review of Schedule 5 of the Broadcasting Services Act

Comments are also sought on compliance costs and related issues associated with the Online Content Co-Regulatory Scheme.

The cost for classification of just one web page by the OFLC is \$510. This is clearly prohibitively expensive, noting especially that content on the Internet is updated very frequently.

Comments are sought

- **on the industry's obligations and activities with regard to community education.**
- **on the role and activities of the ABA with regard to community education.**
- **on the role and activities of NetAlert with regard to community education.**
- **generally on community education under the Online Content Co-Regulatory Scheme.**

We believe that the flow of global Internet content is currently only controllable by limiting access to the computer. This will come as no surprise to parents who have had to confront earlier technical advances such as telephone and TV by the same method.

Education of the community is absolutely central to any successful regime and Australia must engage its citizens in public debate on the impact of Internet technology on community life. We judge that neither the industry, the ABA nor NetAlert have captured the public imagination in any meaningful way to achieve this.

Comment is sought on the effectiveness of referrals of overseas-hosted material to the AFP and to certain Internet complaints hotlines.

While we believe it is wholly appropriate to provide an avenue for such complaints, it is difficult to judge their effectiveness due to the prohibition of any information identifying inappropriate content.

Comments are sought on the role and functions of international cooperation under the Online Content Co-Regulatory Scheme and, in particular, the international liaison activities undertaken by the ABA and NetAlert in this regard.

Comments are also sought on international best practice models and developments and trends in international Internet content regulation.

International developments are set out in some detail in Robert Chalmers' study [1]. Key elements are included here directly quoted from that study.

“Some hope that self-rating and filtering systems will give users choice and offer a means of protection. Such systems rely on voluntary self-labelling of content according to certain standards, which can be automatically picked up by a properly configured Internet browser, which can then screen access to content which is outside of the user set preferences. The concept for child protection purposes is then that adults can set password protected preferences

Submission to the Review of Schedule 5 of the Broadcasting Services Act

for child access - presuming the adult has the requisite skill! However only a tiny portion of content accessible on the Internet has been PICS rated and this is a voluntary self rating system in any event, which could be readily abused.

“The US Child Online Protection Act (COPA) Commission was established to consider strategies for ensuring the safety of children using the Internet. It reported on 23 October 2000, and advocated renewed efforts at education, "user empowerment", and enforcement of existing laws, rather than new legislation.”

Comment is sought on the development of Internet content filtering technologies and whether they have developed to a point where it would be feasible to filter R-rated information hosted overseas that is not subject to a restricted access system.

Comment is sought on the provision of Internet content filtering services under the Scheme.

We have no illusions about the effectiveness of filter technology. Where site information is well known and stable, filters would be effective. However in the real world this is not the case. Web addresses are continually changing and morphing into other sites and, by their very nature, filters will always be in catch-up mode and therefore inherently ineffective. Any attempts to provide real-time censorship based on words, picture recognition etc will also fail, while also cutting across legitimate uses and introducing significant processing delay. In addition, ordinary consumers are in a very weak position to maintain or modify such systems.

Comment is sought on the application of the Schedule to live-streamed Internet content.

Earlier in the year we prepared a report for the ABA titled Media Streaming and Broadband in Australia which was presented at the ABA's second annual conference in April 2002. The report dealt specifically with broadcasting services regulation and in particular with the treatment of online material.

Pivotal to this regulatory regime is whether the material is accessed from storage or not. It appears that only stored content is regulated under Schedule 5. This distinction was initially drawn to avoid the inclusion of personal communication via chat rooms, email and technology such as IP telephony in the regulatory regime.

It could be argued that buffering, an essential part of the streaming process, is a form of storage. On the other hand, the purpose of buffering is to enhance the quality of streamed media and buffered content is erased once it has been displayed. It is an ephemeral storage system and is not intended for later retrieval.

The question of stored content is likely based on a philosophical need to avoid regulation of communications which are of a personal nature (such as voice over IP). However more practically, live content is ephemeral and if such content were offensive, it might be impossible to take action concerning it as there may be no residual evidence to prove that it was offensive.

Submission to the Review of Schedule 5 of the Broadcasting Services Act

Despite this loophole, we also note that live streamed material is a minor component compared to the much greater quantity of stored and potentially offensive material. This means that while it is proper to attempt to include live streamed Internet content within the regulatory regime, preferably through a more technology-neutral approach, at present there does not appear to be any pressing need to do so.

Comment is sought on the application of the Online Content Co-Regulatory Scheme to offensive spam.

Currently emails are excluded from the regulatory system. Offensive spam is a problem but it is hard to see how the Schedule 5 arrangements would do anything meaningful to address it. The NOIE report [5] makes it clear that new legal measures will not provide a “silver bullet” solution to this problem.

In future it is likely that some email domains will be strictly limited to receive only from certain addresses. Users may well operate several addresses and regularly close down those which become spam clogged.

Comment is sought on the potential impact that convergent devices may have on the operation of Schedule 5 to the Act.

We are of the opinion that technological advances (including convergence tunnelling, encryption, anonymising/privacy software and services) will always frustrate any system of regulation based on technical fixes. For example, filtering by its very nature will always be a catch-up regulatory method. Constant technological shifts will always conspire to outpace any system, spurred on by a natural inclination of “hackers” to focus their attention on any such restrictive practices.

A couple of illustrations may place this argument in context:

- Schedule 5 uses the terms “On-line” and “Internet” interchangeably. However, some content, such as that on AOL’s walled garden, is “on-line” but is not available on the Internet and it is not clear whether Schedule 5 is intended to cover such content. Similarly, TransACT and some other broadband providers now provide Video on Demand using the Internet Protocol (IP) to television set-top-boxes. This content uses the IP on a closed network (that is, not the “Internet” but “Online”) and it is not clear whether such a video-on-demand service is intended to be regulated by Schedule 5 or regulated otherwise as a broadcast-like service. There is no implication here that such systems are being used to transmit offensive material, but the point is that, short of judicial precedents being established, the service providers concerned cannot be sure how their services fit in the context of the BSA, if at all.
- The MPEG-4 standard represents a multimedia presentation in the form of a number of audio-visual objects within a “stage” area which then perform according to a script, rather like a stage play or the fictional holodeck of Star Trek. It is quite possible for an innocuous MPEG-4 presentation to be modified by user intervention or automatic preference into potentially offensive material at the user’s terminal. Currently it is easy to associate transmitted content with the rendered presentation. In the case of MPEG-4, it

Submission to the Review of Schedule 5 of the Broadcasting Services Act

is no longer clear. While such multimedia magic may seem some way off, the fact is that MPEG-4 display software is available today and related object-oriented coding systems such as Flash are widely used.

Comments are sought generally on the scope and coverage of Schedule 5.

There are some notable gaps and shortcomings in the scope and coverage of Schedule 5, including the issues dealt with above with regard to convergent devices and also, but not limited to:

- The lack, after 3 years, of uniform State mirror legislation (except for the very recently enacted South Australian legislation), which is a crippling problem for the co-operative federal scheme.
- The lack of transparency of administration. When the AAT handed down its decision in *Electronic Frontiers Australia Incorporated*, it evidently had difficulty in trying to balance administration of the system against public rights of access to information relating to that administration. The AAT acknowledged that there were:

“important issues relating to censorship, openness of government and even to the confidence that the public has in the agencies of government to implement and administer its schemes with integrity for secrecy can ultimately lead to the public’s questioning integrity even where there is no need for such questioning” [6]

The Government’s proposed response in the Communications Legislation Amendment Bill 2002 would not seem designed to further promote transparency and public confidence in the administration of the system.

- The cost of administration
- The lack of real impact in relation to truly offensive material
- Potential restrictions in relation to legitimate uses of the Internet

See further the NSW Legislative Council “Safety Net?” report criticisms [7]

Conclusion

We believe that any focus on technical fixes is bound to fail even if significant resources are applied.

As a consequence, education and empowerment of end users is the only effective regulatory method. As ABA representatives involved in administration of and reporting on the scheme acknowledged in a paper relating to their six month review, “in the end, it is up to individual users to actively manage their own use and that of the young people in their care”. [8]

References

- [1] Robert Chalmers , “Regulating the net in Australia: firing blanks or silver bullets” forthcoming publication – accepted for E Law - Murdoch University Electronic Journal of Law (<http://www.murdoch.edu.au/elaw/>)
- [2] Media Streaming and Broadband in Australia available at <http://www.aba.gov.au/abanews/conf/2002/papers/ctin.pdf>
- [3] See Schneier “Secrets & Lies – Digital Security in a Networked World” (Wiley, 2000)
- [4] See, inter alia: CSIRO report “Effectiveness of Internet Filtering Software Products” – prepared for NetAlert and the ABA – available at <http://www.aba.gov.au/internet/research/filtering/index.htm>; American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996), aff'd, 521 U.S. 844 (1997); 47 U.S.C. §§ 230, 231 (1998); American Civil Liberties Union v. Reno, 31 F. Supp. 2d 473 (1999), aff'd, 217 F.3d 162 (3d Cir. 2000), American Library Association v United States May 31, 2002 - available at http://www.eff.org/Legal/Cases/Multnomah_Library_v_US/20020531_cipa_court_opinion.html)
- [5] NOIE, “The Spam Problem and how it can be countered”, 16 July 2002, available at http://www.noie.gov.au/projects/confidence/improving/Spam/Interim_Report/contents.htm
- [6] *Electronic Frontiers Australia Incorporated and Australian Broadcasting Authority* (Q2000/979) at paragraph 93 of the decision.
- [7] Parliamentary Paper Number 89 from the Legislative Council’s Standing Committee on Social Issues, "Safety Net? Inquiry into the Classification (Publications, Films and Computer Games) Enforcement Amendment Bill 2001"
- [8] Stephen Nugent and Andree Wright, “Australia’s co-regulatory scheme for internet content: the first six months” at p.11, available at www.aba.gov.au