INTERNET CONTENT CONTROL IN AUSTRALIA: ATTEMPTING THE IMPOSSIBLE?

PETER CORONEOS*

I. INTRODUCTION

A difficult problem confronts governments in attempting to regulate illegal and offensive content on the Internet. Like any communications medium, the Internet can be used to publish all manner of material, some which people may find indecent or offensive, and some which certain countries will deem illegal. The 'old media' are controlled by regulatory authorities through licence conditions, import controls, and domestic censorship and criminal laws. Physical media and short-range transmissions are amenable to control. However, this is not the case with the Internet, which is global (and therefore transjurisdictional), instantaneous and diffuse.

While logic would dictate that the publishers of content should bear the responsibility for ensuring it is legal in the place where it is published, the Internet has a habit of rendering traditional control paradigms irrelevant or unworkable and conventional laws unenforceable. So far, the Internet has tended to challenge as many social policy ideals as it has promoted, although in future years this situation will hopefully improve as we better understand the medium and adapt to it. While the following analysis outlines Australia's response to online content regulation, the concerns we face are shared in most other countries with an emerging Internet culture.

This paper will consider the problems associated with controlling online content. It will then examine Australia's recently enacted online content legislation, the *Broadcasting Services Amendment (Online Services) Act* 1999 (Cth) ("*Online Services Act*"). Finally, it will present an example of how the Internet industry has responded to the challenge of providing a solution that balances the broad policy objectives of the legislation against a need to foster the growth and development a diverse, dynamic and viable information industry.

* Executive Director, Internet Industry Association.

II. SHOOTING THE MESSENGERS

A common temptation for those confronting the limits of jurisdiction is to pin liability on the facilitators of the communication – in the case of the Internet, Internet service providers ("ISPs"). ISPs provide the connection between the home or office computer and the interconnected web of worldwide computers collectively constituting the Internet. For governments responding to legitimate community concerns regarding Internet content, the fact that ISPs are identifiable and are likely to be tied to a geographic location within somebody's bailiwick, is arguably enough to warrant attaching at least a contingent liability for the acts of third parties (who are often the real culprits, if blame is to be laid). In some circumstances this may be justified, for example, where ISPs are unwilling either to disclose the identity of online offenders who have been traced to their networks, or to act upon notices by relevant authorities to stop an infraction of a third party, where that is possible. Further, for private interests pursuing private rights, the deep pockets of larger ISPs will yield more than the mere infringer, who may well be a starving hacker or a naïve teenager.

Some examples of shooting the messenger include:

- suing ISPs for defamation because they carried newsgroups containing defamatory material;[1]
- suing ISPs because they allegedly authorised a breach of copyright by providing connectivity to the Internet to persons who used it to download unlicensed musical works;[2]
- attaching criminal liability to persons who "transmit" or "make available" restricted material to minors.[3]

The problem with regulating Internet content is that most material that is likely to be considered illegal or offensive in Australia is hosted on computers located overseas and out of reach of both our regulators and our courts. The blocking of content originating overseas is problematic, with technologies

---

1 *Laurence Godfrey* v *Demon Internet Ltd* (unreported, High Court of Justice, Queens Bench Division, Morland J, 26 March 1999) <www.courtservice.gov.uk/godfrey2.htm> at 26 March 1999 (Copy on file with author).

2 For example, see the 1996 Australian Performing Rights Association ("APRA") action against OzEmail. This matter subsequently settled with no admission of liability. APRA was seeking to licence ISPs and collect a royalty payment of $1 per subscriber per annum from all ISPs on the basis that works for which they held copyright in Australia were available over the Internet through ISPs. They made this claim under what the Internet industry regards as an opportunistic interpretation of the present *Copyright Act* 1958 (Cth) s 36 which proscribes the transmission of unauthorised copies of works "over wires to subscribers of a diffusion service". In 1998, the Federal Government announced its intention to review the provisions of the Act under the long awaited 'Digital Agenda' reforms to take account of developing technologies and, among other things, the need to limit the liability of ISPs in their capacity as carriage service providers. Senator Richard Alston and Senator Chris Ellison, "Government Addressing Copyright Challenges", Media Release, 23 January 1998. As of writing, we are still waiting for the relevant amendments to be enacted.

3 See for example the *Censorship Act* 1996 (WA), s 102(1) and (2). These provisions are drafted widely enough to catch ISPs. See also the *Classification (Publications, Films And Computer Games) (Enforcement) Act* 1995 (Vic), s 58.

making it possible to disguise the origin of material ('spoofing'), or permit the origin to change location within seconds ('dynamic addressing'). In addition, material is easily encrypted making it difficult to discern the content of files, even if intercepted. Furthermore, tunnelling technologies are well established and freely available over the Internet, permitting the circumvention of proxy filters by allowing a user utilising a different protocol to bypass the block and access prohibited content by requesting it back in a form which filters cannot block.

Content hosted within Australia (which probably constitutes less than one percent of illegal or offensive material available online) is, in theory, more easily controlled. The National Classification Code[4] serves as a uniform standard for classifying content and a benchmark for State and Territory legislation. However, there are differences in how States and Territories allow for the possession and the dealing with some categories of content. The new content regime promises a consistent national approach with States enacting complementary legislation, but this is yet to be realised. Our State governments do not have a particularly good track record in achieving uniformity, with the patchwork of defamation laws a case in point. The problem is all the greater in an age where geographic boundaries have become meaningless. States no longer have the luxury of acting in isolation, particularly given that their legislation will not have extra-territorial effect.

The liability of ISPs as mere conduits of data is a contentious issue. Generally, they will have no knowledge of material transmitted by their users whether illegal or not. ISPs are akin to mail carriers; unaware of the contents of the packets they store and deliver. Accordingly, the Internet industry is opposed to sheeting home liability to ISPs, except in cases where they have direct knowledge of, or are actively participating in illegal acts. This approach is consistent with the Agreed Statement accompanying the 1996 WIPO Copyright Treaty[5] which holds that a person should not be considered as communicating material merely by virtue of providing the physical means of that communication.

For reasons of practicality and as a matter of principle, the Internet industry has opposed both the monitoring of sites and preemptive intervention by ISPs to identify content which may be illegal. Most Internet users would find it intrusive to have their ISPs, many of whom also offer content hosting services, to routinely search their personal web space for illegal material. In addition, the volume of material on ISPs servers makes this an unworkable proposition. A large ISP in Australia may host upwards of 80 000 sites, all of which can be changed remotely and instantaneously by the end-user without the ISP's knowledge of the content of such changes.

Furthermore, ISPs are in no position to judge what is likely to be illegal. What constitutes illegality is not always clear. Preemptive action, particularly where

4 A schedule to the *Classification (Films, Literature and Computer Games) Act* 1995 (Cth).

5 Agreed Statements Concerning the WIPO Copyright Treaty, adopted at the WIPO International Conference: Certain Copyright and Neighboring Rights Questions, Geneva, 10 December 1996.

there is inadequate contractual protection, could render an ISP liable for damages to their customers for wrongfully removing material that they think may be illegal. Conversely, where the State requires action and an ISP stumbles across material that they wrongfully deem *not* to be illegal, criminal liability may arise.

III. THE NEW LEGISLATION

It is against this background that the Federal Government passed the *Online Services Act*. This legislation amends the *Broadcasting Services Act* 1992 (Cth) to include the regulation of the transmission and hosting of Internet content in Australia.

The Explanatory Memorandum to the Broadcasting Services Amendment (Online Services) Bill 1999 states:

> Concern has been expressed both within the community and at government level about the nature of material that may be accessed by means of online services, specifically in relation to the perceived ease of access to material that is either pornographic or otherwise unsuitable for children...
>
> The objective of further proposals is to ensure that the regulatory framework is commensurate with community concerns about online content, particularly that the range of material to be controlled is consistent with the range controlled in conventional media. The Government also considers that the complaints process proposed in 1997 should be revisited to ensure that an unreasonable onus is not placed on service providers and to provide for more timely and efficient handling of complaints to prevent access to material that is of serious concern.[6]

While recognising the difficulties involved in regulating the Internet, the Government believed that these should not prevent an attempt. There was a view that developing technologies would eventually make the regulation of Internet content easier, but that industry should do all that was feasible at this time. In a clear departure from principles espoused by the Government in 1997,[7] the *Online Services Act* raises the bar to create a default obligation upon ISPs to use all reasonable efforts to prevent access to content hosted offshore. This would occur in circumstances where ISPs were notified of the existence of content that the Government deemed to be unsuitable for domestic consumption.[8]

The amending legislation expressly provides for Commonwealth law to prevail over previous State and Territory attempts to regulate ISPs and Internet content hosts ("ICHs"), except where the laws can operate concurrently.[9] By agreement, it is expected that complementary legislation from the States and

---

6 Explanatory Memorandum to the Broadcasting Services Amendment (Online Services) Bill 1999 at [5].

7 *Principles for a Regulatory Framework for On-Line Services in the Broadcasting Services Act 1992*, 15 July 1997, available at <http://www.dcita.gov.au/text-welcome.html> at 1 February 2000 (Copy on file with author). See also Senator Richard Alston and Attorney-General Darryl Williams, "National Framework for On-Line Content Regulation", Media Release, 15 July 1997.

8 *Broadcasting Services Act* 1992, Schedule 5, cl 40(1)(c) (as amended by the *Online Services Act*).

9 *Ibid*, ss 90 and 91.

Territories will be enacted to control the activities of content providers and end users, to cover the field of Internet activity in Australia as far as content goes.

For the Internet industry, the most significant changes arising from the legislation involve the imposition of potential liability on ICHs and ISPs for material that they store or provide access to. The default provisions of the legislation vest in the Australian Broadcasting Authority ("ABA") the right to issue notices, and to direct ISPs and ICHs to comply with industry standards that will be devised to respond to content of which the ABA is aware. The scheme is complaints driven; that is, the ABA will not normally undertake own-motion investigations, but will only respond to complaints about Internet content reported to it.[10] It will have discretion to disregard complaints that are in its opinion frivolous, vexatious or likely to undermine the administrative processes of the regime.[11] The ABA also has the power to have content evaluated by an independent body and to form views as to suitability on that basis.[12] Content is defined broadly but will exclude anything which is not stored and accessible to the public[13] and, following amendments, will also exempt most forms of email.

Many of the decisions of the ABA will be subject to merits review by the Administrative Appeals Tribunal,[14] and "interim take-down notices" in respect of domestically hosted content are reversible where not subsequently found by the classifying body (the Office of Film and Literature Classification) to be prohibited.[15]

Interestingly, s 91 of Part 9 of the *Broadcasting Services Act* 1992 (Cth) (as amended by the *Online Services Act*) grants immunity to ISPs and ICHs against civil and criminal liability, including State or Territory law, for a range of conduct which might otherwise arise by virtue of the activities of their subscribers. This immunity operates only where the ISP or ICH has no knowledge of the conduct. It would appear from the explanatory memorandum that this safeguard is included to avoid the development of a patchwork of risk, particularly in those States and Territories that have already enacted legislation affecting ISPs.[16] However, it seems a strange addition to the legislation that is ostensibly about the regulation of unsuitable content and the protection of children. The provision appears to be drafted widely enough to cover issues such as defamation, copyright and possibly liability arising as a result of hacking. While it will be interesting to see how a court will construe these sections, for the moment the breadth of the provision should offer some comfort to industry participants who have generally felt vulnerable in these matters.

Once it became evident that the legislation was not going to be stopped, the Internet Industry Association ("IIA") saw amendments as the only means by which to address those parts of the legislation which it believed to be

10 *Ibid*, Part 4 – Complaints to, and investigations by, the ABA.
11 *Ibid*, s 26(2).
12 *Ibid*, s 28(2).
13 *Ibid*, s 3. See, also, note 6 *supra*, p 16.
14 *Ibid*, s 92.
15 *Ibid*, s 34(1).
16 Note 6 *supra*, p 2.

unworkable and likely to result in unintended consequences, such as lower network performance and, ultimately, higher access costs for end-users. Fortunately, those amendments that were secured (generally with the support of all three political parties) made way for the creation of an alternative regime, with industry codes as the basis of implementation.

IV. THE INDUSTRY DEVELOPED SOLUTION

The passage of the Broadcasting Services Amendment (Online Services) Bill 1999 through the Senate, in June 1999, spurred the IIA to move quickly to finalise the self-regulatory content elements of its existing draft Code of Practice ("Code"). The legislation provided that unless industry codes were registered and in place by the end of 1999, the default content blocking provisions of the legislation would come into play.[17]

Three modules within our larger Code were devoted to content control. Each, as a code in its own right, was subsequently registered by the ABA in December 1999 (hereafter, "Content Codes") and came into operation on 1 January 2000.[18]

The approach underlying the IIA response is "industry facilitated user empowerment". This term recognises that end-users are ultimately in the best position, given the nature of the Internet, to control what content they are able to access online. However, the Internet industry does not abrogate all responsibility here – there are things that can be done to enhance the ability of end-users to assume control, specifically through the provision of information and tools to end-users.

Accordingly, the Content Codes mandate that ISPs will provide to end-users one of a selection of "approved filters" which are contained in Schedule 1 of the Content Codes. The sixteen approved filters listed are included as a result of an independent study of available options by the CSIRO.[19] However, it is anticipated that more will be added over time as technologies expand and improve. Some filters are 'client side' products, like Net Nanny, which the user installs on their home computer. Others are 'server level' filters, like Internet Sheriff, which operates at the ISP end – but only as an optional 'differentiated service offering' – which end-users can choose to dial into as a separate access number. ISPs are not expected to absorb the costs associated with meeting this obligation.[20]

A condition of inclusion of filters in Schedule 1 was that filter provider companies agree to take updates from the ABA in respect to sites that it identifies, as a result of its complaints handling process, to be potentially prohibited.

---

17 Note 8 *supra*, s 40(1)(b) and (c).

18 The Content Codes, as registered by the ABA, will be incorporated into a more comprehensive code addressing other issues ranging from online privacy to e-commerce, which the IIA will finalise in the first quarter of 2000.

19 *Blocking Content on the Internet: A Technical Perspective*, June 1998.

20 Content Code 2, cl 6.2.

The suppliers of the filtering technologies, who in most cases will not be the ISPs themselves, are required to update their products and services to filter any additional material which the ABA has classified as prohibited.[21] This is akin to the developers of anti-virus software providing automatic updates on new virus 'definitions'. The providers of the technologies will also be expected to provide help lines, online information resources and the like. It is not the intention of the IIA that ISPs be burdened with that task, unless ISPs themselves choose to develop and have accredited access control measures for use with their own (applicable) customer base. The Content Codes also contain exemptions where no filters need to be supplied by ISPs. Exempted circumstances include the provision of Internet access to schools or corporate customers who are already utilising filtering technologies, whether to limit their legal liability (in the case of businesses) or otherwise.[22]

In practical terms, the registration of the IIA's Content Codes means that the ABA cannot issue access prevention notices to ISPs in Australia.[23] In cases where serious material is referred to the ABA, the Authority will independently inform relevant law enforcement agencies in the host country through the appropriate channels.[24] Except in this instance, it is anticipated that the industry-developed code alternatives will entirely circumvent ABA action in respect of internationally sourced content. This is as it should be, since the default alternatives in our view were unlikely to provide any better level of protection than what industry can itself achieve through the Content Codes, although the power of the ABA to direct compliance is welcome.

It is important to note that end-users will not be forced to install or use content filters. It is our view that empowerment assumes the right to use the Internet in an unfiltered form, both for performance reasons and for reasons of choice. However, in accordance with the spirit of the legislation, adults who find certain content offensive and parents who are worried about what their children might view will now have the means of control.

The Content Codes also oblige ISPs to:

- take reasonable steps to ensure that Internet access accounts are not provided to persons under the age of 18 years without the consent of a parent, teacher or other responsible adult;[25]
- take reasonable steps to encourage commercial content providers to use appropriate labelling systems and to inform them of their legal responsibilities in regard to the content they publish;[26]
- take reasonable steps to provide users with information about supervising and controlling children's access to Internet content, procedures which parents can implement to control children's access

21 Content Codes, Schedule 1, para 1.
22 Content Code 2, cl 6.4.
23 Note 8 *supra*, s 40(1)(b) and (c).
24 Note 8 *supra*, cl 40(1)(a).
25 Content Code 1, cl 5.1.
26 *Ibid*, cl 5.2.

> to, Internet content, their right to make complaints to the ABA about online content and procedures by which such complaints can be made.[27]

The Content Codes contain deeming provisions for "reasonable steps" which provide options for ISPs and content hosts by which they can meet these obligations without undue detriment.[28]

For ICHs, the main requirement will be that they remove prohibited or potentially prohibited content hosted in Australia upon notification by the ABA.[29] In the case of other material which is illegal in Australia, ICHs will be required to follow lawful directions from other "Relevant Authorities" to remove it.[30] This is in accordance with current best practice, applying, for example, to hosting unlicensed online gambling sites in NSW.[31]

V. CONCLUSION

In international terms, the co-regulatory approach and the obligation on ISPs and ICHs to provide end-user tools is unprecedented in the area of online content. While no one pretends that the solution will provide an absolute guarantee of protection, it is in our view the best available option and is likely to be perceived by most industry players as a workable scheme. Costs will ultimately be borne by end-users, but that is no different from any other form of regulatory compliance. In spite of this, we believe that competitive market pressures will ensure that any increases will be insignificant within the scheme of Internet costs generally. While the circumstances in which the initiatives were developed were not ideal, and the time frame in which industry was required to respond was very short, the IIA is confident that the outcome will be meaningful protection for families and those with thin sensibilities. To be most effective, the measures must be accompanied by education and international cooperative arrangements between industry, and between governments. While we are all still coming to terms with the social and cultural implications of the Internet revolution, legislators must eventually understand that statutory intervention in the new communications environment has profound limitations and cannot operate in a vacuum.

---

27 *Ibid*, cl 5.3.
28 *Ibid*, cl 5.4.
29 Content Code 3, cl 7.09(a).
30 *Ibid*, cl 7.10.
31 Pursuant to s 33 of the *Racing Administration Act* 1998 (NSW).