BRAVE NEW (ONLINE) WORLD

NIRANJAN ARASARATNAM*

Talking about Internet censorship is like discussing abortion; the debate is confused, emotive and polarised. The protagonists mark out their territory based on flawed assumptions and a passionate belief in the absolute truth of their principles. Conservative groups preach family values, industry focuses on e-commerce and civil libertarians obsess with free speech. It is a collision of values and interests, without room for comprise, pragmatism and discretion.

The result? The *Broadcasting Services Amendment (Online Services) Act* 1999 (Cth) ("*Online Services Act*"): confused, ill conceived and very difficult to implement in practice. The *Online Services Act* was passed by the Commonwealth Parliament on 30 June 1999. The Internet industry is now left pondering how much damage it will cause to Australia's emerging e-commerce infrastructure.

I. THE ACT

The *Online Services Act* amends the *Broadcasting Services Act* 1992 (Cth) to bring within its regulatory net the regulation of online services. It establishes a complaints regime under which the Australian Broadcasting Authority ("ABA") will investigate complaints from the public about "prohibited content" or "potentially prohibited content".[1]

Internet content hosted within Australia is prohibited content if the content has been classified 'RC' (Refused Classification) or 'X' by the Classification Board. 'R'-rated content is also prohibited if it is hosted within Australia and is not subject to a restricted access system.[2]

The rules apply to Internet content hosts ("ICHs")[3] and Internet service providers ("ISPs"),[4] with different standards applying to each. In summary,

---

* Solicitor, Allen Allen & Hemsley.

1 The terms "prohibited content" and "potentially prohibited content" are defined in the amended *Broadcasting Services Act* 1992 (Cth), Schedule 5, ss 10 and 11 respectively.

2 *Broadcasting Services Act* 1992 (Cth), Schedule 5, s 10(1) (as amended by the *Online Services Act*).

3 *Ibid*, s 3.

where there is prohibited content hosted within Australia, the ABA will issue "final take-down notices" to the ICH directing it to remove the content from its site.[5] For overseas prohibited content, the ABA must direct ISPs to carry out blocking measures in accordance with a specified industry code or, if there is no industry code, direct each ISP to take all reasonable steps to block the content (a "standard access-prevention notice").[6]

If an industry code governing the blocking of 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".[7] 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.[8]

The ABA may also issue "special take-down notices"[9] or "special access-prevention notices", 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 a take down notice.[10]

ICHs and ISPs must take reasonable steps to develop industry codes (to be registered by 1 January 2000)[11] which deal with procedures educating parents about controlling children's access to Internet content, telling customers about their rights to make complaints and providing information on client-side filtering technologies.[12] The Act also provides for the development by ISPs of codes that detail the steps to take to block access to overseas prohibited content.[13]

All notices must be complied with by no later than 6:00pm on the next business day after the notice was given to the ICH or ISP.[14] The ABA may designate a scheme to deem service of a notice on all ICHs and ISPs.[15]

As the quid pro quo to the censorship regime, the *Online Services Act* grants ISPs and ICHs immunity from State and Territory laws in respect of the carriage or hosting of prohibited material where the ISP or ICH was not aware of the content.[16] The Act also exempts ISPs and ICHs from any State or Territory requirement to monitor, make inquiries about, or keep records of, Internet content carried or hosted by them.[17]

---

4 *Ibid*, s 8.
5 *Ibid*, s 30(1).
6 *Ibid*, s 40(1).
7 *Ibid*, s 40(2)(a).
8 *Ibid*, s 40(4).
9 *Ibid*, s 36.
10 *Ibid*, s 47.
11 *Ibid*, s 59(4).
12 *Ibid*, s 60.
13 *Ibid*, s 60(2)(d).
14 *Ibid*, s 37(1)-(3).
15 *Ibid*, s 51.
16 *Ibid*, s 91(a) and (c).
17 *Ibid*, s 91(b) and (d).

II. CODES OF PRACTICE

The *Online Services Act* relies heavily on industry codes. The Act requires associations that represent ICHs and ISPs to develop codes on the various matters dealt with by the Act, including measures to block access to overseas prohibited material and procedures to inform the public about their rights under the Act.[18]

Just two weeks prior to the implementation of the *Online Services Act*, the ABA registered three industry codes of practice: the first two apply to ISPs in relation to access to content hosted overseas and Internet access generally; and the third applies to ICHs. The codes came into effect on 1 January 2000 and will be reviewed in 18 months time.[19]

The codes were developed by the Internet Industry Association ("IIA") in consultation with the Internet industry and end-user groups, together with negotiation with the ABA. The IIA has, to some extent, steered the Government away from its censorial approach to the Internet. The codes embody an industry facilitated end-user empowerment philosophy under which end-users take primary responsibility for the Internet content that they view by employing client-side filtering technologies.

In particular, the ISP code addresses one of the main controversies of the Act; namely, requiring ISPs to block access to prohibited content hosted overseas. This was one of the more contentious aspects of the Act, given the technical difficulties of content blocking. A CSIRO report prepared for the National Office for the Information Economy concluded that packet level blocking was indiscriminate and would create an unintended "hole" in the Internet infrastructure, thus isolating Australia from the e-commerce infrastructure.[20]

The ISP code relies heavily on client-side filtering technologies, removing any requirement on ISPs to use packet level filtering on users who do not wish to have their Internet experience censored. The code provides that where the ABA has notified ISPs of prohibited content hosted overseas, ISPs must provide to each of its subscribers an approved filter software service. The code states that "provision [of filter software] for use" may occur by means of a link to a download from the ISP or via an installation disk.[21]

The other two codes require ISPs and ICHs to do the following:

- take reasonable steps to ensure that Internet access accounts are not provided to persons under 18 years of age without parental, teacher or responsible adult consent (eg demanding credit cards or age verification information, placing prominent notices or supplying approved filter software);[22]

---

18 *Ibid*, s 60(1).

19 Content Code 1, cl 5.9; Content Code 2, cl 6.5; Content Code 3, cl 7.12.

20 *Blocking Content on the Internet: a Technical Perspective*, June 1988. For a further description of the technical problems associated with online content blocking see N Arasaratnam, "Internet Censorship: See No Evil, Speak No Evil, Hear No Evil" (1999) 18(2) *Communications Law Bulletin* 4.

21 Content Code 2, cl 6.2.

22 Content Code 1, cl 5.1; Content Code 3, cl 7.1.

- provide end-users with information about their rights and responsibilities under the Act;[23]
- institute procedures for dealing with complaints relating to pornographic SPAM;[24] and
- encourage content providers to use appropriate labelling systems.[25]

Conveniently, ISPs and ICHs will satisfy these requirements by placing such information on their home page or by a link from their web page to a code-approved website containing such information, such as the IIA website. ICHs must also include in their web hosting contracts or acceptable use policies terms prohibiting content providers from uploading prohibited content.[26]

III. EFFECTS ON INTERNET COMMERCE

The carriage of pornography on the Internet is good business. By some estimates, pornography accounts for up to 40 per cent of Internet traffic.[27] Internet censorship will fundamentally alter the economics of an ICH's and an Internet content provider's business. Australian ICHs and Internet content providers will be governed by a more restrictive content regime than their overseas counterparts and this clearly puts them at a competitive disadvantage.[28] While Australian prohibited content is blocked to all end-users, overseas prohibited material will be filtered only by those end-users who do not wish to view such content.

The provision of the approved filter software may prove too expensive for smaller ISPs. ISPs must put in place warehousing and distribution arrangements for disk-based software, or implement a link to a download from the ISP's website. While the costs of implementing the arrangements may be passed on to the end-user, it is entirely uncertain whether or not end-users will opt to purchase the filter software. Potentially, at least, the ISP will be left to bear the brunt of the implementation costs. Smaller ISPs serve rural areas where many larger ISPs do not find it profitable to build points of presence. The *Online Services Act* serves to reduce Internet access and connectivity in precisely the areas the Government has identified as in need of more sophisticated communications.

Filter software is not 100 per cent effective, with the result that legitimate sites will be blocked. Many companies use the Internet as the primary source of its product information. The effective use of the World Wide Web depends on

---

23 Content Code 1, cl 5.5; Content Code 3, cl 7.6.

24 Code Code 1, cl 5.7; Content Code 3, cl 7.8.

25 Content Code 1, cl 5.2(a); Content Code 3, cl 7.2(a).

26 Content Code 3, cl 7.5.

27 R Swan, Eros Foundation spokesperson in K Hannon, "Law to Set Up Net Porn Watchdog" *Courier Mail*, 27 May 1999.

28 The vigour with which movie producers fight to have their movies rated 'M' as opposed to 'R' is a testament to the commercial effects of a rating system.

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 search engine favoured by Senator Alston, returned 8545 entries on Alta Vista and a paltry 1591 on Iseek.[29] In the USA, filter software resulted in breast cancer sufferers being unable to access government-sponsored websites.[30]

Filter software slows network performance and increases delays in Internet response times. For example, attempts by the German Government 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 October 1999, the President and Chief Executive of the Bertelsmann Multimedia Group, Dr Klaus Eierhoff, stated that nation-based content regulation would fail because it will force content providers offshore.[31] The *Online Services Act* will drive content outside Australia. The Internet is already an USA-centric medium. The Act will add to the disproportionate amount of traffic from Australia to the USA. As non-USA ISPs have to pay for both ends of the transoceanic circuits that are required to connect to USA backbones, the costs of Internet transmission for Australian ISPs will increase.

IV. DEFICIENCIES IN THE *ONLINE SERVICES ACT*

A. Email Exclusion

The *Online Services 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 website. It seems relatively easy for an ICH or ISP to buy Internet protocol 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. The ABA codes do recognise this dilemma and require ISPs and ICHs to provide users with information as to how to minimise such emails. However, this measure in no way eliminates the problem.

B. Provision of Approved Software

Under the ABA codes, where the ABA notifies ISPs of overseas prohibited content, ISPs must provide to their subscribers approved filter software.[32] The codes contemplate the provision of the software by disk or download either at

29 See H McNally, 30 May 1999, Decisions and Designs Pty Ltd, <www.decisions-and-designs.com.au/the censor.html> at 10 January 2000 (Copy on file with author).

30 P Wilson, "Anti-Smut Agenda Overwhelmed in Digital Millennium" *Courier Mail*, 27 January 2000, p 17.

31 K Crawford, "Industry Gets an A But Government Told to Do Better" *Sydney Morning Herald*, 29 October 1999.

32 Content Code 2, cl 6.2(a).

the registration stage or by notification.[33] Curiously, the IIA has stated that end-users will not be required to implement the filter software and that in no event shall ISPs invade subscribers' privacy in order to confirm the installation of the filter solution.[34] It is a counter-intuitive policy result to require ISPs to make filter software available without some compulsion on the part of users to implement the software. Indeed, by presenting certain filter software in the code and allowing ISPs to choose which filter software it makes available, the code may have the unintended consequence of limiting the range of filter software available in the market.

C. Definitional Problems

The *Online Services 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 chat rooms; 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 Internet protocol connectivity to other ISPs and Internet access providers. The *Online Services 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. Only the codes make a rudimentary attempt to distinguish these players by isolating those ISPs who have "commercial subscribers".[35]

D. Not Just Porn

One of the key myths of the *Online Services Act* is that it is confined to illegal and highly offensive content, such as sex and violence. On the contrary, the Act's tentacles extend to the depiction of 'adult themes', drug use and language. Under the National Classification Code promulgated pursuant to the *Classification (Publications, Computer Games and Films) Act* 1995 (Cth), in order to avoid a 'R' rating, the content must adhere to the following guidelines: coarse language that is very strong, aggressive or detailed should not be gratuitous; the treatment of themes with a high degree of sensitivity should be discreet; drug use should not be promoted or encouraged; and depictions of violence should not have a high impact.[36] There has been insufficient consideration as to whether or not content standards for film and television are appropriate for the Internet.

---

33 *Ibid.*

34 "Guide for Internet Users – Information About Online Content", IIA, <www.iia.net.au/guideuser.html> at 20 December 1999 (Copy on file with author), [7].

35 Content Code 2, cll 6.2(b) and 6.4(a).

36 Office of Film and Literature Classification, *Guidelines for the Classification of Films and Videotapes (Amendment No 2)*, 15 April 1999.

E. Vague Requirements for Backbone Providers

The codes refer to those ISPs who have "commercial subscribers". The ISP code requires such ISPs to provide a facility or arrangement that takes account of the subscriber's network requirements and is likely to provide a reasonably effective means of preventing access to prohibited and potentially prohibited content.[37] The codes refer to measures including the provision of approved filter software or facilitating access to consultancy services with respect to firewalls.[38] This requirement is somewhat vague and some work needs to be done to provide backbone providers and larger ISPs some comfort as to the discharge of their obligations under the *Online Services Act*.

F. Are the Codes Representative?

The *Online Services Act* relies heavily on industry codes. It 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. The ABA must be satisfied that the body or association actually represents the ISP and ICH sections of the Internet industry.[39]

The ABA has registered three codes, all of which were developed by the IIA. It is difficult to see how the ABA can claim that it has approved industry-sanctioned codes of practice. The IIA represents a small portion of the 600 odd ISPs in Australia, while it is unclear what body truly represents ICHs. (This fact was one of the reasons put forward by the Government in the Senate Select Committee's report against the use of codes of practice for content regulation.) Industry codes assume some level of alignment of commercial interests amongst the industry players that may not always be the case. The IIA cannot achieve industry consensus on a code of practice governing things such as billing practices, privacy and content rating. It is somewhat ambitious of the ABA and the IIA to foist the codes on the Internet industry without a clear mandate to do so.

On the other hand, the IIA should be commended for steering the Government away from its imperialistic approach to content regulation. The codes accommodate a fair degree of the end-user empowerment philosophy which the Internet industry appeared to favour at the Senate Select Committee hearing.

G. Anti-Avoidance Measures

The anti-avoidance measures, under which the ABA can direct ICHs to block content similar to prohibited material, are a real cause for concern. ICHs will become precisely what many of them do not want to be – editors of content held on their servers. ICHs who host content for third parties, by and large, do not view, let alone edit, content held on their servers. Indeed, most standard web hosting contracts contain terms prohibiting content providers from posting

37 Content Code 2, cl 6.2(a).

38 *Ibid.* A firewall is a system or group of systems that enforces an access control policy between two networks.

39 Note 2 *supra*, s 59(1) and (2).

offensive, defamatory and illegal content. However, the new anti-avoidance measures will force ICHs to scour their sites and networks each day to identify prohibited material. Once they discover any questionable material, ICHs will have to decide whether the content is similar to prohibited content, a judgment on which significant penalties hang.

H. Will the Take-Down Notices Work?

The take-down notices directing ICHs and ISPs to remove or block content may not be workable. Under the *Online Services Act*, content must be "set out" or "described".[40] 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 could be modified to make it non-prohibited, or to move it from one classification to another. Another problem will arise where take-down notices are issued against ICHs who host content on behalf of their customers. Those ICHs will need to locate the content and delete it from their servers. This may take more time than is prescribed by the *Online Services Act*.

I. Complaint Flooding

The censorship regime established by the *Online Services Act* is open to abuse. The main scope for abuse is complaint 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.[41] 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. Do the ABA and the Classification Board have the resources to respond to all such complaints? Under the *Online Services Act*, the ABA's only way of filtering complaints is by disregarding frivolous and vexatious complaints. It will be interesting to see how the ABA exercises this discretion.

J. Lack of Procedural Fairness

The *Online Services Act* fails to afford adequate natural justice to ICHs and ISPs. The ABA is not required to inform the ICH or ISP that it is investigating a complaint against content hosted or carried by it. There is no time limit for it to carry out its investigations. ISPs and ICHs are not informed of the identity of the complainant, nor are they given any opportunity to respond to a complaint. The

---

40 *Ibid*, s 49.
41 *Ibid*, s 29.

ABA may conduct the investigation as it thinks fit and its information gathering powers are cast extremely broadly.[42] The ABA, Classification Board and their staff are protected against criminal proceedings in relation to the collection, possession and distribution of any material in connection with the exercise of any power under the *Online Services Act*.[43] Finally, ABA decisions are not stayed while an ISP or ICH appeals an ABA decision to the Administrative Appeals Tribunal.[44]

K. Restricted Access Systems

Internet content hosted in Australia is prohibited if the content has been classified 'R' by the Classification Board and access to the content is not subject to a "restricted access system".[45] A restricted access system may only be declared by the ABA (without any guide as to the declaration process other than the objective of protecting children from exposure to unsuitable Internet content).[46] On 7 December 1999, an ABA declaration setting out the system requirements for restricted access systems was tabled in Federal Parliament. The restricted access system must be a PIN or password. In order to qualify for a PIN or password, certain prescribed age verification information must be provided (ie the name of the applicant, a declaration that the applicant is 18 years of age or over, and credit card details/digital signature (for online applications) or credit card details/evidence of age (for hard copy applications).

Electronic Frontiers Australia ("EFA") has raised two significant problems with the ABA declaration.[47] First, the proposals require users to provide personal identifying information that goes far beyond proof of age. The EFA believes that this is likely to act as a deterrent even for genuine adults. Second, the proposed identification details are easily forged.

V. CONCLUSION

The global reach of the Internet renders nation-based Internet regulation largely ineffective. The ABA approved codes are a stark recognition by the Government that content regulation of overseas material is a futile exercise. However, the result is a two-tiered standard of online content regulation, significantly favouring overseas content providers. As Australia does not have the political and economic power to drive international Internet standards, the

42 *Ibid*, ss 26-8.

43 *Ibid*, s 89.

44 Schedule 5, Part 10 of the amended *Broadcasting Services Act* 1992 (Cth) provides for the review of ABA decisions by the Administrative Appeals Tribunal.

45 Note 2 *supra*, s 10(1)(b).

46 *Ibid*, s 4(1) and (2).

47 EFA, "Comments on Australian Broadcasting Authority (ABA) Consultation Paper on Restricted Access Systems", <www.efa.org.au/Publish/ABAresp9911.html> at 9 November 1999 (Copy on file with author).

Online Services Act will exacerbate Australia's online isolation and diminish our position in the global e-commerce milieu.