

Online legislation is an Iron Curtain

Delia Browne, executive director of the Arts Law Centre of Australia, explains what the draft legislation means to the online industry in Australia, and highlights some of its problems

The government's *Broadcasting Services Amendment (Online Services) Bill 1999* aims to enforce the blocking and removal of certain illegal or offensive material hosted by computers connected to the Internet in Australia, moving all objectionable content outside Australia and building a fortress with an army of conscripted Internet Service Providers (ISPs) to block access to such content outside Australia. ISPs and Internet Content Hosts (ICHs) are the most easy and visible targets in the battle to control access to and regulate Internet content.

The proposed framework

The Bill has four main objectives: to create an industry code of practice; provide a means for addressing complaints about Internet content; establish an Australian Broadcasting Authority-based (ABA) regulatory regime; and to block certain Internet content - that which is likely to cause offence to a reasonable adult or is unsuitable for children.

The ABA, rather than the offending ISP, will be the first point of contact for complaints about content. The government also intends to establish a community advisory body to monitor online material, supply advice about the complaints mechanism, provide community education and information, for example about filtering products, and operate a public complaints hotline to receive information about offensive material.

At first glance, the Bill is aimed at ICHs, defined as anyone who hosts Internet material in Australia. Although the explanatory notes of the Bill expressly exclude newsgroups, Brendan Scott, an intellectual property specialist at Gilbert & Tobin, states that *prima facie* anyone who has an email account is an Internet host and that all material on their computer will be subject to review because it is all available for access via an Internet carriage service (in that it can be emailed to anyone). The Bill is therefore somewhat tougher than the legislation that applies to broadcasting.

The complaints scheme will be administered by the ABA which has been given the power to monitor the Internet. Suspect material will be judged on the basis of ratings used for film and television broadcasting. Content that is classified R (which includes material that adults can rent legally from a video store) and hosted in Australia must be subject to a password protection scheme, permitting adults-only access. Overseas content is also subject to this restriction. If someone suspects that an ICH is not complying with the Act, they may complain to the ABA. The ABA is required to investigate the complaint and notify the complainant of the result. But the ABA is not required to notify the ICH of the complaint or the investigation. The ICH is not entitled to know the identity of the complainant.

If the ABA finds that content about which complaints are made falls into either RC or X classification, or R if there are not adequate adult verification procedures in place for getting access to it, the ICH is issued with an interim take-down notice. The ABA then awaits the views of the Office of Film and Literature Classification (OFLC). A final take-down notice is given if the OFLC decides that the content falls within one of the prohibited categories (see page 3 for more on this subject). The ICH must then remove the relevant content within 24 hours of the notice being sent. Under the anti-avoidance provision, the ABA can also stop the ICH from hosting substantially similar content.

Filter or not to filter

The Bill does not make filtering content by ISPs mandatory if it is not technically feasible or commercially viable. But it is almost impossible to identify in what circumstances it will be technically feasible or commercially viable for ISPs to block material. An ISP cannot easily stop the incoming traffic. It is not possible to monitor the enormous quantity of network traffic, literally thousands of emails, newsgroup messages, files and web pages that travel in various combinations of text and binary formats.

Impact on freedom of expression

Most Australians assume that they possess a general right of freedom of speech, when in fact there is only an implied guarantee of freedom of political communication under our Constitution. The implied right is not absolute and the High Court in *Lange v ABC* articulated the limits of the implied right - it does not extend to commercial speech or other material

such as parody or satire or artistic expression.

This Bill raises serious questions as to the status of freedom of expression in Australia as well as our vulnerability to invasions of privacy and access to confidential information. Interestingly, the ABA has invoked China and Malaysia as role models of online content and control.

Government legislative action that is primarily aimed at protecting children should not take the form of unconditional prohibition of content that is freely available to adults in other media. Innocent and educational sites and material may become casualties of blocking software. It is not technically possible to totally block pornography but it may make it easier to block out educational, artistic or politically inconvenient content.

The US government attempted to create a similar regime to regulate online content under the doomed *Communications Decency Act 1996* which was struck down as unconstitutional in 1997 in *Reno v American Civil Liberties Union*, 117 S Ct.2329(1997).

Current laws

Existing legislation does cover illegal activities on the Internet. There are no illegal activities that become less illegal on the Internet. *The Classifications (Publications, Films and Computer Games) Act 1995* (Cth) requires mandatory classification of all computer games as with film and videos before they can be sold or hired or demonstrated in a public place. It also prohibits people from knowingly accessing or transmitting objectionable material such as child pornography or restricted material to a person under the age of 18.

Various state and territory legislation also prohibits the distribution or publication of obscene or indecent material, with some creating offences specific to the Internet. There has been successful prosecution of offenders possessing illegal pornography on computers and it is

arguable whether the additional state legislation will lead to further successful prosecutions.

E-commerce bloc

The government contends that the proposed regime will not inhibit the development of the online economy. But it fails to recognise the effect of these regulations on small and medium ISPs. Australia's primary Internet trading partner is the US and the government's fortress approach may impede online trading with America and other trading partners. Imposing costs on ISPs through enforced regulation or capital expenditure for equipment to block sites and deployment of additional resources to monitor online content will effectively make the local Internet industry less competitive.

Another failing of the legislative initiative is that it treats the Internet as a jurisdiction that can be defined by geography. Australian law can only bind and govern those people within Australia's geographical boundaries.

What is the alternative?

In a recent article in the *Stanford Law Review* David Johnson and David Post suggest that the most effective way to regulate cyberspace is to classify it as a physical place and subject it to a separate jurisdiction. The effect of logging on would be the same as crossing a state or national border - cyber laws apply equally to all users irrespective of where they log on.

A separate cyberspace jurisdiction could be created through internal cooperation and treaties. Such networks are already in place, policing online criminal activity and regulating e-commerce. In the UK, for instance, the police were successful in identifying an international paedophile ring as a result of substantial online collaboration between various national police forces.

The need for international cooperation was highlighted in the CSIRO report *Blocking content on the Internet*

- *A Technical Perspective* prepared for the Federal Government and presented in June 1998. The report stated that blocking Internet material would be ineffective and that effective filtering would only work where suitable policies and supervision were in place. Effective policing of objectionable material requires the cooperation of overseas regulatory bodies. It should be noted that in light of the *Reno v ACLU* case, the US will not be able to ratify an international treaty that attempts to regulate online content if the treaty infringes the First Amendment and, therefore, any such law would held to be unconstitutional.

Conclusion

The online community is grappling with a paradox. On one hand, the Internet is promoted by the government as an economic goldmine ripe for prospecting by Australian business. On the other, it is viewed as an anarchic place rife with paedophiles, racist and Nazi propaganda, drug pushers and bomb makers. "The Internet - a great place to do business but I wouldn't want my children to play or shop there".

The proposed legislative fortress promised salvation from highly offensive and illegal online material but in reality delivers little in the way of protection. Parents and teachers will still need to supervise children and be responsible for protecting them from accessing pornographic and other content they consider harmful to their development. No government censorship can replace or abrogate parental and community control and responsibility.

Whether the Internet will enhance or retard freedom, culture or business will depend on the rules under which it operates. It is all very well to designate and arm a watchdog, but who watches the watchdog? <

Delia Browne