benefits that have flowed from the Internet and will:

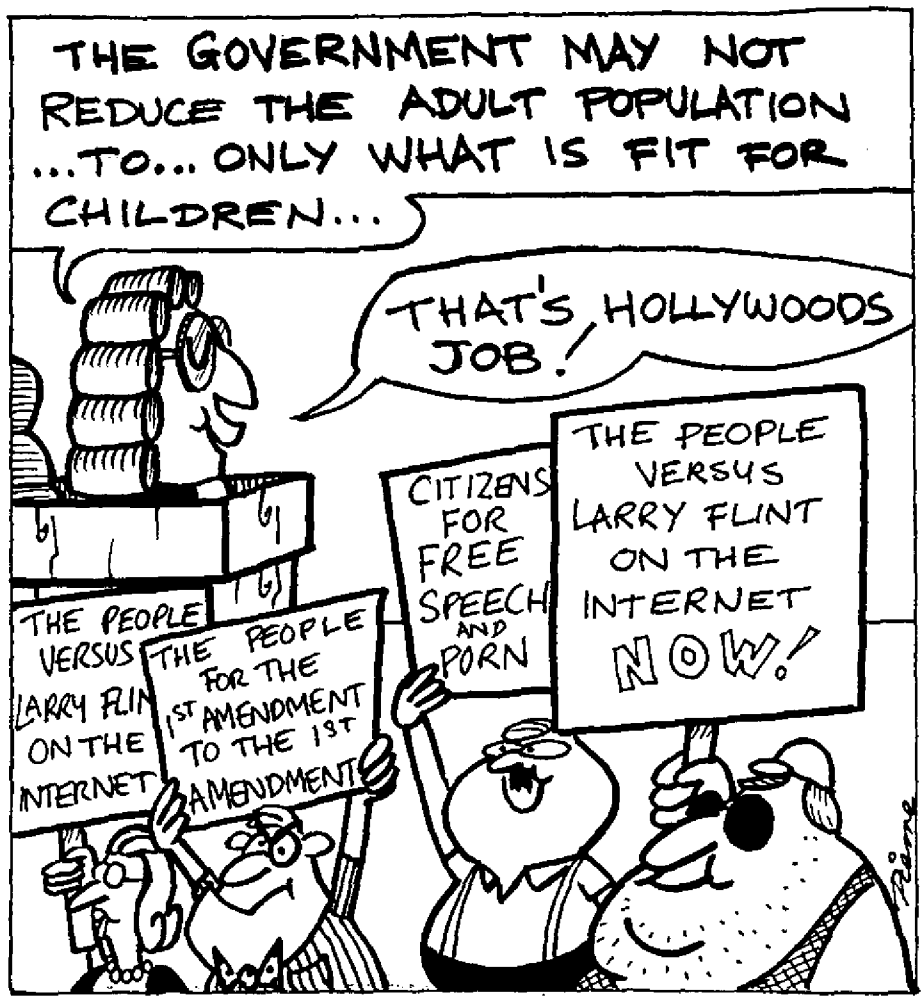
> *"threaten to torch a large segment of the Internet community."*

Judge Stewart Dalzell in the District Court wrote in part:

> *"If the goal of our First Amendment jurisprudence is the 'individual dignity and choice' that arises from 'putting the decision as to what views shall be voiced largely into the hands of each of us', then we should be specially vigilant in preventing content-based regulation of a medium that every minute allows individual citizens actually to make those decisions."*

The Supreme Court accepted this approach and rejected the Government's argument that availability of "indecent" and "patently offensive" material on the Internet is driving countless citizens away from the medium because of the risk of exposing themselves or their children to harmful material.

John Corker is a legal officer and Pauline Sala is a legal assistant at the Australian Broadcasting Authority.



Self-regulation v. Censorship – ISPs & Internet Content Legislation in Australia

Andrew Lambert looks at the differing approaches taken at a State and Federal level with regard to the censorship of on-line content and some of the implications for Internet Service Providers.

Internet enthusiasts may argue the intrinsic value of free expression and the benefits of the free flow of information. However, this is not nearly as newsworthy as the idea of technologically literate kids surfing an Internet awash with pornography, neo-Nazis, paedophiles and bomb-making recipes. Media focus on the potential for the Internet to expose minors to harmful or inappropriate material has understandably led to concern in the community.

Politicians at a State and Territory level in Australia, responding to the imperative of such media attention, have taken an interventionist approach and have moved to censor content on the Internet. The Federal Government has been more reluctant to regulate on-line services, preferring to promote industry self-regulation and to refer specific issues, including copyright, to a variety of advisory bodies. The past few years have seen a profusion of Government enquiries relating to Cyberspace issues.

The most important has been the *Investigation Into the Content of On-line Services* by the Australian Broadcasting Authority (**"ABA"**) released on 30 June 1996 (the **"Report"**). This seems to have been adopted by the Federal Government as its preferred approach (discussed below). This has not prevented Victoria, Western Australia and the Northern Territory passing specific laws relating to content on the Internet.

State and Territory moves for On-line Censorship Laws

Recently there have been concerted moves by various States and Territories to introduce specific criminal offence provisions in relation to on-line content in Australia, which have attempted to co-ordinate their legislative response through the forum of the Standing Committee of Attorneys General ("SCAG"). However, there is some doubt as to whether the States and Territories actually have the power to do so given

that section 51(v) of the *Constitution* has been held to reserve the power to regulate communications of all kinds to the Commonwealth.

In 1996 SCAG proposed the development of model criminal offence provisions which would be introduced in a co-operative scheme between the States and Territories.

The New South Wales Parliamentary Counsel's Office drafted a discussion draft of criminal offences ("**Model Offence Provisions**") at the request of Ministers in charge of censorship in the various States and Territories following SCAG discussions.

The draft Model Offence Provisions proposed to make it an offence to send, receive, permit access to or retrieve "objectionable material" through an "on-line service". The provisions were subject to considerable criticism by the on-line services industry on the basis that they were generally unworkable. Although ostensibly designed to catch people who introduce offensive material on-line they effectively shifted criminal liability onto on-line service providers.

Phillip Argy of the Australian Computer Society commented that the Model Offence Provisions were the equivalent of making:

> *"Australia Post liable for carrying objectionable material inside sealed envelopes, Telstra liable for what people say on the telephone, local councils liable for what the public puts on community bulletin boards, shopping centre owners liable for what shopkeepers do in their shops and everyone criminally liable for the contents of unsolicited mail they receive".*[1]

Much to the relief of on-line service providers ("ISPs") the introduction of the Model Offence Provisions was postponed at the meeting of SCAG on 11 July 1996 following the release of the findings of the ABA Report. However on 9 July 1997 the annual meeting of SCAG announced that they may revive the project of drafting uniform national censorship legislation to deal with on-line services.

The ABA Report

Fortunately for the on-line community in Australia and ISPs in particular, the ABA Report seems to have forestalled any further cooperative legislative activity by SCAG and the States and Territories.

The key elements of the Report were:

(1) that the most appropriate approach to the regulation of on-line services content is a self-regulatory approach based on ISP industry codes of practice;

(2) the identification of matters which should be included in codes of practice for ISPs, which provide appropriate community safeguards, including complaints handling procedures;

(3) the registration by the ABA of such codes of practice, developed by ISPs after a process of public consultation; and

(4) the monitoring of the codes of practice and their effectiveness by the ABA.

The ABA recommended that compliance with any applicable industry code of practice should be provide a defence to an ISP in any prosecution under any State or Territory censorship laws, where such industry codes of practice were registered by the ABA. This was to occur as part of a co-ordinated regulatory and enforcement strategy applicable to the on-line industry.

The Report recommends that a complaints handling regime should be developed specifically for on-line services.

A range of matters which ISPs need to include in their codes of practice were identified including age verification procedures intended to limit the holding of an open line account to persons over the age of 18 to prevent children's access to open on-line services without adult supervision. Reasonable procedures to deal with objectionable material are to be adopted including practical steps which can be taken in respect of objectionable material once an ISP was made aware of that material. However, the ABA recognised that in some circumstances the measures which ISPs could take in relation to this material were limited.

In considering strategies to limit children's access to material which is unsuitable for them, the ABA offered encouragement for the Platform for Internet Content Selection ("**PICS**") which is an Internet protocol which can support the labelling of Internet content. This allows content providers to rate their web pages and for third parties to rate pages on the basis of a preset criteria. Parents or educational facilities can use this to screen access to unclassified pages or to pages with a rating which they consider inappropriate for their children or students. Parents can rely on self-classification by content providers according to this protocol or in accordance with a third party classifier whose moral viewpoint they agree with.

Other software is available which blocks access to sites which are based on PICS, including Cyber Patrol, Safe Serve, Net Shepherd and Net Nanny. They are combinations of filter software and labelling schemes for sites which provide parents and educational institutions with periodic notifications of problem sites.

The Report was widely praised in the on-line community and by ISPs. Since its release last June a number of Internet industry associations have commenced the process of drafting codes of practice which aim to meet the requirements of the ABA including:

- the Internet Industry Association of Australia;
- the Committee of University Directors of Information Technology; and
- the EROS Foundation.

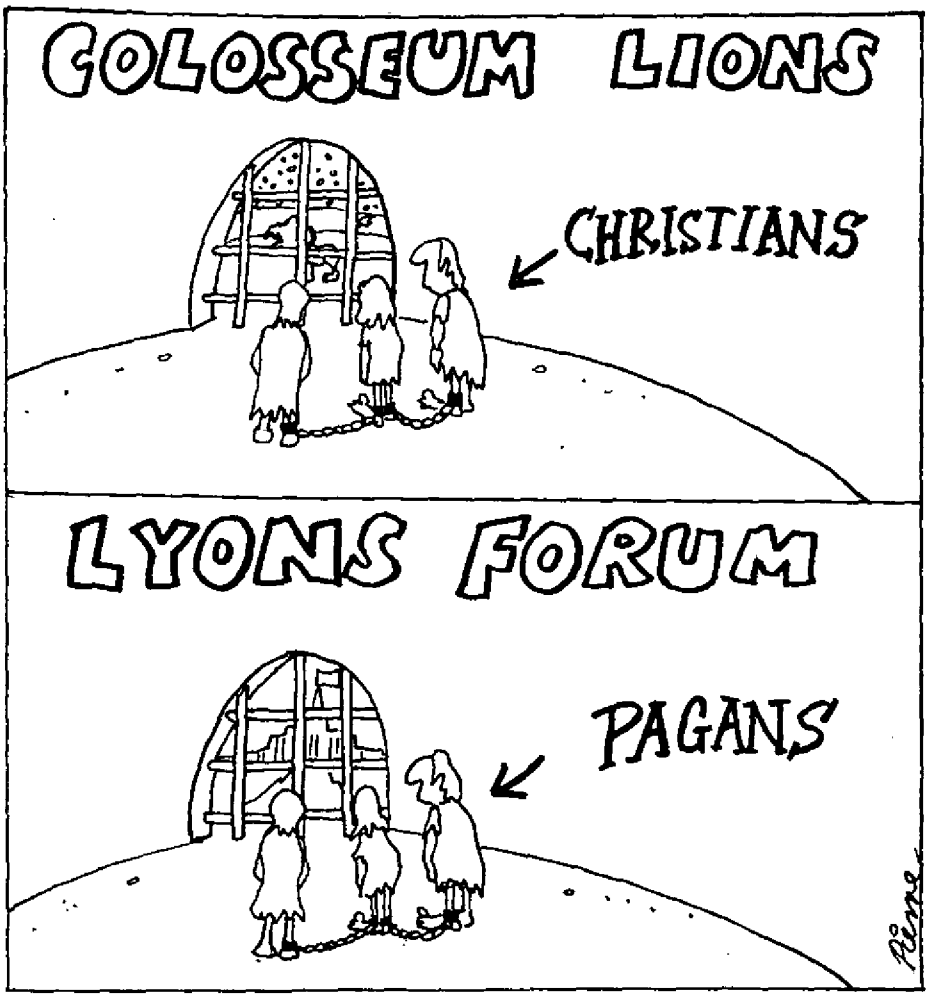
The Senate Committee Report

Just when the Cyberspace and its denizens in Australia were breathing a collective sigh of relief after the ABA Report (and the US Supreme Court's upholding of the US District Court for the Eastern District of Pennsylvania's decision in *Reno v ACLU*)[2], the Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technology (the "**Committee**")[3] delivered its report in June 1997. Deeply concerned with community moral standards, the Committee represents the other end of the spectrum on theories of the appropriate way of controlling on-line content to those of the ABA. Its recommendations included:

(1) fines of up to $100,000 per offence for the electronic transfer of pornographic or other "offensive material";[4]

(2) that on-line service providers be held responsible for on-line material;[5]

(3) that all States and Territories amend their classification and



censorship legislation to make it an offence to transmit objectionable material and to cover the transmission of material unsuitable for minors through computer on-line services, in a uniform manner;[6] and

(4) that specially designated units of State and Territory police forces should conduct random on-line checks to detect illegal activity.[7]

Federal Government Policy

However, the Federal Government appears to be following the path recommended by the ABA Report. On 15 July 1997 the Minister for Communication and the Arts, Senator Richard Alston, and the Attorney General, Mr Daryl Williams, announced principles for a national approach to regulate the content of the Internet based on the ABA's Report and on-going industry consultation.

The framework will be based on industry-developed codes of practice which will be supported by relevant amendments to the *Broadcasting Services Act* 1992 ("BSA"). The principal elements of the Commonwealth's approach include:

(1) facilitating the establishment of on-line industry codes of practice, incorporating an "effective, appropriate and fast complaints procedure";

(2) pursuing the development of international collaborative arrangements, such as PICS, industry codes of practice and industry forums;

(3) encouraging greater community awareness and fostering education programs; and

(4) encouraging the States and Territories to adopt an approach which is supportive of Australia's industry-based scheme, through both SCAG and the new "On-line Government Council".

The ABA will be the industry regulator to implement and monitor the national scheme. The BSA will be amended to provide the on-going authority for the ABA to work with the industry in developing codes of practice and as the industry co-ordinating body within the Federal Government.

The proposed arrangements recognised that ISPs were often not in a position to be aware of all material transmitted through their service and cannot be held responsible in every case for material they have not created. ISPs would meet their obligations by complying with industry codes of practice and acting quickly to resolve complaints.

Existing State and Territory Legislation relating to On-line Content

Victoria, Western Australia and the Northern Territory have all passed legislation directed at on-line content, either prior to or subsequent to the ABA Report. Western Australia and the Northern Territory's legislation was based on the discredited Model Offence Provisions.

The problem with all three pieces of legislation arises from determining where a breach is said to have occurred. Is it where the material is "transmitted" (uploaded on to the Internet) or where it was downloaded? This legislation has no extra-territorial effect and cannot prevent the transmission of such material into Victoria, Western Australia and the Northern Territory from other Australian jurisdictions and from outside Australia, if such material is legal in those jurisdictions. Serious questions about conflict of Australian law would arise should the relevant Police attempt to prosecute ISPs who intentionally or unintentionally provided access to material which is prohibited under local laws from servers located outside the jurisdiction.

The Western Australian and Northern Territory legislation create offences of transmitting "objectionable material" or "restricted material" to a minor or making restricted material available to a minor. The legislation does not define "transmit" but their definition of "computer services" is so wide it could catch any level of ISP (though not the telecoms carriers themselves). The breadth of the relevant definitions in the Western Australian and Northern Territory legislation for "computer service" would also apply the prohibitions on the transmission of "objectionable" or "restricted" material to e-mail.

The problem with this legislation as enacted is that it creates a strict liability offence placing the onus on ISPs to establish a defence. The Victorian act is different in that the offence is that of "knowingly" creating, publishing, transmitting or making available on-line objectionable material or material

unsuitable for minors, the onus being upon the prosecution to prove the element of knowledge.

The Northern Territory and Western Australian legislation assumes that on-line service providers are exactly aware of what is flowing across their networks and who exactly is accessing all relevant information, including the content of e-mail messages.

None of the means and protocols for accessing information on-line - e-mail, list servers, browsers, web-crawlers, search engines, indexes, bulletin boards, news groups, chat lines etc. - can effectively track the millions of users and screen out those under 18. ISPs could possibly age verify their own Internet subscribers but do not have the technical or human resources to control or even monitor the content of their subscriber's websites and communications in anything more than a random fashion. Nor can they be certain of preventing minors accessing materials on the Internet through the subscribers' terminals, whatever PIN or restrictive identification processes were adopted.

Other problems with the Western Australian and Northern Territory legislation are their definitions. The definitions of "objectionable material" includes by reference to material classified "RC" under the *Classification (Publications, Films and Computer Games) Act* 1995 (Cth) or that would if classified be so classified. This raises a question of how a person could be found to have knowledge of how unclassified material would be classified when the classification structure on which it is based is a subjective guideline. It may be difficult for a prosecution to prove the necessary criminal intent in respect of material that has not been classified by the Office of Film and Literature Classification (as is the case of virtually all material on the Internet).[8]

However, this may not be of much comfort with potential penalties for ISPs of up to $15,000 and 18 months imprisonment for individuals and up to $75,000 in other cases for the transmission of "objectionable material" by its users of which it had no actual knowledge. A more likely course of action is that large ISPs may simply avoid establishing their servers or Internet business operations in Western Australia or the Northern Territory.

Conclusion

The approaches adopted by the Federal Government and the States and Territories reflect the differing regulatory models of content specific and content neutral regulation.

The Senate Committee clearly has an agenda in imposing its moral strictures on a new medium the reality of which they do not understand and the primary feature of which - the free expression of ideas - they are profoundly hostile to. State and Territory politicians have responded to the spectre of Net pornography conjured by media reports with a knee-jerk regulatory response. Together these groups have attempted to apply traditional censorship laws developed to control content on the print and broadcast media to the Internet. Chasing headlines and sound bites is no way to draft policy and the ill-conceived Model Offence Provisions and the Western Australian and Northern Territory legislation it influenced are the result.

It is clear that applying censorship standards based on film and broadcasting content regulations to ISPs as if they were newspaper publishers or TV stations is inappropriate. However, merely treating them as a conduit akin to a telecommunications carrier removes obligations which the ISPs which do exercise editorial control over content on their services should rightfully be subject to.

It may be that the Internet as a new medium of communications needs new regulatory paradigms to control the content which can be accessed in Cyberspace. ISPs must play their part in preventing transmission of criminal material (especially child pornography) and restricting the access of minors to unsuitable material. However, this burden cannot be totally moved by regulators onto one component of the Internet, as has been attempted in the Northern Territory and Western Australia.

Industry self-regulation seems to provide a regulatory stop-gap until legislators can become more familiar with the working realities of this new medium rather than the hyberbole which surrounds it. Industry self-regulation also provides a safe haven for ISPs from the liability stemming from some State and Territory legislation. Most importantly it provides a forum in which the industry may be able to determine the most appropriate regulatory mechanism to govern it.

Federal Government policy favouring this approach seems, for the moment, to have given ISPs and industry groups breathing space in which to do so and to prove that they can act responsibly. They would be well advised to take advantage of it before the opportunity is lost.

Unfortunately, until a more equitable distribution of legal responsibility is effected by regulators, ISPs would also be well warned to avoid establishing their operations in jurisdictions which assume they can control or are even aware of the content that their subscribers are accessing and uploading via their services.

Andrew Lambert is a lawyer with the Sydney office of Deacons Graham & James. The views expressed in this article are the author's own and do not necessarily represent those of Deacons Graham & James.

1 Argy, Phillip "Internet Censorship Proposals" hhp:/www.msj.com.au/argy/intreg1.htm1.

2 No. 96-511, 26 June 1997.

3 Committee members include Senators Brian Harradine and John Tierney.

4 Recommendation 4.

5 Recommendation 1.

6 Recommendation 8.

7 Recommendation 9.

8 Op. cit. Argy.