Australia's Internet content regulation in the International context

Carolyn Penfold, Lecturer, University of NSW

Carolyn Penfold is a Lecturer in the Faculty of Law at the University of New South Wales, and a Research Associate of the Baker and McKenzie Cyberspace Law and Policy Centre at the University of NSW. Carolyn is currently conducting research into the effects of the Online Services Amendment to the Broadcasting Services Act on freedom of speech in Australia.

1. Introduction

The title of this paper itself raises an interesting contradiction. Firstly, it is repeatedly said that the internet, as a global phenomenon, cannot be effectively regulated except in the global context.[1] To a great extent this is of course true, in that there are no physical or geographical boundaries on the internet, and thus traditional ideas about territorial limits do not hold true. Consequently, when we look at any kind of regulation or censorship of material on the internet, we do need always to look to the international context.

On the other hand however, there is a very marked lack of 'international context' in internet content regulation. While we are now beginning to see some efforts to extend legislative schemes beyond individual borders, there has not been any real 'international' movement toward agreement in this area. Thus to a great degree, countries like Australia wishing to introduce content regulation have really been able to act only within the local context. In the absence of international agreements or norms, they have needed to take individual action to deal with 'problematic' material emanating from both within the country and outside.[2]

This paper briefly outlines the current Australian scheme for content regulation, then goes on to examine what other nations have done in their attempts to control content which they find problematic. The difficulty of negotiating international agreements in this sphere is discussed, and suggestions are made for re-thinking Australia's content regulation scheme.

2. A brief overview of the Australian scheme for regulating internet content

The *Broadcasting Services Amendment (Online Services) Act* 1999 (Cth)[3] (***"Online Services Amendment"***) came into force in July 1999, with substantive provisions taking effect from 1 January 2000. The scope of the legislation can be broken into three main parts:

a) censorship and content regulation - initiated by complaints from the Australian public;
b) the creation of industry codes of practice; and
c) community education – the responsibility for which was largely given to NetAlert, a body set up specifically to undertake this role, but shared with the Australian Broadcasting Authority (ABA).

2.1 Provisions of the *Online Services Amendment* and Codes of Practice.

Under the *Online Services Amendment*, censorship and regulation of internet content is intended only to be initiated by complaints. While the ABA can investigate and take action as a result of those complaints,[4] it is not intended that the ABA will actively monitor internet content for censorship purposes. [5]

Complaints may be made about prohibited or potentially prohibited content accessible via the internet.[6] The Act defines 'prohibited content' to include Australian hosted R-rated material which is not subject to a restricted access scheme, and all material rated X or RC,[7] wherever hosted.[8] 'Potential prohibited content' is unclassified content which, if classified, would be substantially likely to be prohibited content. [9]

When a complaint is received about material which is prohibited or potentially prohibited, the ABA takes different action depending on where the material is housed. If such material is hosted within Australia, the content host will be given a notice to remove the material from the site.[10]

For material hosted outside Australia, s40(1) of the *Online Services Amendment* provides (in summary) that if in the course of an investigation,the ABA is satisfied that Internet content hosted outside Australia is prohibited content or potential prohibited content, the ABA must:

a) refer anything sufficiently serious to a law enforcement agency;
b) if an industry code is registered, notify the content to Internet service providers under the designated notification scheme set out in the code; and
c) if paragraph (b) does not apply, give each Internet service provider known to the ABA a written notice directing the provider to take all reasonable steps to prevent end-users from accessing the content. [11]

It appears from the wording of the legislation that the Australian Government actually intended that steps be taken to prevent internet users from accessing prohibited or potentially prohibited content. The legislation did not specify how this was to be done, only that 'all reasonable steps' should be taken to that end.

However, the Industry Codes of Practice (**"Codes"**), written by the Internet Industry Association and registered by the ABA just before the

complaints scheme came into effect, significantly soften the blow to industry which the legislation may otherwise have made.[12] Once the Codes were registered, s40(1)(b) came into play and internet service providers (ISPs) had then to comply only with the Codes, rather than with s40(1)(c) which now had no application.

The Codes registered by the ABA state that ISPs will be taken to have complied with the legislation in regard to overseas-hosted content if they provide for their users a content filter, or filtered ISP service. They need not take steps to block prohibited or potentially prohibited material. The ABA notifies makers of the approved filters that the material in question is to be blocked, and the makers undertake to include notified material in their filter block lists. There is no obligation on internet users to use the filters or filtered services.

So in effect, while prohibited and potentially prohibited material (X and RC material, and R material without a restricted access system) cannot be hosted in Australia, there is no censorship or regulation under this legislation of any material hosted outside Australia. (There may of course be restrictions under other general legislation, for example restrictions in state Acts on selling or possessing child pornography). Internet users, adults and children alike, can freely access any material they wish from overseas sites. If they choose to use a filter, they may filter out some problematic material, but filter products have proven so unreliable that they could not really be used as a means of stopping access to problematic content.[13]

3. Overseas Regulation and Censorship

To understand Australia's internet content legislation in the international context, it is necessary to look to the various methods currently used around the world for censoring and regulating internet content. Although no international agreements or rules presently exist in this sphere, many countries have attempted to regulate or censor internet content in a multitude of ways.

3.1 Methods of censorship and regulation

One method by which some countries control access to content, is to allow only a trusted few to have access to computers and internet connections. In Myanmar (formally Burma) it is forbidden to access the world wide web, unauthorized use of a modem is punishable by 7 to 15 years in jail, and email is restricted to fewer than 1000 people close to the ruling party (SPDC).[14] In Cuba, the number of Cubans using the internet has grown steadily but, as Drake noted:

> "the potential pace of growth is limited by public policy allowing internet access only through approved institutions – select universities and places of employment. This policy ensures that the internet is used mainly by the politically trustworthy, and only in environments where use can be informally monitored. There are still no Internet Cafes allowed in Cuba, and individual access is prohibited, beyond a few well connected individuals who work out of their homes. Essentially, internet diffusion in Cuba is determined by government policy rather than the market..."[15]

In other countries, all information coming into the country via the internet is required to be routed through a government monitored server, so that the Government itself has direct control over monitoring and blocking material it deems problematic. The United Arab Emirates apparently forces all internet traffic through a single gateway.[16] Saudi Arabia spent almost two years developing the technology necessary to filter almost all web data entering the country through a central server.[17]

Another method employed to control access to content is to allow easy access to computers and to the internet, but allow only licensed or registered ISPs to operate. Conditions for operating ISPs can be very strict, and can include requirements for monitoring and blocking material. For example, regulations announced by China late last year require ISPs to be registered, to keep records for two months of all content which appears on their web sites and of all users who dial onto their servers, and hold ISPs responsible for blocking vast categories of internet content.[18] Singapore also requires registration of ISPs and has stringent rules about what material should be blocked by them.[19]

Still other countries have allowed and indeed encouraged unrestricted access to computers and to the internet, and have encouraged a growth in ISP and Internet Content Host ("**ICH**") numbers to increase service levels and competition. However, they have then tried to regulate access to specific content or types of content through legislation aimed at controlling various combinations of content providers, content hosts, ISPs, and those accessing material. Examples of this include the *Online Services Amendment* in Australia, the United States' *Communications Decency Act 1996*, ("**CDA**", which prohibited online display and transmission of indecent material to minors under 18 years of age) and the *Child Online Protection Act 1998*, ("**COPA**", which prohibited knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, making any communication for commercial purposes that is available to any minor and that includes any material which is harmful to minors). Both the CDA and COPA have been struck down as unconstitutional. The latest attempt in the United States is the *Children's Internet Protection Act 2000* (known as both "**CIPA**" and "CHIPA"). The aim of the CIPA is to force federally funded internet access (such as in libraries and schools) to be subject to content filters. However the CIPA may also be struck down.

Another attempt to control content where access to computers and the internet is freely available is the situation where general local laws (ie not internet specific) are used in attempts to stop content being made accessible. Such attempts have been

aimed at both ICHs and ISPs. Examples include the decision of a French court against Yahoo,[20] and the decision of a German court against Frederick Tobin.[21] In both cases the legislation used was not in any way related to the internet, but the internet 'happened' to be the source of the material at issue.

In other instances, hotlines have been set up which take complaints about allegedly illegal material online, and which then act as conduits for channeling that information on to police and other law enforcement agencies. These hotlines, established 'to prevent illegal activity and abuse of children', have become so common in Europe that INHOPE (Internet Hotline Providers of Europe)[22] has been established with support from the European Commission to provide a forum for hotline providers to share their experiences and concerns. Such a hotline also runs in the United States (Cybertipline)[23] and aims to encourage the reporting of trafficking of child pornography and online solicitation of children, and to allow that information to be passed on to various international law enforcement agencies. The various hotlines draw some funding from government but have also been supported by funding from the private sector. They have not required legislative backing as the hotlines are concerned about material and behaviour which is illegal per se, not just because it is on the internet.

The most 'international' approach to regulating internet content is the treaty currently being drafted by the Council of Europe, known as the Draft Treaty on Cybercrime,[24] which would require signatories to:

(1) make criminal certain behaviour relating to computers, and
(2) set up frameworks for the prosecution of such offences.

While this has been both hailed, (at last a step toward controlling what happens on the internet) and decried (losing sovereignty and individuality to other states or the international community), it appears that this treaty will also do little to regulate online content even within signatory states. The only section of the treaty which deals with content related offences in fact deals only with child pornography. Article 9 Paragraph 1 of Title 3, "Content-related offences," requires signatories to establish the following acts as criminal offences:

a) producing child pornography for the purpose of its distribution through a computer system;
b) offering or making available child pornography through a computer system;
c) distributing or transmitting child pornography through a computer system;
d) procuring child pornography through a computer system for oneself or for another; and
e) possessing child pornography in a computer system or on a computer-data storage medium.

Article 9, Paragraph 2 of Title 3 states that for the purpose of Paragraph 1, "child pornography" includes pornographic material that depicts:

a) a minor engaged in sexually explicit conduct:
b) a person appearing to be a minor engaged in sexually explicit conduct; and
c) realistic images representing a minor engaged in sexually explicit conduct.

Article 9, Paragraph 3 of Title 3 states that the term "minor" shall include all persons under 18 years of age. While Article 9 appears minimal at most, signatories have the right to implement laws that fall short of these standards. Signatories may specify a lower age limit, defining a minor as under 16 rather than 18 years, and also need not apply, in whole or in part, paragraphs 1(d) and 1(e), and 2(b) and 2(c).

Therefore, the minimum required is, that signatories must establish as criminal offences:

a) producing child pornography for the purpose of its distribution through a computer system;
b) offering or making available child pornography through a computer system; and
c) distributing or transmitting child pornography through a computer system,

where "child pornography" includes pornographic material that depicts a minor under 16 years engaged in sexually explicit conduct.

It is clear from the discussion above that many states around the world do wish to see some kind of content regulation, and are not happy for content on the internet to be a 'free for all.' Further, it is clear that those states wishing to see restrictions are not necessarily those states we would usually associate with restrictions on freedom of speech or information. However, the nature of the internet, its technological make-up, and its disrespect for the geographical boundaries of sovereign states, have made attempts to control content within individual states less than ideal. Unfortunately, heavy-handed and intrusive methods of content regulation seem currently to be the most effective in creating 'boundaries' for the spread of internet content. It seems that the more a nation feels threatened by content coming from outside, the larger the boundaries it needs to build to resist that threat. It may be then that if there were more international co-operation regarding internet content, more effective, and more refined, regulation may be possible.

4. International Agreements

Given the global nature of the internet, and given the desire of so many states to control its content, why haven't there been more moves toward international agreements in this sphere? There are a number of reasons, which include varying levels of infrastructure for information technology and communications, domestic or internal restrictions on states, social and political expectations within and beyond individual states, existing domestic regulatory policy, and differing governments' intentions.

However, most of these difficulties exist for any agreement being negotiated at an international level, and clearly such difficulties *can* be overcome or there would not be any international agreements. But in the case of internet content regulation, a

further difficulty is the extreme variation in what each country wants regulated, and why.

Apart from child pornography (which is addressed in the Draft Treaty on Cybercrime) and perhaps even excluding that, it would be impossible to find even one type of content that all, or even most nations, believe should be censored. For example, France and Germany do not want their citizens to access hate speech/ vilification/ nazism, but free speech principles in the United States protect these forms of speech; probably no country wants its citizens to access child porn, but there is no consensus between countries regarding access to other types of porn; pro-democratic material would be freely available in some countries yet not in others, likewise anti-democratic material, pro-communist material and so on. As Lessig and Resnick note:

> "What constitutes "political speech" in the United States (Nazi speech) is banned in Germany; what constitutes "obscene speech" in Tennessee is permitted in Holland; ...what is harmful to minors in Bavaria is Disney in New York."[25]

Like the Draft Treaty on Cybercrime, it appears then that any international agreement aimed at censorship would need to aim at the level of the lowest common denominator. However, chances are that the lowest common denominator is already illegal and punishable in most countries.

Even if some kind of international agreement could be reached, due to the nature of the internet, content could only be censored if every country censored it. If all but one country stopped hosting the material, it would still be available. If that one country is small and unimportant, perhaps all other countries would be willing to block all communications coming from that country, and coming from any country which doesn't block communications coming from that country.

But what if that country were the United States? The ABA claims that 80% of the prohibited and potentially prohibited content notified to it in the 6 months to December 2000 was housed in the United States,[26] and the UK Internet Watch Foundation has come up with similar figures. Two attempts by the United States to regulate internet content (ie CDA and COPA) have already been knocked down. It seems unlikely that the Unites States could possibly agree to regulate anything but the barest minimum.

5. Alternatives

It may not be possible to reach international agreement on censorship, but there may be scope for negotiating other international agreements which increase the ability of individual countries, and individual internet users, to make more effective decisions about regulating internet content for themselves.

Suggestions have been made for 'zoning the internet' by delineating areas as adults only areas or kid safe areas. Technology already allows for various user profiles to be set up on a computer and such profiles, selected by adults or supervisors, can identify the user of a given password as a child.[27] In this way, sites themselves could be required to deny entry to child internet users, or could allow access only to certified adult users. The adult verification system used for Australian hosted R-rated material under the *Online Services Amendment* is an example of such 'zoning,' (for locally hosted material). This adult zoning has been strongly criticized as unnecessarily cumbersome,[28] and the alternative child zoning has generally been preferred.

However, the use of an adult verification scheme, or a child identification scheme, would still require agreement between governments, or within the internet industry itself, that sites be appropriately identified. This again raises the question of what is or isn't appropriate for a child or an adult to view. Furthermore, it is a particularly coarse method of regulating internet content; whole sites are deemed suitable or unsuitable for children, with no distinction between the ages of various children, nor of what their families or communities might think appropriate for them to view.

Geographic zoning could also be a possibility. Following the decision of the French court in *LICRA et UEJF vs Yahoo! Inc and Yahoo France,*[29] it appears it may be possible to zone sites as, for example, complying with French law, Japanese law, or Australian law or alternatively, as not complying in which case the sites would be required to block users from specific locations. The technological possibilities of geographical blocking were canvassed by three experts who concluded that it could possibly be as much as 90% accurate. It is a development of which we are likely to hear a lot more.

Less coarse than zoning, and allowing more individual control over content selection, is the idea of labelling. In the late 1990s there was a strong movement internationally toward the development of a content labelling scheme. Prior to the *Online Services Amendment*, the ABA had itself concluded[30] that the Government should support further development of such a system, which would allow labelling of content by owners and providers, or by third parties. This type of system would then allow internet users themselves to decide which categories of material they want to access or restrict.[31] The ABA's 1996 report listed many advantages of labelling, and went on to strongly support it as the preferred method of regulating internet content stating:[32]

> "It seems to offer parents and supervisors a method of protecting minors from material which may be inappropriate for them, allows adults themselves to be shielded from material which they do not wish to view, whilst at the same time maximising freedom of speech and choice for ... users who do not want to have their access to Internet content unduly limited."[33]

Such schemes have the potential to offer a more refined basis for content selection, and to allow users more responsibility in this sphere. This view is supported by Senator Alston who

said in 1998 that the Government was 'pursuing international collaboration to establish content labelling and filtering standards worldwide. These standards will give all users, and particularly parents, the power to identify and control the type of material to which they have access on the internet."[34]

This type of system is still being pursued in Europe,[35] and the latest ABA Report notes that a rating system 'which can be adapted to different national, cultural and individual needs' was launched last December.[36] A filter allowing parents to set their own controls will be launched sometime this year, 2001.[37]

The introduction of such a system would still require international agreement, but such agreement may be easier to reach as the system requires labelling but not censorship or control. While labelling would involve a number of keywords being assigned to content by content providers or by third parties, no choices would be made at that level as to what content was desirable, appropriate, dangerous etc. At the user level, or filter level, choices could be made as to what content could or couldn't be viewed.

An agreement on such a scheme may be less difficult to achieve than one requiring agreement regarding censorship. Also, unlike agreements on censorship which would work only if all nations agreed, agreements on labelling could be beneficial if sufficient labelling occurred to give a 'critical mass' of labelled material. Once there was enough labelled material on the internet, filters could be used to exclude unlabelled material, which would provide an incentive for others to label their material, whether or not their nation was party to an agreement. For this to work initially however labelling would need to be mandated in at least some of the major content providing nations; the United States would probably need to be involved. It would be necessary to apply sanctions for not labelling material, or for wrongly labelling material, but such sanctions might fall foul of freedom of speech rules in the United States and some other countries. Mandating the use of labels however has been criticized as providing an easy aid to government censorship.[38] It is said that once content providers are required to label their own material, it would be only a small step for governments to say all material with a particular label or labels is to be blocked by ISPs, or is illegal to access.[39] As a result, while agreements on labelling are still being heavily pursued in Europe, such schemes do not seem to be attracting so much support globally.

6. Changes to the Australian Scheme

For the moment individual countries wishing to regulate or censor content on the internet need to act for themselves, and we have seen from the above examples that many have done that. Most of those attempts however are, at most, only slightly more successful than the Australian scheme, if at all.

In Saudi Arabia for example, the two years work on blocking technologies was circumvented by SafeWeb, a technology that can mask the destination of requested information. Within weeks of SafeWeb becoming available, thousands of Saudi surfers were using it daily to access prohibited information. In fact, when the Saudi Government discovered and stopped access to SafeWeb, daily page-views dropped immediately from over 70,000 to zero.[40] Even without technology such as SafeWeb, monitoring can be circumvented by connecting through foreign-based servers, using satellite phones, or using File Transfer Protocal or "FTP". In Singapore, ISPs are required to limit access to 100 high impact pornographic sites as a statement of societal values.[41] Why not 10 sites, or 1000? How many such sites are still accessible? These attempts in both Singapore and Saudi Arabia are good examples of the ineffectiveness of many current attempts at internet content regulation and censorship.

The Australian *Online Services Amendment* is also ineffective. While a number of complaints have been made and take-down notices issued for content hosted within Australia, there has been no restriction placed on access to overseas hosted content, nor has there been any real improvement in the ability of individuals to regulate content for themselves. The Australian legislation however is hamstrung not only by a lack of international co-operation or even internet technology, but suffers also from a lack of clear objectives. The legislation had a number of aims, each emphasized to different degrees at different times. All of the following objectives could be ascribed to the *Online Services Amendment*:[42]

- to protect children from material likely to harm them;
- to give people an avenue of complaint and a feeling of redress;
- to make illegal online what is illegal offline;
- to encourage internet use;
- to restrict access to material likely to offend reasonable adults; and
- to appear to be doing something,

all without overly burdening industry.

It is quite unclear in the Australian legislation whether any of these aims are more important than others, and if so which ones are more important. However, avoiding a burden on industry has consistently been a top priority for government as Senator Alston stated in 1998:

> "In considering the best way to regulate cyberspace, the Government favours competitive market-based solutions wherever possible, that don't stifle innovation and growth with over-regulation. However, the Government also believes it has a role to ensure that the internet is a safe and secure place for all users, especially children."[43]

Unless the Government has a clear objective it is unlikely to achieve its aim. If the aim is to protect children from danger and exploitation, that will probably require different methods to the aim of keeping from adults material likely to offend any reasonable adult. If the aim is to

empower users to control their own online experience, different methods will be required from those which enable a government to control what users see. Objectives probably also need to be weighed against one another; are competitive market based solutions to be preferred even if they don't actually give children any protection? Is providing an avenue of complaint an objective in itself, or does it require that some effective resolution occurs as a result? These are the kind of questions which still need to be answered more than two years after the *Online Services Amendment* was introduced to Parliament.

Even once those aims are clarified and prioritised, the nature of the internet will make them difficult to achieve in the absence of international agreements. However, enacting ineffective legislation, and monitoring and enforcing that legislation, diverts resources and attention away from the real objectives. We will get no closer to protecting children nor empowering adults while time and money are spent on such legislation. These resources should be devoted to further developing useful internet technologies, and attempting to negotiate agreements which can actually make a difference.

7. Conclusion

Looking at the regulation of internet content in the international context, it is clear that nations wishing to censor or regulate online content have had to take their own steps to do so. Many different methods have been and are being used, many of which are ineffective, expensive, time-consuming, cumbersome, or more restrictive than is necessary to achieve their objectives.

Furthermore, international agreement on censorship or regulation of internet content is unlikely to occur as there is not sufficient commonality in what various nations want in this respect. However, some kind of international co-operation will likely be necessary if any real control over internet content, by individuals or by governments, is to be forthcoming.

---

1 See for example Peter Coroneos, 'Internet Content Control in Australia: Attempting the Impossible?' *UNSWLJ Forum, Internet Content Control* 6(1) March 2000 p26.

2 In discussions of content regulation or censorship, terms such as illegal, obscene, harmful, offensive, and dangerous commonly occur, often with little distinction being made between the terms. This paper, unless referring to a particular type of content or particular legislation, uses the term 'problematic content' to discuss content which nations may wish to censor or regulate.

3 Now incorporated to become schedule 5 of the *Broadcasting Services Act* (1992) (Cth).

4 *Broadcasting Services Act* (1992) (Cth) schedule 5 s27.

5 Second Reading Speech, Senate, 21/4/1999 (Official Hansard No 5 19/23 April 1999) p3960.

6 *Broadcasting Services Act* (1992) (Cth) schedule 5 s22.

7 Internet content is classified as film. Under the Australian scheme for the classification of films an R rating means 'unsuitable for a minor to see'; an X rating means 'unsuitable for a minor to see, and explicitly depicts sexual activity without violence, non-consent or coercion, and likely to cause offence to a reasonable adult.' RC means the film is or would be refused a classification. John Dickie, Director of the Office of Film and Literature Classification, 'Classification and Community Attitudes,' Centre for Media, Communications and Information Technology Law, Law School, University of Melbourne, *Research Paper No.5*, January 1998.

8 *Broadcasting Services Act* (1992) (Cth) schedule 5 s10.

9 Ibid s11.

10 *Broadcasting Services Act* (1992) (Cth) schedule 5 s30.

11 Ibid summary of s40.

12 Internet Industry Codes of Practice, registered by the ABA 16 Dec 1999, commenced 1 Jan 2000.

13 For further discussion of the problems with filters see C. Penfold, 'The Online Services Amendment, Internet Content Filters, and User Empowerment.' *National Law Review*. November (2000) NLR 7. <http://web.nlr.com.au/nlr/HTML/default.htm >

14 Sandy Barron, "Myanmar Works Hard to Keep the Internet Out." *New York Times* 14/7/2000.

15 William J. Drake, Shanthi Kalathil, Taylor C. Boas, "Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba." *Information Impacts Magazine*, Oct 2000 http://www.cisp.org/imp/october_2000/10_00drake.htm

16 Jennifer Lee, "Punching Holes in Internet Walls" New York Times, 26/4/2001.

17 Ibid.

18 "China's Iron-Fisted Internet Regs" *Wired News* 16th Oct 2000 http://www.wired.com/news/politics/0,1283,39192,00.html

19 Singapore Broadcasting Association, SBA's Approach to the Internet, <http://www.sba.gov.sg/work/sba/internet.nsf/ourapproach/1>

20 *LICRA et UEJF vs Yahoo! Inc and Yahoo France,* Tribunal de Grande Instance de Paris (Superior Court of Paris), 20/11/2000 <http://www.gigalaw.com/library/france-yahoo-2000-11-20.html>

21 Charges against Frederick Tobin relating to holocaust denial literature on the internet were dropped last year, when a German court ruled that as the relevant website was housed outside Germany the court had no jurisdiction. The Federal Court of Germany has now overturned that decision, stating that there is jurisdiction as the material can be accessed by users in Germany. ABC News Online, 'German Court Rules on Holocaust Revisionist.' <http://www.abc.net.au/news> accessed 13/12/00

Note that Tobin has also been ordered by HREOC to remove material on the Adelaide Institute website. A request for enforcement of that decision is currently before the Federal Court.

22 http://www.inhope.org/

23 http://www.missingkids.com/cybertip/

24 http://conventions.coe.int/treaty/EN/projets/cybercrime25.html

25 Lawrence Lessig and Paul Resnick, "Zoning Speech on the Internet: A Legal and Technical Model " 15/12/99 http://cyberlaw.stanford.edu/lessig/content/index.html

26 Australian Broadcasting Authority, *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation*, July to Dec 2000. April 2001

27 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) p176.

28 Ibid, and see for example Electronic Frontiers Australia: "The proposals are administratively onerous to the extent that few Australian content hosts would be prepared to incur the costs involved in setting up the relevant systems. It would be far easier to simply set up sites offshore in a country where such regulatory burdens are not imposed... The proposed identification details are easily forged, demonstrating conventional wisdom that effective age-authentication systems are almost impossible to implement on the Internet." *Comments on Australian Broadcasting Authority (ABA) Consultation Paper on Restricted Access Systems* <http://www.efa.org.au/Publish/ABAresp9911.html#summ> accessed 25/6/2001.

29 Tribunal de Grande Instance de Paris (Superior Court of Paris), 20/11/2000 <http://www.gigalaw.com/library/france-

yahoo-2000-11-20-lapres.html>

30 Australian Broadcasting Authority, *Investigation Into the Content of On-line Services, Report to the Minister for Communications & the Arts*, (Sydney: ABA, 30 June 1996) p158.

31 A number of such labelling schemes are in development. For a critique of such systems see <http://www.efa.org.au/Issues/Censor/cens2.html#filter> accessed 26/6/2001.

32 Australian Broadcasting Authority, *Investigation Into the Content of On-line Services, Report to the Minister for Communications & the Arts*, (Sydney: ABA, 30 June 1996) pp156-158.

33 Karen Koomen "Freedom of Speech and the Internet in Australia" Speech delivered at the Communications Law Centre Conference on 'Free Speech in Australia' Sydney, 10/9/96 p16.

34 Senator Alston, speech entitled 'Regulatory Challenges in Cyberspace' delivered at *Interactive Kids '98*. Sydney May 18th 1998.

35 David Kerr, *Action Plan on Promoting Safer Use of the Internet, Preparatory Actions – Self Labelling and Filtering*, Internet Watch Foundation, April 2000.

36 Australian Broadcasting Authority, *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation*, July to Dec 2000. April 2001

37 Ibid

38 Irene Graham "The Net Labelling Delusion: Saviour or Devil?" <http://rene.efa.org.au/liberty/label.html> accessed 21/6/2000; Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999) esp pp177-182.

39 Irene Graham, "The Net Labelling Delusion - Saviour or Devil?" http://libertus.net/liberty/label.html

40 Jennifer Lee, "Punching Holes in Internet Walls" New York Times, 26/4/2001.

41 Singapore Broadcasting Association, SBA's Approach to the Internet, http://www.sba.gov.sg/work/sba/internet.nsf/ourapproach/1

42 The OSA itself states that it is intended

(k) to provide a means for addressing complaints about certain Internet content; and

(l) to restrict access to certain Internet content that is likely to cause offence to a reasonable adult; and

(m) to protect children from exposure to Internet content that is unsuitable for children. *Broadcasting Services Act* (1992) (Cth). s3(1)(k),(l), & (m).

43 Senator Alston, speech entitled 'Regulatory Challenges in Cyberspace' delivered at *Interactive Kids '98*. Sydney May 18th 1998.

Cybercrime: Proposed legislation clamps down on use of technology to commit serious offences

Irene Zeitler, Partner, Freehills

Irene Zeitler is a partner in the Intellectual Property Group at the Freeehills Melbourne office and a consultant to the associated patent attorney firm, Freehills Carter Smith Beadle. Irene has substantial expertise in the field of information technology, intellectual property and trade practices.

A Bill recently introduced by the Federal Government contains new updated computer offences.[1] These offences are based on the offences recommended in the January 2001 Model Criminal Code Damage and Computer Offences Report.[2] The Bill is also consistent with the terms of the draft Council of Europe Convention on Cybercrime.

The purpose of the new offences is to overcome perceived deficiencies in existing computer offences inserted into the *Crimes Act* in 1989. These deficiencies arise from advances in computer technology and electronic communications which have given rise to new means for committing Cybercrimes, such as hacking, denial of service attacks and virus propagation. The Bill repeals existing offences.

The Bill has been referred to the Senate Legal and Constitutional Legislation Committee which is due to report on the Bill on 28 August 2001.

In summary, the new offences include the following:

Offence of causing unauthorised access to data held in a computer or any unauthorised modification of data held in a computer or any unauthorised impairment of electronic communications to or from a computer

To commit this offence, a person must know that the access, modification or impairment is unauthorised. The person must furthermore intend to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth by the access, modification or impairment.

A serious offence is an offence punishable by life imprisonment or a term of five years or more. The new offence carries a maximum penalty equal to the maximum penalty for the serious offence the person is intending to commit.

This covers offences against State and Territory laws where the unauthorised access, modification or impairment is caused by means of a telecommunications service.

The proposed offence is intended to cover the unauthorised use of computers to commit serious offences such as a fraud or stalking. An example of this is where a person uses the internet to hack into the computer system of a bank in order to access credit card details for the purpose of obtaining money.

Offence of causing any unauthorised modification of data held in a computer