The Internet and the Law: Emerging Issues for Australian Schools

Peter Williams, School of Business Law, Curtin Business School,
Curtin University of Technology, Perth, WA
&
Ken Dillon, Teacher Librarianship, School of Information Studies,
Charles Sturt University, Wagga Wagga, NSW

Abstract

This article explores some of the legal issues raised by access to the Internet in Australian schools. There have been a number of government enquiries into on-line services generally, and it has been acknowledged that access to the Internet by children poses special considerations. Some states have introduced legislation in an attempt to regulate access to the Internet generally, but the application of some aspects of the legislation to Internet use in schools is problematic. In addition, there are strategies available to schools to regulate access to the Internet in schools, such as filtering software and acceptable use policies. However, some of these strategies also come with their shortcomings. As more Australian schools go on-line, it is important that schools address the issues in order to harness the benefits that access to the Internet provides for them.

Introduction

> The Internet is the world's biggest collection of computer networks. The actual size of the system is unknown. It has been likened to 'an enormous spider web comprising thousands of smaller webs, permitting a continuous line to be traced from any point on any of the smaller webs to any point on any other web'... Once a user has access to the Internet - for example, via an Internet access provider such as Oz-Email - that user is free to move, uncontrolled, through countless networks. There is no central server through which all data passes and no-one regulates the flow or content of information transmitted through the Internet (Butler, 1996: 195).

In a recent report for the Schools Council of the National Board of Employment, Education and Training on management of student access to controversial material on the Internet, it is noted that there have been several government inquiries into regulatory frameworks for on-line services generally, reflecting the 'topicality of [the] subject and the fluidity of issues surrounding it' (Spalding, Gilding and Patrick, 1996: 10).[i] The report also notes that the use of the Internet in schools is 'in a stage of enthusiastic experimentation, but also of rapid expansion' (p. vii).[ii] The topic of regulation of the Internet has prompted much debate, involving issues as provocative as basic freedoms and censorship (e.g. Healey, 1997; Jones, 1995; Shiff, 1996; The Net Censorship Dilemma;[iii] Walsh, 1996). Regulation of the Internet in schools, it seems, is simply

part of that larger community debate about whether and how use of the Internet should be regulated. However, there does appear to be general agreement that access to the Internet by children poses special considerations.

The Internet in Schools - Legal Dimensions

Sometimes described as the most recent of the information revolutions in the history of mankind (Burnside, 1997: 1), the Internet offers access to a wide variety of on-line services such as electronic mail (e-mail), newsgroups, bulletin boards, Internet relay chat and the World Wide Web.[iv] Access to the Internet in schools thus presents teachers and schools with unique challenges.

The Internet has an impact on the roles of teacher and teacher-librarian directly. The fundamental role of the teacher-librarian in a networked school does not change: he/she must continue to meet the information needs of users and to facilitate information literacy development. What does change is how information services are provided, the nature of the collaborations between teachers and teacher-librarians, and how information as a strategic resource in schools is managed. Some commentators, for example, have foreshadowed a change of nomenclature and function from 'teacher-librarian' with responsibility for the 'school library program' to 'information service facilitator' or 'director of information services' with whole-school responsibility for an 'information services centre' or similar (Barron, 1995; Hay and Kallenberger, 1996; Ohlrich, 1996). Under such models, the teacher-librarian or information technology studies co-ordinator might be part of the 'information services unit', along with others employed on either a full-time or part-time basis, e.g. programmer, editor, computer technician, library technician, the mix very much depending on the circumstances of individual schools. Such ideas themselves suggest that a complete re-thinking of existing school structures and management practices may well be long overdue.

The use of the Internet in schools also raises important questions for the school-student relationship. Of considerable concern to the community in general, and to the school-student relationship in particular, is a collection of issues which might conveniently be termed 'student welfare' issues. One of the main problems with the Internet that members of many school communities envisage is student access to 'unsavoury' information, particularly pornographic and violent material. A second and even more disturbing problem relates to personal security of student users on the Internet. The potential for paedophiles, for example, to 'meet' potential victims on-line with the intention of arranging real time meetings is of particular concern. But while such concerns are valid, it appears there is little evidence to support the proposition that the Internet is as dangerous as the media sometimes portrays it to be (e.g. Australian Broadcasting Authority, 1996 [the ABA Report]; Collins, 1996; Leonard and Waters, 1997). In their study of selected Australian schools, Spalding, Gilding and Patrick (1996) found that few schools reported incidents of students stumbling across pornography and related material while accessing the Internet. Be that as it may, there is some force in the proposition that just as teachers owe a duty to take reasonable care for the physical safety of students in the 'real' school yard, so, too, should teachers bear some legal responsibility for the physical safety of students who, while at school, confront reasonably foreseeable risks of injury in cyberspace.

Access to the Internet by students at school also raises concerns that might be categorised as 'legal liability' concerns. A number of commentators note, for example, that the range of areas

in which the rights and obligations of on-line users may be affected by civil and criminal law include freedom of expression, defamation, privacy, vilification, discrimination and harassment, copyright, and protection of consumer rights (e.g. the ABA Report; Averill, 1997; Burnside, 1997; Hughes, 1997; Watts, 1996, 1997; Yastreboff, 1997). Already in Australia, the author of defamatory statements published on a Usenet newsgroup has been found liable for defamation (*Rindos v Hardwick*, unreported, Supreme Court of Western Australia, 1994). Interestingly, no legal action was pursued against the service provider of the electronic newsgroup, although in some American cases, liability for defamation has been found against the service provider of an electronic bulletin board (Averill, 1997). Legal actions have been initiated in Australia for defamatory statements made by teachers or students in the 'real' school environment. In *Stevenson v McCracken* (unreported, WA Supreme Court, 1985), a student and her father drew up a petition objecting to the 'foul and obscene behaviour' of a named teacher. The petition was circulated at a suburban high school by the student, and the court awarded the teacher damages after he had sued the student and her father for defamation. Had the case arisen in 1998, it is not too difficult to imagine that the petition might well have been forwarded by e-mail to other students and to school staff or posted on an electronic bulletin board to be read by others.

Regulating Internet Access in Schools

In some states, but not others, legislation has been introduced to deal specifically with computer technology, including the Internet, despite the amorphous nature of the on-line services to which the Internet provides access. In addition, many schools themselves have taken on the challenge of devising management strategies for student access to the Internet, sometimes with the assistance of guidance from education departments and authorities in the form of policies addressing management of the Internet (e.g. Education Department of Western Australia, 1996; New South Wales Department of School Education, 1997).

Regulating the Internet by Legislation

There has been 'a plethora of government enquiries, meetings of standing committees of Attorneys-General and broadcasting authority reports' (Shiff, 1996: 22) into regulation of the Internet.[v] In its investigation into the content of on-line services in Australia, the Australian Broadcasting Authority examined the question of whether on-line services, such as e-mail and the Internet relay chat tool, were covered by legislation governing traditional broadcasting services (the ABA Report). It took the view that, while on-line services that deliver television or radio broadcasts in real time may fall within the regulatory regime applying to broadcasting services, the vast majority of on-line services would not do so as there were fundamental differences between the provision of on-line services and traditional broadcasting services. It concluded that regulation of these on-line services could not therefore be accommodated by the *Broadcasting Services Act 1992* (Cth) in its present form.

One of the points of debate about regulation of on-line services in Australia has been the appropriate model for regulating the Internet. There appear to be two 'diametrically different' existing models that have sometimes been viewed as possible models for regulation of the Internet in Australia: the 'post/telecommunications' model [the 'P/T' model] and the 'broadcasting/cinema' model [the 'B/C' model] (Leonard and Waters, 1997: 92-94).

Under the 'P/T' model, the content of the message between users is seen as totally private, and users are free, with the exception of a very restricted body of material such as child pornography, to send and receive whatever content they wish through the post or over the telecommunications network. Under existing federal legislation, the carrier of the article or message bears no responsibility for the content of the item carried. Under the 'B/C' model, on the other hand, video material, computer games and film are categorised according to accepted criteria into viewing classifications, and federal and state laws then impose obligations, on distributors, broadcasters and cinema owners. Breach of the obligations attracts penalties. Under this model, the person making the material available to members of the public is accountable at law for the content of the medium and for allowing to see it those who should be protected from seeing it.

There would appear to be general agreement that if regulation of the Internet is to occur in Australia, neither the 'P/T' model nor the 'B/C' model is the perfect model. Leonard and Waters (1997: 93-94) comment:

> In our view, regulating the Internet only in accordance with a post/telecommunications model would not be appropriate. While some uses of the Internet, such as e-mail and newsgroups, are similar to posting a letter or making a telephone call and therefore retain a primarily private nature, other uses involve the provision of the information on an indiscriminate and widespread basis, analogous to the display of information in a public place or by traditional mass media communications, such as newspapers, television and cinema.
>
> ...
>
> The Internet differs fundamentally from the traditional mass media for which the broadcast/film censorship model was developed. Rather than a limited number of sources of information broadcasting to many constituting a passive audience, the Internet permits each member of the audience to be a 'broadcaster' to every other member of the audience. Individual Internet subscribers can publish their own electronic newspapers, establish newsgroups and their own home pages which can be accessed by any other Internet user.

Acknowledging the complexities associated with regulating a technology that seems to change by the minute, the ABA Report argued for a co-operative and co-ordinated approach by state and federal authorities to the development and adoption of a regulatory framework governing the Internet in Australia. However, some states have not waited for a national strategy to deal with the Internet. At least three jurisdictions, including Western Australia, have passed their own legislation in an attempt to regulate use of the Internet.[vi]

In 1996 the Western Australian Parliament passed the *Censorship Act 1996* (WA) [the WA Act]. While the WA Act consolidates into the one statute various provisions from other statutes dealing with the classification and control of such matters as publications, films, videotapes and indecent articles, it also incorporates new provisions dealing with computer games and computer services, including the Internet.

The approach that the WA Act takes with respect to the Internet is interesting. The WA Act attempts to regulate the behaviour of content users and content providers, namely persons who put material onto the Internet and who download material from the Internet. Clearly, the WA Act

applies only within the state, and consequently a short-coming of any state statute attempting to regulate the Internet becomes immediately apparent: the bulk of information on the Internet originates outside the state, so that the vast majority of content providers are simply not caught by the provisions of the state statute. However, students attending government and non-government schools in Western Australia, as well as teachers in those schools, are clearly governed by the WA Act. The WA Act also contains provisions that arguably apply to Internet service providers [ISPs] (Greenleaf 1996: 35), and the second reading speech in relation to the WA Act in the Western Australian Legislative Assembly confirms that such was the Parliament's intention (WA Parliamentary Debates, 1995: 10079).

The WA Act creates certain criminal offences involving the use of a 'computer service' relating to both 'objectionable material' and 'restricted material'. 'Computer service' is defined quite broadly as 'a service provided by or through the facilities of a computer communication system allowing [inter alia] the input, output or examination of computer data or computer programmes' (s.99 of the WA Act). This clearly means that the WA Act is intended to cover the Internet, bulletin board systems, and any form of computerised private communications, such as e-mail (Greenleaf, 1996: 33), and again the second reading speech confirms that such was the Parliament's intention (WA Parliamentary Debates, 1995: 10079).

'Objectionable material' is defined to include, among other things, child pornography (defined in s.3), as well as an article (defined in s.3 to include such items as a computer program and associated data, a book or a photograph) that promotes crime or violence, or instructs in matters of crime or violence. It is also defined to include an article that describes or depicts, in a manner that is likely to cause offence to a reasonable adult, various activities, including the use of violence or coercion to compel any person to participate in, or submit to, sexual conduct (ss.3 and 99 of the WA Act).

Examples of some of the offences created by the WA Act are:

> 101.(1) A person must not use a computer service to -
>
> (a) transmit an article knowing it to be objectionable material;
>
> (b) obtain possession of an article knowing it to be objectionable article;
>
> ...
>
> (e) request the transmission of objectionable material knowing it to be objectionable material.

The WA Act also provides that it is a defence to an offence created under s.101 to prove that the article is 'an article of recognised literary, artistic or scientific merit' and that transmitting or obtaining of the article is justified as being 'for the public good' (s.101(2) of the WA Act). It seems that there are some aspects of these provisions that might not operate effectively in a school setting. For example, if a student were to download a copy of a Robert Mapplethorpe photograph from the Internet for inclusion in an Art assignment. The Art teacher might be most enthusiastic but the student's parents might be horrified.

Questions of criminal responsibility and age aside, an essential element of the offences created by s.101 is 'knowing' that the article concerned is objectionable material. In respect of the example above, some people argue that Mapplethorpe's photography is 'objectionable material' as

defined in the WA Act; others argue that it is not. If adults vehemently disagree, as they seem to, about the nature of Mapplethorpe's work, when can it be said that the student 'knows' that the article downloaded from the Internet is 'objectionable material'?

Further, the WA Act indicates that before the defence under s.101(2) applies, it has to be proven that the article is of 'recognised' literary, artistic or scientific merit. One might reasonably ask: recognised by whom? Presumably it would be insufficient for a teacher or teacher-librarian simply to hold the view that an article is of literary or artistic merit. The defence will only apply if, in addition, the article is 'justified as being for the public good', however and by whom such a standard might be determined. In the parliamentary debates relating to the passage of the Act through the legislature, it was noted that, rather than imposing on the prosecution the onus of establishing that the article is contrary to the public good, this provision unfairly imposes the onus of establishing public good on the person who seeks to raise the defence (WA Parliamentary Debates, 1996: 1127). Structured in this way, this provision could be particularly onerous for a teacher who, after taking so-called 'objectionable material' (a Mapplethorpe photograph?) off the Internet for teaching purposes, must then convince a worried principal that 'educational benefit' is necessarily compatible with the 'public good'.

It is interesting to note, too, that since an ISP is initially unlikely to know that any article it transmits is objectionable material, it would appear that an ISP does not breach s.101 simply by transmitting objectionable material. However, if a school complained to an ISP about objectionable material at a particular site accessed by a student through that ISP, could that ISP face prosecution if, fully aware of the nature of the school's concerns, it does not take steps to respond to those concerns? The Western Australian Parliament believed so (WA Parliamentary Debates, 1995: 10079).

Various commentators have expressed concerns about attempts some individual states have made to regulate the Internet (e.g. Electronic Frontiers Australia Inc., 1997; Greenleaf, 1996; Shiff, 1996). And it is apparent that the legislative regimes put forward by statutes such as the WA Act can only go so far and address only some of the concerns of teachers and parents concerning access to the Internet in schools. Ironically, in the second reading speech referred to above, the Minister responsible for the passage of the WA Act through the Western Australian Parliament proffered the view that

> [d]espite any legislation which is put in place, the ultimate responsibility for protecting minors must rest with parents and members of educational institutions who, through physical supervision, control of access and use of filtering software programs, can determine what their children or students can access via a computer service (WA Parliamentary Debates, 1995: 10079).

Regulating Internet Access by Non-legislative Means

Spalding, Gilding and Patrick (1996: 29) note that there are, broadly speaking, two main types of management strategies that schools employ, singularly or in combination, to deal with student behaviour and the Internet. These strategies include both organisational strategies and technological strategies:

- organisational arrangements

- supervision
- signing a register before using a computer with Internet access
- acceptable use policies
- student contracts
- working with parents to develop shared responsibility, and
- placing reliance on student responsibility.

· technological mechanisms
- vetting material (e.g. incoming and outgoing e-mail)
- using a specialist service provider who limits access to certain sites or newsgroups
- restricting access to particular Internet tools (e.g. Internet Relay Chat, newsgroups)
- blocking access to specific sites, either at school or service provider level)
- downloading specific Internet information for student access (as opposed to allowing students direct access to the Internet)
- keeping log filers and running random checks of sites students have accessed, and
- using filter software.

The pros and cons of these strategies, and how they tend to operate, have been explored elsewhere (e.g. Spalding, Gilding and Patrick, 1996: 29-38; Dillon, 1997). The strategies which have attracted considerable attention in schools are the use of intelligent software filters, or filtering software, and the promulgation, implementation and enforcement of an acceptable use policy.

(i) Filtering software

There are a number of software packages specifically designed to limit student access to potentially controversial material on the Internet. Producers of software, such as Surfwatch, CyberPatrol, Net Nanny and others,[vii] claim that their software can be customised to filter out objectionable material. However, the extent to which this can be achieved is dependent upon a number of factors, including the techniques used to 'block' or exclude material, how active users are in recommending 'unsavoury' sites, how up-to-date the list of excluded sites is, and how clever the maintainers of blocked sites are in getting around the software.

Some commentators have questioned the use of filter software (e.g. Allison and Baxter, 1995; McKenzie, 1996; Schneider, 1997). Allison and Baxter (1995) consider the use of intelligent software to filter information a 'technological fix' and at best a partial solution, and they question the feasibility of software filters in the absence of a broad-based system of Internet content classification. Of special interest is a recent report (1997) of the Electronic Privacy Information Center in America which reveals some alarming results of comparisons between 100 searches using Net Shepherd Family Search, a web-based search engine that filters out web sites

judged to be 'inappropriate and/or objectionable to average user families', and the unfiltered Alta Vista search engine.[viii] The study concluded that, overall, Net Shepherd regularly blocked access to over 99 per cent of documents from sites of potential interest to children, including such seemingly innocuous sites as schools, charitable and/or political organisations (e.g. UNICEF), educational, artistic and/or cultural institutions (e.g. Disneyland, San Diego Zoo), and 'miscellaneous concepts or entities' (potential research topics), such as astronomy, eating disorders and photosynthesis.

ISPs can also limit access to selected sites on an ongoing basis. In Australia, schoolsNet, for example, uses software called 'CensorMan'[ix] to block access to sites in the schools it services. But as Ingvarson (1995) points out, the decision to block one or more sites is a school decision and not a decision of the ISP - ISPs are merely providing a service to schools. It is also impossible for ISPs to guarantee blockage of every potentially controversial site for schools, partly because of the sheer number of new sites appearing every day and partly because it is difficult to predict the types of sites schools want blocked. For example, some seemingly innocent sites, such as the home pages of television programs like *The Simpsons*, have been the subject of requests for blocking by schools because of their 'potential for wasting valuable student time on-line'.

(ii) Acceptable use policies

In addition to the use of intelligent software filters, schools have attempted, either voluntarily or by direction, various other means of monitoring student access. The most common of these means is supervision of access, but clearly such a strategy is not a practical solution in many cases. An increasingly common strategy of monitoring student access to the Internet is by means of an acceptable use policy [AUP].

Defined as 'a framework outlining the terms and conditions for operating and using a computer network', 'AUP' is also 'the term recently given to formal school guidelines that regulate student usage of the Internet' (Spalding, Gilding and Patrick, 1996: 129). Central to the operation of an AUP is its form. It is a written document containing provisions as to use of the Internet and signatures of the student, his/her parents and the teacher, supposedly indicating agreement with the provisions contained in the document. AUPs are usually instituted by the education authority or by an individual school. To a large extent, an AUP seems to overlap in purpose and function with another common strategy for monitoring student access to the Internet, viz. a student contract, but an AUP generally requires the signature of both student and the student's parent or guardian, while a contract will generally only require the signature of the student. The contents of a typical AUP include such matters as a description of what the Internet is, an explanation of how students will access the Internet at school, examples of how the Internet will be used to enhance student learning, a list of student responsibilities while on-line (addressing such matters as legal constraints, resource utilisation and etiquette), and the consequences flowing from breach of the AUP (Heide and Stilborne, 1996: 67). While the differences in purpose between an AUP and a contract are difficult to discern, the end-point with both an AUP and a contract appears to be identical: the withdrawal of the privilege of using the Internet if the terms of either document are not adhered to by the student.

'Contracts' designed to regulate student behaviour and learning at school are not uncommon in Australian schools, but it is difficult to argue that such contracts are enforceable as

contracts in the legal sense; indeed, the generally accepted view is that they have no legal force. Such a contract, seemingly based upon what has been termed the 'behaviour modification' model of contracts (Blair and Waddington, 1997), is not a contract in the legal sense; it does not impose legal obligations on the student, breach of which entitles the teacher or the school to sue the student before a court. The AUP may not be a legal 'nonsense' but it would appear, at most, to be 'a sheep in wolves' clothing'. An AUP is nothing other than an attempt more formally to articulate expectations relating to student behaviour, expectations that can equally be articulated orally or by simply posting a list of rules. The fact that parents may have signed the document does not, it is suggested, change the nature of the document.

A more serious concern is the penalty for a student who fails to adhere to the provisions of the contract or of the AUP: a withdrawal of the privilege of accessing the Internet. How should an AUP deal with the matter of the penalty? The answer to this question should, perhaps, depend upon the extent to which Internet access and use are tied to the teaching and assessing of curriculum areas. Should the penalty be imposed when a teacher has 'knowledge in fact' of breach of the rules about Internet use, or should it be imposed when the teacher merely has 'reasonable grounds for believing' that the rules have been breached? How often will the penalty be imposed? And does it matter that imposition of the penalty might mean that the student will not acquire skills and knowledge that will form the basis of his/her assessment in particular curriculum areas? Should an AUP set out a number of possible penalties so that the more closely Internet access and use are tied to the teaching and assessing of curriculum areas, the less likely it is that a student will be denied access to the Internet?

Some AUPs go to great lengths to make them appear legally credible. One particular AUP quotes almost word for word section 85ZE of the *Crimes Act 1914* (Cth). That section provides:

> 85ZE A person shall not knowingly or recklessly:
>
> (a) use a telecommunications service supplied by a carrier to menace or harass another person; or
>
> (b) use a telecommunications service supplied by a carrier in such a way as would be regarded by a reasonable person as being, in all the circumstances, offensive.
>
> Breach of s.85ZE attracts a penalty of imprisonment for 1 year.

The inclusion of such a provision in an AUP raises a number of questions. Could the inclusion of this provision be seen in some situations not as a prohibition against a student's particular use of the Internet, but almost as a sanctioning of it? A student may access the Internet and download what the teacher feels is offensive material. However, to attract the liability imposed by s.85ZE(b), the use has to meet an 'offensive to a reasonable person' test. A reasonable person might not find the material offensive at all, and the material will therefore be legally permissible. To put it another way, s.85ZE is the outer framework beyond which a person accessing the Internet should not go, but within that framework there would be much that is permitted by the reasonable person. If it is the case, as has often been argued, that teachers tend to err on the side of caution when confronted by controversial issues, s.85ZE may permit much more than the teacher is likely to permit. In such circumstances, the inclusion of s.85ZE in an AUP may not achieve what the teacher had hoped it would achieve.

There is another problem with the inclusion of the section in an AUP. Echoing the views of Leonard and Waters (1997) about the 'P/T' model of Internet regulation, there is an argument that the section was never intended by the Parliament to cover use of the Internet and that, therefore, a court would not interpret the section as being applicable to the Internet. It has been argued (Butler, 1996: 198-199) that s.85ZE was designed to deal with obscene and harassing telephone calls that a recipient does not wish to receive; it was not intended to apply to the contents of a totally private telephone call between consenting persons. Thus, extending s.85ZE generally to situations involving several people corresponding via a bulletin board, for example, may be going beyond what the section was ever intended to do. If that is the case, the inclusion of s.85ZE as an integral component in a school's AUP is somewhat misleading (Williams, 1997).

Many Australian schools are adopting the AUP as a method of managing student access to the Internet. However, Spalding, Gilding and Patrick (1996: 32) have cautioned, that determining student access to the resources of the Internet according to whether a student's parent has signed an AUP effectively disadvantages those students whose parents have refused to sign. Use of an AUP by itself may therefore not be the answer, and it may well be the case that it is 'more a question of parents understanding what is being offered, what particular controls [a] school has in place and feeling reassured about the capacity of their child to handle the consequences of an inadvertent exposure to controversial material' (Spalding, Gilding and Patrick, 1996: 32).[x]

Conclusion

The Internet provides for schools and students throughout Australia access to resources that are overwhelming. But by its very nature, it presents schools with a diversity of challenges. There are many good reasons why schools should develop sound guidelines for student use of the Internet, not the least of which are concerned with questions of legal liability.

Because the technology is so new and global, the development of laws by governments in Australia to deal with the Internet has been both cautious and, some might say, unsatisfactory. Even in states where such legislation has already been introduced, it has brought its own problems of interpretation and application. In addition, the very technology that has given substance and form to the Internet has provided filtering tools in an attempt to make access to the Internet 'safe', but filtering technology also seems to come with its own shortcomings. Strategies, such as the AUP, are useful innovations, but they may be even more acceptable if they are accompanied by strategies that keep parents informed of the true nature of the Internet.

As more and more Australian schools 'go on-line', it is important that they address the range of issues the Internet brings. They should attempt to develop policies that are workable, in both a practical and legal sense, in order to ensure that the obvious benefits of access to the Internet are harnessed and put to good use in schools.

Keywords

Internet; Regulation; Australia; Schools.

References

Allison, L. and Baxter, R. (1995) *Protecting Our Innocents*. Report of the Department of Computer Science, Monash University, Melbourne (Technical Report 95/224). Available WWW: **http://www.cs.monash.edu.au/publications/ftp/1995/TR224/1995.224.html**.

Australian Broadcasting Authority (1996) *Investigation into the Content of On-line* Services. Report to the Minister for Communications and the Arts. Available WWW: **http://www.dca.gov.au/aba/invest.html**.

Averill, M. (1997) Defamation - The Internet and the world-wide-web. In P. Leonard (ed), *Internet Law Anthology*. Sydney: Prospect Publishing.

Barron, D. (1995) Information Services Facilitators to Replace School Library Media Specialists. *School Library Media Activities Monthly*, 11(8): 48-50.

Blair, A. and Waddington, M. (1997) The Home-school' Contract': Regulating the Role of Parents. *Education and the Law*, 9(4): 291-305.

Burnside, J. (1997) The Internet: General legal issues. In *Internet: Legal Issues*. Melbourne: Leo Cussen Institute.

Butler, A. (1996) Regulation of Content of On-line Information Services - Can Technology Itself Solve the Problem It has Created? *UNSW Law Review*, 19(2): 193-221.

Collins, S. E. (1996) A Fear of Rare and Mysterious Dangers. Available WWW: Web66 **http://web66.coled.umn.edu/Ramble/ChildSafety.html**.

Dillon, K. (1997) Nasties on the Net: Media Hype or Major Concern for Schools? In *Language, Learning and Culture - Unsettling Certainties: Proceedings of the First Joint National Conference of the Australian Association for the Teaching of English, the Australian Literacy Educators' Association and the Australian School Library Association.* Darwin: Northern Territory Department of Education.

Education Department of Western Australia 1996, *Policy Guide*, WA Education Department, Perth.

Electronic Frontiers Australia Inc. (1997) A brief history of Internet regulatory activity in Australia. In K. Healey (ed), *Censorship: Issues for the Nineties*. Australia: The Spinney Press.

Greenleaf, G. (1996) Law in Cyberspace. *The Australian Law Journal*, 70(1): 33-36.

Hay, L. and Kallenberger, N. (1996) The Future Role of the School Information Services Unit in the Teaching/Learning Process. Paper presented at the *Electronic Networking and Australasia's Schools Conference*, Sydney, April 11-13.

Healey, K. (1997) *Censorship: Issues for the Nineties.* Australia: The Spinney Press.

Heide, A. and Stilborne, L. (1996) *The Teacher's Complete & Easy Guide to the Internet*. Toronto: Trifolium.

Hughes, T. (1997) Intellectual property and browsing the web. In P. Leonard (ed), *Internet Law Anthology*. Sydney: Prospect Publishing.

Ingvarson, D. (1995) Censoring the Internet: The Practicalities. Paper presented at *The Information Highway and the Nation's Schools Conference*, Sydney, June 10.

Jones, M. (1995-1996) The ISP Dilemma. *Internet Australasia*, 1(2): 78-83.

Leonard, P. and Waters, P. (1997) Censoring the Net in Australia: Brave New World or 1984 Revisited? In P. Leonard (ed), *Internet Law Anthology*. Sydney: Prospect Publishing.

New South Wales Department of School Education (1997*) Student Access : Developing A School Internet Policy*, Sydney, NSW, Australia.

McKenzie, J. (1996) Filtering the Web: A tale of fishnet stockings and Swiss cheese - A dozen reasons why schools should avoid filtering. In *From Now On: A Monthly Electronic Commentary on Educational Technology Issues*. Available WWW: **http://fromnowon.org/fnomar96.html**.

Ohlrich, K. (1996) What Are We?: Library Media Information Specialists, Computer Technology Coordinators, Teacher Instructional Consultants, School-based Team Management Members, or What*? School Library Media Activities Monthly*, 12(9): 26-28, 32.

Schneider, K. G. (1997) *A Practical Guide to Internet Filters*. New York: Neal-Schuman.

Shiff, G. (1996) Internet Censorship in Australia. *Metro Magazine*, 108: 21-25.

Spalding, B., Gilding, J. and Patrick, K. (1996) *Management of Student Access to Controversial Material on the Internet.* A Report for the Schools Council of the National Board of Employment, Education and Training (Commissioned Report No. 48). Canberra: AGPS.

Walsh, V. (1996) Regulating the Internet? *LASIE*, 27(3): 67-71.

Watts, D. (1996) *The Internet: Legal Issues*. Melbourne: Leo Cussen Institute.

Watts, D. (1997) Electronic commerce. In *Internet: Legal Issues*. Melbourne: Leo Cussen Institute.

Western Australia, Legislative Assembly (1995), *Parliamentary Debates*, vol. 327, pp. 10074-10080.

Western Australia, Legislative Assembly (1996), *Parliamentary Debates*, vol. 331, pp. 1123-1155.

Western Australian Education Department (1996*) Internet Usage: Policy and Guidelines*, Perth, Western Australia.

Williams, P. (1997) Censuring the Censor - Does the Law Help or Hinder? Drawing Lines in the Sand. Paper presented at the *Tasmanian Secondary College Teacher Librarians' Annual Conference*, Launceston, December 1-2.

Yastreboff, N. (1997) Copyright for on-line databases on the Internet. In P. Leonard (ed), *Internet Law Anthology.* Sydney: Prospect Publishing.

Endnotes

i See, for example, reports such as:
- Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technology (1995), *Report on Regulation of Computer On-line Services* - Part 1, September 1995; Part 2, November 1995;
- Australian Broadcasting Authority (1996) *Investigation into the Content of On-line Services:*

Report to the Minister for Communications and the Arts [the ABA Report], available at **http://www.dca.gov.au/aba/hpcov.htm**.

ii An executive summary of the report is available at **http://teloz.latrobe.edu.au/circit/scexec01.html**.

iii At **http://smople.thehub.com.au/~rene/liberty/**.

iv For useful explanations of the Internet and on-line services see, e.g., the ABA Report; G. Smith (ed) (1996) *Internet Law and Regulation*, FT Law & Tax, London; D. Watts (1996) *The Internet: Legal Issues*, Leo Cussen Institute, Melbourne.

v For discussion and analyses of these reports, see, for example, A. Butler, Regulation of Content of On-line Information Services - Can Technology Itself Solve the Problem it has Created? (1996) 19 *UNSW Law Journal* 193; S. Oddie, The Internet: Regulation of Delivery and Content (1996) *Media and Arts Law Review* 86; V. Walsh, Regulating the Internet? (1996) 27 *LASIE* 67.

vi See *Classifications (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic); *Classification of Publications, Films and Computer Games Act 1996* (NT); *Censorship Act 1996* (WA).

vii A list of producers of filter software and their products can be found at **http://www.pitsco.inter.net/p/safe.html**.

viii The report titled 'Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet' can be found at **http://www.epic.org/reports/filter-report.html**. See also the work of Schneider (1997), parts of which are available at the TIFAP (The Internet Filter Assessment Project) site at **http://www.bluehighways.com/tifap/**.

For comparative reviews of Internet filters see, e.g.:

- Internet World's comparisons at **http:www.internetworld.com/print/monthly/1996/09/safe.html**;
- PC Magazine's comparisons at **http://www8.zdnet.com/pcmag/features/utility/filter/_open.htm**.

Pro-Internet filtering information is located at the cleverly (deceptively?) titled 'Filtering Facts Home Page' at **http://www.filteringfacts.org/**.

ix At **http://www.schnet.edu.au/CensorMan/**.

x There are a number of collections of sample school policies and AUPs for student access to the Internet. Some of the most well known include:
- Department of Education and Children's Services, South Australia. Internet User Guidelines. At **http://www.nexus.edu.au/Publicat/Other_Publications/AUP.html**;
- Ministry of Education, Victoria. Using the Internet - Taking Care on the Internet. At **http://www.sofweb.vic.edu.au/internet/takecare.htm**;
- Pitsco's Launch to Acceptable Use Policies. At **http://www.pitsco.inter.net/p/accept.html**;
- Acceptable Use Policies (Rice University). At **http://www.rice.edu/armadillo/acceptable.html**.