Pornography and the International Internet: Internet Content Regulation in Australia and the United States

Meghan A. Wharton

Follow this and additional works at: https://repository.uchastings.edu/hastings_comm_ent_law_journal

Part of the Communications Law Commons, Entertainment, Arts, and Sports Law Commons, and the Intellectual Property Law Commons

Recommended Citation
Available at: https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol23/iss1/4

This Article is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Communications and Entertainment Law Journal by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.
Pornography and the International Internet: Internet Content Regulation in Australia and The United States

by

MEGHAN A. WHARTON

I. Factual Background – The Nature of the Internet ..............123
II. Internet Regulation in Australia ........................................126
   A. Government Investigations ..........................................126
   B. The Broadcasting Services Amendment (Online Services) of 1999 ..................................................128
      1. Summary of Regulatory Scheme Provided by the Amendment ........................................128
      2. Key Definitions ......................................................129
      3. Categories of Content ..............................................130
      4. Classification and Reclassification of Content ............132
      5. Prohibited Content and Potential Prohibited Content ..................................................133
      6. Complaints Process .................................................134
         a. Content Hosted in Australia ..................................136
         b. Content Hosted outside Australia .........................137
      7. Industry Codes and Standards ....................................141
      8. Online Provider Rules .............................................143
      9. Civil and Criminal Immunity ......................................144
     10. Effect on State and Territory Laws ............................144
     11. Appeals to the Administrative Appeals Tribunal (“AAT”) ...........................................145
   C. The Legislation in Action .........................................145

* J.D. 2001, Georgetown University Law Center; B.A. 1996 University of Texas at Austin. The author will join the Phoenix law firm of Brown & Bain P.A. in April 2001. The author would like to thank her family and friends. In particular the author would like to thank her mother, Marsha Rae Stites, for her love and support without which this paper would not have been possible.
D. State and Territory laws.............................................................147
   1. Victoria .............................................................148
   2. Western Australia.....................................................149
   3. Northern Territory ................................................149
   4. New South Wales, Queensland, and
      South Australia......................................................150
E. Educating Australia About the Internet ..............................150
F. Criticisms of the Australian System ..................................151

III. Comparisons with United States Efforts to Regulate the
      Internet........................................................................152
    A. United States' Attempts to Regulate the Internet ............152
    B. Differences and Similarities between the United States
       and Australian Approach.............................................154

IV. Conclusion..........................................................................156
Introduction

In 1995, Time magazine ran an article describing the vast amount of pornography available on the Internet. The article set off a storm of concern about "cyberporn" in the United States and abroad. The article prompted the United States Congress to pass the Communications Decency Act in 1996 ("CDA"). The Australian government dealt with the situation in a much less hasty manner. In 1995, the Australian government began investigating possible regulatory schemes for online content. These studies culminated in the Broadcasting Services Amendment (Online Services) of 1999 ("Online Services Amendment"). The Online Services Amendment, as well as accompanying state/territory legislation, attempts to address the presence of pornography on the Internet.

This paper addresses the approaches of the United States and Australia to Internet content regulation. While the bulk of this paper covers the Australian system, I have provided a brief discussion of the United States system as a background for comparison. Part I of this paper provides an overview of the Internet and looks at the different problems that have arisen in the unique medium. Part II looks at Australia's Broadcasting Services Amendment of 1999 and specifically analyzes the Internet regulatory regime instituted by the legislation. Finally, Part III looks at the United States' attempts to regulate the Internet and compares the Australian and United States approaches in this context.

I

Factual Background - The Nature of the Internet

The Internet is not a physical object that is present at any one location at a specific point in time. It is an "international network of interconnected computers." Although the Internet had modest beginnings, it has experienced extraordinary growth in the 1990's in both Australia and the United States. For instance in Australia:

- Fifty-Seven percent of Australian adults have access to a computer;

Twenty-five percent of Australian adults have access to the Internet;
Twenty-one percent of Australian businesses have access to the Internet;
Forty-two percent of Australian households (including farms) have computers;
Fourteen percent of Australian households (including farms) access the Internet from home; and
Thirteen percent of children aged fifteen through seventeen and twelve percent of children aged ten through fourteen frequently used a home computer and accessed the Internet.\(^4\)

In the United States, the most recent numbers are even more astounding. The most recent government study was performed in 1997. It showed that:
One in five people, three-years old and older, have used the Internet;
Forty-seven percent of United States adults use a computer at home or at work;
More than half of the children who have accessed the Internet have only done so at school; and
Half of all United States children have a computer in their home.\(^5\)

People access the Internet through various methods. Often people are able to access the Internet through a connection provided by employers, libraries or schools.\(^6\) Frequently, people access the Internet through an Internet service provider. These Internet service providers often provide customers access to their extensive propriety networks as well as access to the Internet. Microsoft Network, America Online and CompuServe are some of the largest Internet service providers in the United States.\(^7\)

The most vast and well known form of information available over the Internet is the World Wide Web. The Web “allows users to

\(^6\) Id. at 850.
\(^7\) Id. at 850-51.
search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites.\textsuperscript{8} The Web is a collection of documents stored on distant computers, which are made accessible through the Internet.\textsuperscript{9} Often Web pages contain 'links' to other documents available on the Internet. By using a mouse to select the link, the user is automatically transported to the Web page corresponding to that link.\textsuperscript{10}

Web pages exist on the Internet for all types of commercial and informational purposes. Many Web sites are free to the public, while some sites are only available after the payment of a fee. Frequently, Web sites have been used to engage in commercial transactions. Today, nearly anything you would like to purchase and have delivered to your home can be found on the World Wide Web. The nature of the Web is “comparable, from the readers’ viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.”\textsuperscript{11}

The Internet also offers publishing capabilities to every person who can access the Web. Internet users have a “vast platform from which to address and hear from a world-wide audience of millions of readers, viewers, researchers and buyers.”\textsuperscript{12} The nature of the Internet means that it is decentralized. “No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web.”\textsuperscript{13}

Although the Internet has tremendous benefits to society, its decentralized nature provides a mechanism for the transmission of inappropriate material. Sexually explicit material is widely available over the Internet. This includes text, pictures, and chat and “extends from the modestly titillating to the hardest-core.”\textsuperscript{14} This material is placed on the Internet in the same manner that all other Internet material is posted. A user accesses the material by either engaging in a search on a search engine or typing the URL.\textsuperscript{15}

The presence of sexually explicit material on the Internet has led to the development of software and other tools designed to prevent

\begin{itemize}
  \item \textsuperscript{8} \textit{Id.} at 852.
  \item \textsuperscript{9} \textit{Id.}
  \item \textsuperscript{10} \textit{Id.}
  \item \textsuperscript{11} \textit{Id.} at 853.
  \item \textsuperscript{12} \textit{Id.}
  \item \textsuperscript{13} \textit{Id.}
  \item \textsuperscript{14} \textit{Id.}
  \item \textsuperscript{15} \textit{Id.}
\end{itemize}
children’s access to material which may be inappropriate to them. Much of this technology has been developed in the United States.

First, a user can purchase Internet access which only allows access to certain sites. The software is centered around a list of approved sites. The user is unable to access Internet sites which are not on the list. Second, a user may install on their computer a software program that blocks out certain sites. This software uses a list of unacceptable sites and refuses the user access to them. Finally, a user may use either of these techniques with a search-engine filter. This filter monitors words typed into a search. When an inappropriate search term is used, the filter prevents the user from running the search.

Site-based mechanisms can be employed to prevent children from accessing inappropriate material. For example, a site containing inappropriate material can employ an age verification system which refuses to allow access to information to users who cannot show that they are adults. This is frequently done by requiring credit card validation or through the assignment of a password or personal identification number.

II

Internet Regulation in Australia

The Online Services Amendment constitutes one tier of a three-tiered approach to Internet regulation in Australia. This legislation regulates Internet service providers and Internet content hosts. A second level of state regulation is required because the national government does not have the power to censor or regulate end-users or content providers. The second tier of regulation will be made up of State/Territory laws imposing obligations on producers of content and end-users who access or upload content. The third tier of the regulation will be made up of non-legislative actions monitoring Internet content and providing education to the public about Internet content.

A. Government Investigations

This section discusses the period of time leading up to the presentation of the legislation. The Parliament considered several government studies in structuring the legislation. The seeds for this

---

16. Id. at 854-55.
legislation were planted in 1993 when the Senate Select Committee on Community Standards ("SSCCS") found that the availability of pornographic and violent material on the Internet posed a threat to Australian citizens. Their report also acknowledged the "complex regulatory problems" arising from attempts to limit access to such material originating in foreign countries and entering Australia via mass communications lines.\(^\text{18}\) The report argued that the censorship Ministers should consider possible solutions.\(^\text{19}\)

In 1994, the Minister for Communications and the Arts created the BBS Task Force to examine possible regulation of computer bulletin boards. The BBS Task Force along with SSCCS hearings in 1995 resulted in the July 1995 government published consultation paper on the regulation of all Online services.\(^\text{20}\)

In August 1995, the SSCCS began an examination of possible regulation of Online services in Australia. They recommended criminal penalties for transmission of RC, X, and R material over the Internet. Sites would be rated by the Office of Film and Literature Classification. They also recommended self-regulation by industry bodies and the institution of a complaints system.\(^\text{21}\)

In July 1995, the Minister for Communications and the Arts ordered the Australian Broadcasting Authority ("ABA") to investigate Internet content and regulatory possibilities. This investigation resulted in the very influential publication *Investigation into the Content of Online Services: Report to the Minister for Communications and the Arts* ("Investigation Report").\(^\text{22}\) The Investigation Report set out a frame-work for Internet regulation. The frame-work provided for industry created codes of practice approved by the ABA with the ABA monitoring their effectiveness.\(^\text{23}\)

In 1997, the SSCCS evaluated the situation and made several regulatory recommendations. They recommended criminal penalties for transmission of RC material, the creation of an independent complaints handling board, the development of industry codes of


\(^{19}\) Id.


\(^{22}\) Australian Broad. Auth., *Investigation into the Content of On-Line Services* (June 1996).

\(^{23}\) See id.
practice, the creation of a task force for Online labeling, and the use of restricted access systems for Online material classified R.\textsuperscript{24}

In a July 1997 Media Release, the government set out principles for regulation based on discussions in the Investigation Report. This statement recognized the industry’s interest in regulating not inhibiting growth. In the release, the government recognizes that any regulation must not be more burdensome than that which is applied to film and print. They also recognize that service providers do not always have knowledge of material traveling through their server.\textsuperscript{25}

The Parliament also considered technological information. The National Office for the Information Economy ("NOIE") commissioned the division of Mathematical and Information Sciences to investigate the technical aspects of blocking content on the Internet. This investigation produced a report to the government about the process of Internet content filtering. The report also examined a user’s ability to circumvent these filtering programs through various methods.\textsuperscript{26}

\section*{B. The Broadcasting Services Amendment (Online Services) of 1999}

\subsection*{1. Summary of regulatory scheme provided by the Amendment}

The Amendment adds Schedule 5 to the Broadcasting Services Act of 1992 ("BSA"). This new Schedule provides for the regulation of Online services. The legislation has three stated purposes. First, the Parliament wanted to set up a system for dealing with complaints about inappropriate Internet content.\textsuperscript{27} Second, the legislation intends to restrict access to content which a reasonable adult would find offensive.\textsuperscript{28} The legislation seeks to protect minors from exposure to inappropriate material.\textsuperscript{29} Finally, Internet service providers are to develop industry standards to deal with the presence of prohibited material based outside Australia.\textsuperscript{30}

The legislation sets up a new scheme for regulation of Online

\begin{thebibliography}{9}
\bibitem{24} Sen. Select Comm. on Community Stands., \textit{Report on Regulation of Computer Online Services Part 3} (June 1997).
\bibitem{25} Minister for Communications and the Arts and Atty.-Gen., Jt. Media Release, \textit{National Framework for Online Content Regulation} (July 15, 1997).
\bibitem{26} Natl. Off. for the Info. Econ., \textit{Blocking Content on the Internet: a Technical Perspective} (June 1998).
\bibitem{28} \textit{Id.}
\bibitem{29} \textit{Id.}
\bibitem{30} \textit{Id.} sch. 5, cl. 2.
\end{thebibliography}
Services, but the system incorporates many standards and definitions from the regulation of film. The regulation provides a complaint-based system of Internet content regulation. When a person files a complaint about the presence of prohibited content on the Internet, the ABA must investigate. The Act defines prohibited content. Content will be dealt with under different rules depending on whether it is hosted in Australia or outside Australia. The legislation provides for a take-down process for Australia-based content.

2. Key definitions

There are several definitions in the Act which are key to its interpretation. Internet content is defined as information that: (a) "is kept on a data storage device; and (b) is accessed, or available for access, using an Internet carriage service; but does not include: (c) ordinary electronic mail; or (d) information that is transmitted in the form of a broadcasting service." E-mail and content in the form of broadcast are specifically excluded from the definition of Internet content. Content from chat-rooms, listservs and bulletin boards does not appear to be regulated. An Internet content host is a person or company hosting content in Australia or proposing to host content in Australia.

Two other key definitions are provided for in their own clauses. An Internet Service Provider is a person who "supplies, or proposes to supply, an Internet carriage service to the public." Supply to the public is defined three ways in the Act. A service meeting any of these three definitions will be considered "to the public."

1. The service is used for transferring information between two end-users and each end-user is outside the circle of the supplier.

2. The service is used to provide "point-to-multipoint services to end-users" and at least one end-user is outside the immediate circle.

3. The service is supplies content other than point-to-multipoint service and at least one end-user is outside the immediate circle.

When the statute uses the phrase "outside the immediate circle

31. Id.
32. Id.
33. Id. sch. 5, cl. 3.
34. Id.
35. Id. sch. 5, cl. 8 (an Internet carriage service is a "listed carriage service that enables end-users to access the Internet," Id. sch. 5, cl. 3).
36. Id. sch. 5, cl. 9(2).
37. Id. sch. 5, cl. 9(3).
38. Id. sch. 5, cl. 9(4).
of the supplier of the service” it appears that this is excluding Intranet systems set up by companies or educational facilities. Items posted to web sites encompassed in an Intranet would not be considered supplied to the public.

3. Categories of Content

Content is to be classified by the Classification Board created under the Classification (Publications, Films and Computer Games) Act 1995 (“Classification Act”). If the content consists of an entire film or computer game which has already been classified under the Classification Act then the content “is taken to have been classified by the Classification Board in the same way as the film, or the computer game, was classified under that Act.” If the film or computer game has not been previously classified by the Classification Board, then the Classification Board “is to classify the Internet content under this schedule in a corresponding way to the way in which the film or computer game . . . would be classified under the [Classification Act.]” Most Internet content does not consist of a film or computer game. This content is to be classified “in a corresponding way to the way in which a film would be classified under the [Classification Act.]”

This scheme results in most previously unclassified content being classified under the standards set out for classifying films. All previously unclassified content will be classified under the film standards unless the content is considered to be a computer game. In the cases of unclassified computer games the computer games standards will apply.

The standards for classifying films are set out in the Guidelines for the Classification of Films and Videotapes. The Online Services Amendment only regulates content classified as R, X or RC, therefore I will only discuss the standards surrounding these classifications. Of the three classifications RC, Refused Classification, is reserved for material considered illegal and thus

39. Id. sch. 5, cl 12(1).
40. Id. sch. 5, cl 12(2).
41. Id. sch. 5, cl 13.
42. Office of Film and Literature Classification, Guidelines for the Classification of Films and Videotapes (Apr. 15, 1999) [hereinafter Film Guidelines].
43. The Guidelines also provide for G, PG, M and MA classifications. Id.
44. Online Servs. Amend., sch. 5, cl. 10.
deemed refused classification." RC material is often referred to as objectionable material. The X category consists of sexually explicit material legally restricted to adults. The R category consists of material legally restricted to adults. This material is often referred to as unsuitable for those under 18. Material classified as R is considered to be only suitable for an adult audience.

45. The Guidelines state:

The Classification Code sets out the criteria for refusing to classify a film or video. The criteria fall into three categories. These include films that:

(a) depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should be classified RC.

(b) depict in a way that is likely to cause offence to a reasonable adult a person who is or who looks like a child under 16 (whether or not engaged in sexual activity, or;

(c) promote, incite or instruct in matters of crime or violence.

Further, the Film Guidelines list types of films that will be refused classification. This list includes films which contain "instruction in pedophile activity," "depletions of child sexual abuse," detailed instruction in matters of crime or violence or the use of proscribed drugs, or "depictions of practices such as bestiality." Films will also be refused classification if "they contain gratuitous, exploitative or offensive depictions of violence with a very high degree of impact or which are excessively frequent, prolonged or detailed; cruelty or real violence which are very detailed or which have a high impact; sexual violence; sexual activity accompanied by fetishes or practices which are offensive or abhorrent, or incest fantasies which are offensive or abhorrent." Film Guidelines.

46. The X classification is

[A] special and legally restricted category which only contains sexually explicit material. That is material which contains real depictions of actual sexual intercourse and other sexual activity between consenting adults, including mild fetishes. No depiction of sexual violence, sexualised violence or coercion, offensive fetishes, or depictions which purposefully debase or abuse for the enjoyment of viewers is permitted in this classification.

Film Guidelines.

47. The R classification "is not intended as a comment on the quality of the material. Some material may be offensive to some sections of the adult community. Material which promotes or incites or instructs matters of crime and/or violence is not permitted." The Film Guidelines further set out items that will or will not be permitted under the R classification:

Violence: Depictions of violence which are excessive will not be permitted. Strong depictions of realistic violence may be shown but depictions with a high degree of impact should not be gratuitous or exploitative. Sexual violence may only be implied and should not be detailed. Gratuitous, exploitative or offensive depictions of cruelty or real violence will not be permitted.

Sex: Sexual activity may be realistically simulated; the general rule is "simulation, yes - the real thing, no." Nudity in a sexual context should not include obvious genital contact. Verbal references may be more detailed than depictions.

Coarse Language: There are virtually no restrictions on coarse language at the R level.
4. Classification and Reclassification of Content

The Classification Board will only classify online material when the ABA requests that it do so. There is no automatic classification for any material. When material is unclassified, it is considered appropriate for all audiences until the ABA requests the Classification Board to issue a classification. The ABA can request classification on their own initiative or based on a complaint.

After the Classification Board classifies content, the content is not to be re-classified for two years. After the two year period, reclassification may occur when the Minister of Communications and the Arts or the ABA requires. When the Classification Board reclassifies material, it must notify the ABA of the new classification.

The Internet service provider, Internet content host or any “person aggrieved by the classification” may apply to the Classification Review Board to review the classification. The Minister and the ABA may also request review by the Classification Review Board. The Classification Review Board is a separate body from the Classification Board. The Amendment does not set out the fees but does command that they not be excessive. Classification decisions must be written decisions stating the result of the Board’s review.

Adult Themes: The treatment of any themes with a high degree of intensity should not be exploitative.

Drug Use: Drug use may be shown but not gratuitously detailed. Drug use should not be promoted or encouraged. Detailed instruction in drug misuse is not permitted.

Film Guidelines.

49. Id. sch. 5, cl. 14(2).
50. Id. sch. 5, cl. 14(4).
51. Id. sch. 5, cl. 16.
52. Applications for review must be made in writing and signed, and they must be accompanied by the appropriate fee. Id. sch. 5, cl. 17(1).
53. Id. sch. 5, cl. 17(5).
54. Id. sch. 5, cl. 18
If the Classification Board intends to reclassify content, then a public notice and comment submission must occur.\textsuperscript{55} The public is permitted to submit comments to the classification board prior to the reclassification of the content. The Classification Board must “take into account… the issues raised in submissions.”\textsuperscript{56}

5. \textit{Prohibited Content and Potential Prohibited Content}

In determining whether or not content is prohibited, it must first be determined if the content is based in Australia or in a foreign country. Australia-based content is prohibited content if “the Internet content has been classified RC or X by the Classification Board; or both (i) the Internet content has been classified R by the Classification Board; and (ii) access to the Internet content is not subject to a restricted access system.”\textsuperscript{57} Potential prohibited content is content which “(a)… has not been classified by the Classification Board; and (b)… were it to be classified by the Classification Board, there is a substantial likelihood that the Internet content would be prohibited content.”\textsuperscript{58} Internet content based outside Australia is considered prohibited “if the Internet content has been classified RC or X by the Classification Board.”\textsuperscript{59} The legislation is unclear as to exactly how this determination is made. It appears that the Classification Board actually examines the sites to determine if they should be restricted.

When Australia based content is classified R, it can be hosted when it is “subject to a restricted access system.”\textsuperscript{60} A restricted access system is an age verification device which limits access to certain Internet content to persons over age 18. A restricted access system is intended to protect children from exposure to unsuitable material.\textsuperscript{61} Attachment D provides an example of a site sign-on page.\textsuperscript{62} This site is subject to a restricted access system. This site’s restricted access

\textsuperscript{55} Id. sch. 5, cl. 15(1)(c) (“[i]f the Classification Board intends to reclassify the content, then: (c) the Director of the Classification Board must give notice of that intention, inviting submissions about the matter”).

\textsuperscript{56} Id. sch. 5, cl. 15(3).

\textsuperscript{57} Id. sch. 5, cl. 10(1).

\textsuperscript{58} Id. sch. 5, cl. 11(1).

\textsuperscript{59} Id. sch. 5, cl. 10(2).

\textsuperscript{60} Id. sch. 5, cl. 10(1)(b)(i).

\textsuperscript{61} American Broadcasting Authority, \textit{ABA Decides on Adult Verification Systems for Users who Wish to Access R-rated Internet Content}, Press Release, No 130/1999 (Dec. 8, 1999).

\textsuperscript{62} Pinkboard <http://www.pinkboard.com.au/home1/front.html> (visited Oct. 9, 2000) \textit{See} Attachment D (The Attachment is difficult due to the coloring on the site.)
system works in one of two ways. First, the person can post to the site operator evidence of age. This would likely be a scanned form of identification. Second, the person can spend AD$2 to register with a registration service that several sites will use and get an identification number that will be usable on all sites using that service.53

Through authority granted in the Amendment, the ABA has developed “minimum system requirements for restricted access systems for Internet content.”64 On December 8, 1999, the ABA issued a directive setting out minimum requirements for restricted access systems.65 In drafting the declaration, the ABA consulted industry representatives and accepted public comment.66

The directive requires all restricted access systems to, at a minimum, provide registration, qualification/validation, and access functions. The system must “receive applications for registration” in writing or electronically.67 The registration information collected must include name, age and credit card information, or a digital signature.68 Written applications must include name and some form of age statement (in the form of a declaration and a credit card or copy of identification).69 The system must verify age (either by confirming credit card information or authenticating the digital signature) and, upon verification, issue the user a personal identification number or a password.70 Finally, a restricted access system must condition access to R material upon entering the personal identification number or password for verification.71

6. Complaints process

The Online Services Amendment is mainly a complaint-based system. The backbone of the regulation is that consumers will file complaints with the ABA about Internet content. Only Australian residents, corporate bodies conducting business in Australia or

63.  Id.
64.  Online Servs. Amend. sch. 5, cl. 4.
68.  Id. at 3.2.1.
69.  Id. at 3.2.2.
70.  Id. at 2.1(2). See also id. at 4.2.
71.  Id. at 2.1(3).
national and state governments can file complaints with the ABA.\textsuperscript{72} A complaint can be filed when a person finds that “end-users in Australia can access prohibited content or potential prohibited content using an Internet carriage service.”\textsuperscript{73} Complaints can also be filed when a person believes that an Internet content host is hosting prohibited or potentially prohibited content.\textsuperscript{74}

All complaints must set out five things: the Internet content, means of accessing the content, country or origin (if known), reason for belief that content is prohibited, and any other information the ABA requires.\textsuperscript{75} Complaints must be in writing, but the Amendment allows for electronic transmission.\textsuperscript{76} Prior to January 1, 2000 (the effective date of the legislation) the ABA set up a system for receiving online complaints. Australians can log-on to the ABA Website and complete an electronic complaint form. The form provides blanks for all required information.\textsuperscript{77}

The ABA must investigate all complaints unless they find that the complaint is “frivolous, vexatious, not made in good faith,” or if it believes that the complaint was made for the purpose “of frustrating or undermining the effective administration” of the regulation.\textsuperscript{78} The ABA is required to notify the complainant of the results of the investigation.\textsuperscript{79} Attachment C is a response from the ABA which I found on the Internet.\textsuperscript{80}

The ABA may conduct investigations on its own initiative in certain circumstances. It may investigate Internet service providers whom they suspect of enabling end-users to access prohibited or potential prohibited content.\textsuperscript{81} It may investigate any Internet content host whom it suspect hosts prohibited or potential prohibited content in Australia.\textsuperscript{82} It can investigate any provider or host who it believes to have contravened appropriate industry codes.\textsuperscript{83}

\textsuperscript{72} Online Servs. Amend. sch. 5, cl. 25.
\textsuperscript{73} Id. sch. 5, cl. 20(1).
\textsuperscript{74} Id. sch. 5, cl. 20(2).
\textsuperscript{75} Id. sch. 5, cl. 22(3).
\textsuperscript{76} Id. sch. 5, cl. 24.
\textsuperscript{78} Online Servs. Amend. sch. 5, cl. 26(1), (2).
\textsuperscript{79} Id. sch. 5, cl. 26(3).
\textsuperscript{81} Online Servs. Amend. at sch. 5, cl. 27(1)(a).
\textsuperscript{82} Id. sch. 5, cl. 27(1)(b).
\textsuperscript{83} Id. sch. 5, cl. 27(1)(c).
a. Content hosted in Australia

The ABA takes two different approaches to complaints. If the complaint is about prohibited content hosted in Australia, the ABA must give the host “a written notice (a final take-down notice) directing the Internet content host not to host the prohibited content.” 84 The ABA must revoke a final take-down notice when reclassified content, previously subject to a final take-down notice is no longer classified prohibited content. 85 When an appropriate restricted access system is implemented on web sites containing R material previously issued final take-down notices, the ABA must revoke the take-down notice. 86

If the content is potentially prohibited content, and by definition unclassified under the regulation, then the ABA must review the classification to determine what classification it is likely to fall under. If the content is likely to be classified RC or X, then the ABA must give the host “a written notice (an interim take-down notice)” ordering that the content be taken down until classified by the Classification Board. In this situation, the ABA must ask the Classification Board to classify the content. 87 Content likely to be classified R will not be issued an interim take-down notice, but, while the ABA makes the initial judgment regarding the content, the ABA must request the Classification Board to classify the content. 88 When a content host voluntarily removes content subject to an interim take-down notice, the ABA may revoke the notice and notify the Classification that it is not to classify the material. 89

When potentially prohibited content is classified by the Classification Board, the ABA must notify the content host of the assigned classification. 90 If the classification results in the content being deemed prohibited content, then the ABA must issue “a written notice (a final take-down notice) directing the host not to host the prohibited content.” 91

84. Id. sch. 5, cl. 30(1).
85. Id. sch. 5, cl. 34(d).
86. Id. sch. 5, cl. 32(1)(d)(i).
87. Id. sch. 5, cl. 30(2)(a).
88. Id. sch. 5, cl. 30(2)(b).
89. Id. sch. 5, cl. 33(1).
90. Id. sch. 5, cl. 30(4)(a).
91. Id. sch. 5, cl. 30(4)(b).
The ABA also has the authority to issue special take-down notices. These notices instruct a content host "not to host the similar Internet content at any time when the interim take-down notice or final take-down notice...is in force."\(^9\)

Take-down notices must be complied with "as soon as practicable, and in any event by 6 p.m. on the next business day, after the notice was given to the host."\(^9\) Attachment B is an example of what I brought up when I tried to access a site subject to a final take-down notice.\(^9\)

b. Content Hosted Outside Australia

When the ABA finds that prohibited content is hosted outside Australia there are several actions that can or must be taken. If they think that the material is "sufficiently serious" then they should notify law enforcement officials.\(^9\) Next, the Amendment sets out two possible scenarios by which prohibited content hosted outside Australia is to be dealt with. First, if and when an industry code or set of standards is adopted, then the ABA must "notify the Internet service providers under the designated notification scheme set out in the code."\(^9\) If no standard or code applies, then the ABA must give written notice ("a standard access-prevention notice") to each Internet service provider ordering the provider to take reasonable measures to prevent access to the material.\(^9\) Basically, the Internet service provider will be required to block access to the content. It is unclear exactly how this is to be done, but it appears that the providers will have to update their filtering software to block the specific content.

The Internet industry\(^9\) has developed, and the ABA has approved, the *Internet Industry Codes of Practice.*\(^9\) The *Codes of

---

92. Id. sch. 5, cl. 36.
93. Id. sch. 5, cl. 36.
96. Id. sch. 5, cl. 40(1)(b).
97. Id. sch. 5, cl. 40(1)(c).
98. The process and participants involved in developing the *Codes of Practice* are discussed in section II(B)(7) of this paper.
Practice specifically set out a "designated notification scheme" in compliance with clause 40(1)(b). This notification system sets out how Internet service providers will be notified about prohibited or potentially prohibited content. This system comprises: (a) direct notification, whether by means of email or otherwise, by the ABA to the Suppliers of Approved Filters of information by which the relevant Prohibited or Potential Prohibited Content can be identified; and (b) notification by email by the ABA to ISP's on a regular basis of Prohibited or Potential Prohibited Content.

The Codes of Practice go on to say that the "ABA will not issue standard access prevention notices or special access prevention notices while the designated notification scheme contained in clause 6.1 of this Code is in effect."100 The Codes of Practice do not define commercial subscriber, and there is no indication in the statute or literature as to the exact difference between a subscriber and a commercial subscriber. Because the Codes of Practice have been drafted and accepted, the standard access prevention notice provisions of the Act are irrelevant.

The Codes of Practice set out the procedures by which Internet service providers are to deal with prohibited content hosted outside Australia.102 (See the next section for a discussion of the remainder of the Codes of Practice.) The Codes of Practice give Internet service providers two procedures for dealing with prohibited content. First, the Internet service provider providing Internet access to end-users in Australia "will as soon as reasonably practicable for each person who subscribes to an ISP's Internet carriage service provide for use, at a charge determined by the ISP, an Approved Filter."103 The section goes on to define provision for use as providing an Approved Filter as part of online registration, disk-based registration, or through post-registration notification of appropriate link.104 Second, the Internet service provider must provide commercial subscribers filtering software and arrange "access to consultancy services with respect to firewalls."105 This section of the Codes of Practice is very confusing. It

---

100. Id. 6.1.
101. Id. 6.2.
102. Online Servs. Amend. sch. 5, cl. 60(2)(d) (mandating that industry codes must set out procedures for dealing with prohibited content hosted outside Australia and includes the example: "procedures to be followed by a particular class of Internet service providers for the filtering, by technical means, of such content").
103. Codes of Practice, 6.2(a).
104. Id.
105. Id. at 6.2(b).
appears that Internet service providers must actively give their customers access to filtering software, but it is unclear whether or not the end-user must use the software.

The above question is not answered by examining the list of approved “filter products and services.”106 Schedule 1 of the Codes of Practice sets out approved filter products.107 Each of these products has been evaluated for the following characteristics: “(a) Ease of installation; (b) Ease of use; (c) Configurability; (d) Ability for updates in respect of content to be filtered, having regard to the requirements of the designated notification scheme provided for in Clause 6.1 . . . ; and (e) Availability of support.”108 These products were approved, in part, based on a study conducted by CSIRO. CSIRO examined possible filtering techniques at both the Internet service provider and end-user level. The resulting reports of this and other investigations show no indication that the industry is actually concerned about the effectiveness of the filtering technology used in the software. The legislation and the later government reports do not address the level of effectiveness required of filtering software.

CSIRO prepared a detailed report on the features of each of these products.109 Some of these systems are server-based filters.110 Server-based systems subject all end-users of that service to filtering. If this were the only type of filtering offered by Internet service providers, then basically all end-users receiving Internet access in Australia would be forced into receiving filtered content. But several of the approved filtering products are end-user based.111 The legislation implies that when an Internet service provider makes available an end-user based filtering system, that provider has

---


107. *Id.* (Sixteen products have been approved for use by Internet service providers: AOL Parental Control, Bair Filtering System, Csm Proxy Server, Cyber Patrol, Cyber Sentinel, Eyeguard, Genesis, Ifilter, Internet Sheriff, I-gear, KahooTz, Kidz.net, Net Nanny, Surfwatch, Too c.o.o.l, and Websense).

108. *Id.*


110. For example, Bair Filtering operates by routing all user requests “to a central global machine.” If the page has been previously accessed, it will be stored in the cache and retrieved if accessible. If it is not accessible, then the server will notify the end-user. If the page has not previously been accessed, the page is retrieved and examined by BAIR AI software run by supercomputers. The system examines the page for inappropriate text and visual images then makes a blocking decision.

111. For example, Net Nanny is an end-user based filtering software that is installed directly on an end-user’s computer. Net Nanny allows the end-user (parent or school) to structure what material can or cannot be accessed by that computer.
complied with its duty to restrict access to inappropriate foreign material under Clause 40(4).

The Codes of Practice further confuses matters by exempting Internet service providers from the filtering requirements of 6.2 with respect to service to certain end-users where that end-user is likely “subject to an arrangement that is likely to provide a reasonably effective means of preventing access to Prohibited or Potential Prohibited Content.” This means that any end-user that has informed the Internet service provider that he or she employs an Approved Filter or similar protection will not be subject to the requirements of 6.2. There is no duty on the Internet service provider to verify that an Approved Filter in fact has been employed by that end-user. This means that it would be relatively easy for end-users to lie about filter use. They could avoid the requirements of the law completely if they lie to their Internet service provider by merely claiming they have filtering software installed on their computers.

The end result is that there are great difficulties in determining exactly what the law requires for content based outside Australia. It is unclear whether the Internet service provider must offer a filtered service, whether all end-users must have an active filter on their desktops, and whether filters with parental controls will still be accepted if those controls allow the filter to be disabled by a password. As a final note, it is clear that R classified material is in no way regulated when it is hosted outside Australia.

112. Codes of Practice, 6.4.
113. Id. 6.4(c).
114. Online Servs. Amend. sch. 5, cl. 10(2).
### Structure of Australian Internet Content Regulation

<table>
<thead>
<tr>
<th>Classified</th>
<th>Content hosted in Australia</th>
<th>Content hosted outside Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Content is permitted only when subject to an approved restricted access system.</td>
<td>Content fully permitted. The Australian system does not regulate material in any way. (Filters might restrict access to this material even though the legislation does not restrict access.)</td>
</tr>
<tr>
<td>X or RC</td>
<td>Content is not permitted. Complaints based system is intended to monitor compliance. (Filter will most likely restrict access to most content in this category.)</td>
<td>Content is not permitted. Internet service providers are to provide filtering software to customers to prevent access.</td>
</tr>
</tbody>
</table>

7. **Industry Codes and Standards**

The *Online Services Amendment* sets out the procedures by which the Internet industry must develop industry codes and standards. These are to be developed by a body that the ABA “is satisfied . . . represents a particular section of the Internet industry.”

The Internet Industry Association of Australia developed a code of practice which was later approved by the ABA. The Internet Industry Association is a group of sixty Australian Internet service providers. The Association represents fewer than 10% of all Australian Internet service providers. Since the adoption of the

115. *Id.* sch. 5, cl. 52.
116. *Id.* sch. 5, cl 62.
Codes of Conduct, critics have asserted that the Codes represent the interests of the big service providers to the detriment of other Australian Internet service providers. Compliance with the Codes is voluntary according to the legislation, but effectively the ABA has the power to order any Internet service provider to comply with the Codes. A discussion of who can adequately represent Australian Internet service providers is beyond the scope of this paper. I have briefly discussed the Codes of Practice in the previous section, but the Codes address far more than how Internet service providers are to deal with unsuitable content hosted outside Australia.

The Online Services Amendment specifically sets out what material is to be addressed by the industry code. The legislation sets out separate requirements for both industry codes and industry standards, but the Codes of Practice serves as a publication comprising both requirements. This section of the legislation also provides that an industry association of Internet content hosts is to develop codes and standards. Currently, no content host industry standard or code has been released.

The Online Services Amendment sets out the “matters to be dealt with by industry codes and industry standards.” The Codes of...

an estimated 700 Internet service providers in Australia. The membership of the IIA consists of 60 of the largest Internet service providers in Australia).

120. Online Servs. Amend.at sch. 5, cls. 52-77.
121. Internet Industry Association, Codes of Practice (Dec. 1999) 2.1 (setting out the objectives of the Codes as both setting codes and standards).
122. (1) The Parliament intends that . . . an industry code and an industry standard that together deals with: each of the following matters: (c) procedures directed towards the achievement of the objective of ensuring that online accounts are not provided to children without the consent of a parent or responsible adult; (d) giving parents and responsible adults information about how to supervise and control children’s access to Internet content; (e) procedures to be followed in order to assist parents and responsible adults to supervise and control children’s access to Internet content; (f) procedures to be followed in order to inform producers of Internet content about their legal responsibilities in relation to that content; (g) telling customers about their rights to make complaints . . . ; (h) procedures to be followed in order to assist customers to make complaints . . . ; (i) procedures to be followed in order to deal with complaints about unsolicited electronic mail that promotes or advertises one or more Internet sites . . . that enable . . . end-users to access information that is likely to cause offence to a reasonable adult: (j) action to be taken to assist in the development and implementation of Internet content filtering technologies; (k) giving customers information about the availability, use and appropriate application of Internet content filtering software; (l) procedures directed towards the achievement of the objective of ensuring that customers have the option of subscribing to a filtered...
Practice specifically sets out conditions for many of these requirements. Primarily, the Codes set out procedures to which Internet service providers must adhere in order to ensure that minors are unable to open an Internet account.\textsuperscript{123} Other sections of the Codes of Practice cover each of the requirements set out in the legislation.\textsuperscript{124}

8. Online Provider Rules

This section of the legislation provides the enforcement mechanism in the form of “online provider rules.” The legislation defines online provider rules as rules set out in certain sections of the legislation. It appears that an online provider subject to online provider rules would be all entities included in the definition of Internet service providers. This section of the legislation is unclear. Compliance with an interim take-down notice, a final take-down notice, a special take-down notice and a standard access-prevention notice is an online provider rule.\textsuperscript{125} In addition, the compliance with relevant industry codes is considered an online provider rule.\textsuperscript{126} Finally, the ABA may make written determinations “setting out rules that apply to Internet service providers.”\textsuperscript{127} These determinations are considered online provider rules.

A person or corporation commits a criminal offense if it violates an online provider rule.\textsuperscript{128} An Internet service provider who fails to abide by an online provider rule, is punished by 50 penalty points (up to AD$27,000 per day).\textsuperscript{130} When an Internet service provider has violated an online provider rule the ABA issues a written direction to that provider requiring that it take specific action such as monitoring Internet carriage service; (m) procedures directed towards the achievement of the objective of ensuring that, in the event that a participant in the relevant section on the Internet industry becomes aware that an Internet content host is hosting prohibited content in Australia, the host is told about the prohibited content.”

\textit{Online Servs. Amend.}, sch. 5, cl 60.

\textsuperscript{123} Codes of Practice 5.1.

\textsuperscript{124} See id. at 5.2 (setting out how Internet service providers will deal with content hosts), 5.3 (setting out Internet service provider obligations for educating end-users about parental control devices), 5.4 (setting out means by which the Internet service providers will meet the complaint requirements of the legislation), 5.7 (dealing with unsolicited electronic mail).

\textsuperscript{125} \textit{Online Servs. Amend.} sch. 5, at 79.

\textsuperscript{126} Id. sch. 5, cl. 79(g).

\textsuperscript{127} Id. sch. 5, cl. 80(1).

\textsuperscript{128} Id. sch. 5, cl. 79(i).

\textsuperscript{129} \textit{Online Servs. Amend.} sch. 5, cl. 82(b).

\textsuperscript{130} Id. sch. 5, cl. 82.
compliance with rules or educating employees about rules. A person violating an ABA direction commits an offense punishable by 50 penalty points. A person committing an offense is guilty of a separate crime for each day during which the violation occurs. There are separate rules when the violation is committed by a corporate body.

The ABA may also seek relief in an Australian Federal Court. If the ABA thinks that an online provider or an online content host is violating an online provider rule it may request that a Federal Court order that person to stop supplying Internet service or stop hosting certain Internet content. The Federal Court will issue such an order at its discretion.

9. Civil and Criminal Immunity

An Internet service provider or Internet content host cannot be held civilly liable for actions taken in compliance with certain sections of approved industry codes. This includes immunity for filtering actions, compliance with access-prevention notices and compliance with take-down notices.

10. Effect on State and Territory laws

The intended structure of the regulation is for the Commonwealth to regulate Internet service providers and Internet content hosts while the States/Territories regulate end-users and content providers. This part of the regulation is set out by stating that a “law of a State or Territory... has no effect” when it regulates certain conduct of Internet service providers or Internet content hosts. An Internet content host cannot be held criminally liable for hosting content when they are not aware of the nature of the

131. Id. sch. 5, cl. 83.
132. Id. sch. 5, cl. 83(4).
133. Id. sch. 5, cl. 86.
134. Id. sch. 5, cl. 87.
135. Id. sch. 5, cl. 85.
136. Id. sch. 5, cl. 88(1).
137. Id. (providing immunity for actions taken pursuant to Clause 60(2)(d) which allows Internet service providers to deal with certain content by using filtering technology).
138. Id. (providing immunity for actions taken under Clause 48 complying with an access-prevention notice).
139. Id. (providing immunity when an Internet content host complies with a take-down notice under Clause 37).
140. Online Servs. Amend. sch. 5, cl. 91.
content.\textsuperscript{141} States are not permitted to require Internet content hosts to monitor the content hosted.\textsuperscript{142} Internet service providers cannot be punished for carrying material when they are not aware of its content,\textsuperscript{143} nor can they be punished for failing to monitor content.\textsuperscript{144}

11. Appeals to the Administrative Appeals Tribunal ("AAT")

Certain ABA decisions may be appealed to the Administrative Appeals Tribunal. When the ABA makes one of these decisions they must include in a statement of reasons for the decision and "a statement to the effect that an application may be made to the AAT for a review of the decision".\textsuperscript{145} An Internet service provider or an Internet content host can appeal the following decisions: take-down notices, classification decisions, access-prevention notices, a decision about compliance with industry codes, a decision finding a violation of an online provider rule, or an online provider determination.\textsuperscript{146}

C. The Legislation in Action

By the end of January, the ABA had received about 30 complaints.\textsuperscript{147} In April, the ABA released a report discussing the first three months of the regulatory scheme.\textsuperscript{148} The report stated that:

- The ABA issued 31 final take-down notices for Australian-hosted material;
- The ABA referred 45 items of content to the makers of filtering software for blocking;
- The ABA referred 7 items to law enforcement personnel;
- The ABA completed investigations of 99 of 124 complaints received as of March 31, 2000 while 23 complaints remain under investigation;
- Of the 99 investigations, the ABA reached a decision in 71 instances while 28 investigations were terminated because the ABA lacked sufficient information to complete the investigation;

\begin{flushleft}
\textsuperscript{141} Id. sch. 5, cl. 91(1)(a).
\textsuperscript{142} Id. sch. 5, cl. 91(1)(b).
\textsuperscript{143} Id. sch. 5, cl. 91(1)(c).
\textsuperscript{144} Id. sch. 5, cl. 91(1)(d).
\textsuperscript{145} Id. sch. 5, cl. 93.
\textsuperscript{146} Id. sch. 5, cl. 92.
\end{flushleft}
The ABA determined that 2 complaints were not made in good faith and therefore they were not investigated.\textsuperscript{149}

Below are two tables setting out the results of the investigations in which a decision was reached. T-2 sets out the decisions made about the content on the sites. T-3 sets out the actions taken by the ABA to have the content removed or blocked from the Internet.

**Content on Investigated Sites\textsuperscript{150}**

<table>
<thead>
<tr>
<th></th>
<th>Within Australia</th>
<th>Outside Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prohibited or Potentially</td>
<td>9</td>
<td>26</td>
</tr>
<tr>
<td>Prohibited Content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Prohibited or Potentially</td>
<td>27</td>
<td>9</td>
</tr>
<tr>
<td>Prohibited Content</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Action Taken Against Investigated Sites
(Sites can be represented in more than one category)\(^\text{151}\)

<table>
<thead>
<tr>
<th>Content within Australia</th>
<th>Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classified R – RAS not implemented – final take-down notice issued</td>
<td>5</td>
</tr>
<tr>
<td>Classified X – final take-down notice issued</td>
<td>3</td>
</tr>
<tr>
<td>Classified RC – final take-down notice issued</td>
<td>23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content Outside Australia</th>
<th>Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prohibited or potential prohibited – X – referred to makers of approved filters</td>
<td>10</td>
</tr>
<tr>
<td>Prohibited or potential prohibited – RC – referred to makers of filters</td>
<td>35</td>
</tr>
<tr>
<td>Referred to Police</td>
<td>7</td>
</tr>
</tbody>
</table>

Several Australia-based sites have moved to overseas locations in order to avoid certain requirements of the legislation. Australia sites containing R material must use a restricted access system, but R material located overseas is not subject to this requirement. This loophole has caused several sites hosting R material to relocate. Many are forced to drop the "\text{.au}" from their URL’s, but I found two sites that moved overseas while still keeping the "\text{.au}" in their URL.

### D. State and Territory laws

The second part of the regulatory scheme is much less structured. Only states/territories have the power to censor publications, films and other material.\(^\text{152}\) This results in a structure where the Commonwealth has the power to enforce take-down orders and filtering requirements, but it cannot prosecute content providers for

---

151. \textit{Id.}

posting or transmitting content. It is within the states responsibility to prosecute content providers posting or transmitting child pornography and other unsuitable material.

Soon after the passage of the Online Services Amendment, the Censorship Ministers of the States and Territories met to consider possible legislative changes necessitated by the Online Services Amendment. The meeting resulted in the drafting of model legislation to be inserted into the Classification (Publications, Films and Computer Games) Enforcement Act 1995. This Act provided the enforcement mechanism for the Commonwealth’s Classification (Publications, Films, and Computer Games) Act 1995. As of December 1999, no state/territory had taken action on the draft legislation. No state/territory is currently considering the draft legislation.

1. Victoria

Several states/territories have laws in place governing Internet content. Victoria has amended the Classification Enforcement Act to include a section regulating online information services. It is a crime punishable by up to two years imprisonment to publish or transmit, using an online information service, material considered objectionable. Objectionable material is defined as including material refused classification, child pornography or material that incites/instructs crime. It is a defense to prosecution that the defendant “believed on reasonable grounds” that the material was not objectionable.

The legislation also punishes publication and transmission, to a minor, of material unsuitable for minors. If the material made available to the minor is objectionable, publication or transmission is punishable by up to two years in prison. There is only a six month penalty when the material is unsuitable but not objectionable. Defenses are available for defendants who believe that the recipient of the material was an adult, defendants who have “taken reasonable steps to avoid publishing or transmitting” the material to a minor, or

153. See id.
154. See id.
155. See id.
157. Id. at § 58(1)(a).
158. Id.
159. Id.
160. Id. at § 58.
for defendants who believed "on reasonable grounds" that the material was not unsuitable for minors.\textsuperscript{161}

2. \textit{Western Australia}

Western Australia passed the Censorship Act of 1996 which, in part, addresses Internet content. The Act criminalizes the knowing transmission of objectionable material, possession of objectionable material, advertising objectionable material and requesting the transmission of objectionable material.\textsuperscript{162} The definition of objectionable is very broad. It includes material classified RC, child pornography, material that promotes crime or violence, material that depicts violent sex acts, depictions of necrophilia, depictions of urine or excrement in association with sexual conduct, bestiality and depictions of extreme violence.\textsuperscript{163} Violation of this section is punishable by a AD$15,000 fine or 18 months in prison. If the offense is committed by a corporate body it is subject to a AD$75,000 fine.\textsuperscript{164}

The Act also limits access to restricted material as well. Restricted material is material that "a reasonable adult, by reason of the nature of the article, or the nature or extent of references in the article, to matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, would regard as unsuitable for a minor to see, read of hear."\textsuperscript{165} A person must not transmit or make available restricted material to a minor.\textsuperscript{166} An offense under this section is punishable by a fine of up to AD$5,000. Corporate bodies can be subject to a AD$25,000 fine.\textsuperscript{167} The Act provides defenses for complying with restricted access systems and good faith efforts not to make such material available to minors.\textsuperscript{168}

3. \textit{Northern Territory}

The Northern Territory Act is almost identical to the Western Australia legislation with a few exceptions.\textsuperscript{169} The penalty for all violations is AD$10,000.\textsuperscript{170} No prison sentences are provided for. The

\begin{itemize}
\item \textsuperscript{161} Id.
\item \textsuperscript{162} Censorship Act 1996 (WA) § 101.
\item \textsuperscript{163} Id. at § 99.
\item \textsuperscript{164} Id. at § 101(1)(e)(B).
\item \textsuperscript{165} Id. at § 99.
\item \textsuperscript{166} Id. at § 102(1).
\item \textsuperscript{167} Id. at § 102(1)(b).
\item \textsuperscript{168} Id. at § 102(3)
\item \textsuperscript{169} See Classification of Publications, Films and Computer Games Act (NT) § 50X.
\item \textsuperscript{170} Id. at § 50Z.
\end{itemize}
Act provides defenses for “articles of “recognized literary, artistic or scientific merit” and “a bona fide medical article.”

4. New South Wales, Queensland, and South Australia

Legislation in New South Wales, the leader in drafting the draft legislation, has yet to be approved. Queensland and South Australia have not adopted Internet content legislation.

E. Educating Australia about the Internet

The third goal of the regulatory system is to educate Australians about the regulation, the complaints process, filtering options and child Internet safety. The ABA created a website to provide Australians with information about safety on the Internet. The site is a useful resource for parents searching for information about Internet safety. The site provides recommended use rules for children of different ages. It also informs parents about unsuitable information available on the Internet and tools for filtering.

Second, the government created a separate government body, NetAlert, under the supervision of the National Office for the Information Economy. The organization is made up of industry, educational and community representatives. It was established to research new technologies such as filtering and access management. The body is also responsible for communicating to Australian parents ways in which they can keep their children safe online.

171. Id.
173. In 1996, a student was arrested because he possessed, in the form of computer files, objectionable material. Queensland attempted to prosecute the man under the broad language of the computer games section of the Queensland Classification of Computer Games and Images (Interim) Act 1995. The Act defined an image in a computer game as a “computer generated image.” The Judge refused to apply the Act to images transmitted over the Internet. He stated that “this legislation is not intended to be a solution to all problems with which we have been confronted by the information technology revolution. Currently, bulletin boards and the Internet are not regulated by this legislation.” Electronic Frontiers Australia, The First “Net Porn” Trial in Queensland Verdict: Not Guilty <http://rene.efa.org.au/liberty/qcaseone.html> (last updated Dec. 15, 1996).
174. Id.
177. Id.
178. Id.
F. Criticisms of the Australian System

The Australian system can be criticized on several grounds. First, the legislation will be unable to reach most unsuitable material transmitted over the Internet because that material is transmitted by e-mail. Unlike the CDA, the Australian legislation does not reach e-mail and therefore any communication between two end-users will not be punishable. This is a serious concern because, as is widely expressed by proponents of the legislation, one main purpose is to protect children from cyberstalkers.\textsuperscript{179} By not reaching e-mail, the legislation fails to cover the area of the Internet where most of this action occurs.

Second, the law will not reach a great deal of the material at which it is aimed for several reasons. First, the legislation cannot reach material contained on host computers outside Australia. The only protection provided to end-users in Australia from inappropriate material available from overseas is to trust the filtering systems adopted by their Internet service provider. Proponents of the legislation consider a censored Internet a protection, while opponents consider it oppression. An argument about the filtering scheme can be made by both sides. First, the filters will not work to block out some material that people would consider inappropriate. Second, the filters filter out material which is not objectionable and therefore legal for Australian adults to view. Finally, the filter requirement is easily circumvented. A person need only notify their Internet service provider that they have an Approved Filter device to avoid the filter requirement.

Next, the legislation does not even attempt to regulate R-rated material based outside Australia. This material would be subject to a restricted-access system if based in Australia, but is not subject to any access prevention techniques when based overseas. This will force content hosts currently based in Australia to move to foreign countries. Content hosts also are remaining based in Australia, while at the same time basing their content on computers located in foreign countries. They do this in order to get around the restricted-access system requirement which has proven to be very expensive for content hosts.

The regulation is detrimental to the medium and small Internet service providers. Large Internet service providers primarily maintain filtering options which will be conveniently adapted to the Australian

\textsuperscript{179}. This is a situation where a pedophile encounters a child in a chat room and then engages in an e-mail exchange with that child.
requirements at a relatively low cost. Smaller scale providers are forced to either install expensive server based software or offer user based software as part of their service. This is extremely expensive for these companies, which are generally new companies with little capital. The regulation has forced upon them unexpected costs, which they are unable to costs on to their customers because, if they do, they will no longer be able to compete with the large providers that have developed filtering software.

Finally, the legislation is likely to have a chilling effect on Internet speech in Australia. This occurs in two ways. First, content hosts will be inhibited from posting content which might subject themselves to a complaint and subsequent rating. Hosts will not have to deal with the issuance of a take-down notice so they will place only content on their sites that they are sure will not be classified R, X, or RC. Second, Australian end-users will be chilled in what they access. They will be forced to self-identify in order to access any material covered by a restrictive access system. Part of the uniqueness of the Internet is that a person can access information, including pornography, without having to go out into the public to get it. This is a form of freedom that is often associated with a person's right to receive information. The Australian legislation has removed this benefit. End-users will therefore be less likely to access information on the Internet that they have a right to access.

III
Comparisons with United States efforts to regulate the Internet

In this section I will compare the approaches of the United States and Australia regarding Internet regulation. This discussion requires a brief discussion of the United States effort and failure to regulate the Internet. Following this discussion, I will examine both the differences and the similarities between the two approaches. Finally, I will discuss why neither approach is likely to work for the respective countries because of the nature of the Internet.

A. United States' attempts to regulate the Internet

The presence of porn on the Internet encouraged Congress to regulate Internet content. In a 1995 survey, eighty-five percent of Americans polled stated that they were "concerned about children

180. For example, AOL has maintained Parental Control as a part of its proprietary network and the program has been easily altered to meet the requirements of the Australian regulation.
seeing pornography on the Internet.\textsuperscript{181} Congress responded to this concern with the Communications Decency Act of 1996 (CDA).\textsuperscript{182} There are two main parts to the CDA. First, the CDA institutes criminal penalties for the use of a computer service to transmit certain material. Second, the CDA provides Internet service providers with immunity and certain affirmative defenses for certain activities.

Section 502 of the CDA provides criminal penalties for any person who: in interstate or foreign communications - by means of a telecommunications device knowingly - makes, creates, or solicits, and initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication.\textsuperscript{183}

It is important to note that the person need not intentionally communicate inappropriate material to a minor, nor must the material be obscene. This legislation presents delicate jurisdictional difficulties presented by the legislation because it seeks to regulate foreign material. Finally, the Act does not provide a definition for indecent material.

The Act provides three main defenses for Internet service providers. An Internet service provider is immune under a "Good Samaritan" defense when and if it did not take part in the creation of the content.\textsuperscript{184} An Internet service provider will also be immune from liability when it shows that it made a "good faith" effort to ensure that minors do not have access to unsuitable material.\textsuperscript{185} Finally, the service provider will be immune from liability when it restricts access to the content by requiring a valid credit card number or other personal identification number.\textsuperscript{186}

Legal attacks immediately followed adoption of the Act. The American Civil Liberties Union brought a suit seeking a preliminary injunction.\textsuperscript{187} After making extensive findings of fact, the Court held that the Act was an improper restriction on freedom of speech. The
Court's holding struck down the sections of the Act making it a crime to knowingly transmit indecent material. The court did not rule on the immunity provisions.

After the failure of the CDA, Congress passed the Child Online Protection Act ("COPA") in an effort to meet with the constitutional shortcomings of the CDA. The Act was immediately challenged by the ACLU and other parties as an unconstitutional burden on speech. COPA only seeks to regulate the actions of commercial web sites that make available information "harmful to minors" without a system for restricting access to adults. The court found that COPA constituted an undue burden on commercial web site operators because the financial burden of instituting an access system has the effect of restraining expression. The District Court issued a preliminary injunction barring the enforcement of COPA. This decision has yet to be appealed.

B. Differences and similarities between the United States and Australian approach

The most important difference between the laws in Australia and the United States is that the Australian law remains in effect. The CDA and COPA are not good law in the United States and cannot be enforced because they violate the First Amendment. It is likely that the Australian legislation would violate the First Amendment of the United States Constitution, but Australia does not have speech protection similar to the First Amendment. The Australian legislation has not yet been challenged in court.

Australia and the United States shared a similar concern in their effort to regulate Internet content. Citizens of both countries felt that pornography and other inappropriate material easily available on the Internet posed a threat to their children. It is important to note that United States citizens expressed a slightly different concern than Australian citizens. People in the United States were very concerned about "cyber-stalkers." "Cyber-stalkers" are people, generally pedophiles, who enter chat-rooms set up for children and engage the children in conversation. Generally, the "cyber-stalker" continues communication with the child by e-mail. Often the e-mail will slowly become invasive and indecent. Sometimes, the "cyber-stalker"

188. Communications Decency Act, § 502.
190. Id. at § 231(a)(1).
attempts to arrange a meeting with the child. Due to concerns about "cyber-stalkers," Congress included regulation of both e-mail and chat-rooms in the CDA. There is little indication that Australians were particularly concerned about "cyber-stalking." As evidence of this lessened concern, the legislation does not include regulation of e-mail or chat-rooms.

The Australian legislation is directed at information available on web sites on the World Wide Web. The majority of all web sites are based in the United States. While Internet content hosting is growing in Australia, the vast majority of the sites accessed by Australians are based in other countries. Therefore, it was crucial for the crafters of the Australian legislation to set up a regulatory system that could effectively restrict access to non-Australian sites. The United States faced a similar situation, but the problem was not as important in the crafting of the legislation because the United States housed most sites. The CDA and COPA did not specifically address the jurisdictional issue. It is relatively unclear how the United States planned to pass out criminal penalties to foreign citizens for Internet postings made outside the United States.

Australia specifically dealt with the presence of inappropriate international material. The legislation provides separate means of regulating content based on where the content is hosted. Furthermore, the legislation does not seek to reach the content host (that would not appear to be possible). Rather, it seeks to regulate the presence of the international content within their boarders by mandating Internet service provider rules which require Internet filtering. This is very different from the United States approach, because the United States did not place any requirements on the Internet service providers.

Another major difference between the United States and Australian regulatory systems is the definitions used to classify material. The Australian legislation (an accompanying regulations) very specifically sets out when a site will be prohibited content. It will be relatively clear to Australian citizens when they have accessed a prohibited site. The United States statutes define prohibited content as obscene and indecent. This is extremely vague because these are legal terms with specific definitions defined in the common law. 192

192. See Miller v. California, 413 U.S. 15, 24 (1973) (defining obscenity as material which "the average person, applying contemporary community standards would find . . . , taken as a whole, [1] appeals to the prurient interest . . . ; [2] depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law . . . ; [3] [and] taken as a whole, lacks serious literary, artistic, political, or scientific value")
The Australian legislation specifically mandates the use of restricted access systems. This form of age verification will be relatively expensive for content hosts to implement. Australian drafters did not concern themselves with this burden. In the United States, although the legislation did not address the financial burden of age verification systems, the courts found that this expense greatly hindered free expression. It appears that Australia has favored possible censorship resulting from financial hardship over free expression.

Finally, both countries provide immunities from prosecution to certain groups. First, both countries provide immunity for Internet service providers when they filter the Internet. The Australian legislation also provides immunity for content hosts when they comply with the age verification requirement. The United States legislation went further. It provided immunity for Internet service providers who made a “good faith” effort to ensure that minors not be exposed to inappropriate material. The Australian legislation provides immunity for such providers when such effort includes filtering. An Australian Internet service provider can be criminally liable for failing to filter the Internet. In no way does “good faith” effort require Internet service providers in the United States to filter.

### IV

**Conclusion**

The Australian Internet content regulation will be, at best, difficult to enforce. Much of it depends on the effectiveness of filters and the cooperation of Australian Internet service providers. It is a regulatory framework that would most certainly violate the First Amendment of the United States constitution for many of the same reasons expressed in the CDA and COPA decisions. The legislation is still in its infancy, and the effects have not been fully realized. It is certain that content hosts have been forced overseas, and that those who cannot afford the move have been forced to shut down their sites or drastically alter content.