WORLD LEADER OR VILLAGE IDIOT? AN EXAMINATION OF INTERNET CONTENT REGULATION IN AUSTRALIA.

Carolyn Penfold

Thesis submitted for the degree of Master of Laws

University of New South Wales

2004

THE UNIVERSITY OF NEW SOUTH WALES
Thesis/ Project Report Sheet

Surname or Family name: **Penfold**

First Name: **Carolyn** Other Name/s: **Rachel**

Abbreviation for degree as given in the University Calendar: **LLM**

School: **Law** Faculty: **Law**

Title: **World Leader or Village Idiot? An Examination of Internet Content Regulation in Australia.**

Abstract 350 words maximum:

This thesis examines the internet content control regime introduced to Australia in 1999. Considerable conflict surrounded the introduction of the scheme, and it raised many questions which were left unanswered: Could the scheme meet its own objectives? Would it stifle free speech? Would it damage the internet industry? Would it influence internet content control overseas? Were there better alternatives? And above all, did the scheme show Australia to be the village idiot of the internet world, or would Australia in fact turn out to be a world leader in this area?

This thesis attempts to answer these questions. Part one examines the context into which the online content regime was introduced, and discusses both the limitations and the possibilities which arose from this context. Part two examines in depth the introduction of the scheme, its specific provisions, and its operation and effects. Relevant legislation, codes of practice, surveys, studies, submissions and reports on the scheme are used for this purpose. Part three of the thesis attempts to evaluate the regime, measuring its effects firstly against its own objectives, and then comparing it with schemes overseas. Finally, the thesis makes recommendations for changes to the Australian scheme which may remove some of its problems and inconsistencies, and improve the regime for the future.

The thesis concludes overall that Australia is probably neither world leader nor village idiot. The internet content control regime has not been effective in controlling access to internet content, but neither has it crippled the internet industry, or stifled free speech. There is however a great deal which the Government might do to improve the scheme.

ACKNOWLEDGEMENTS

Many thanks to Professors Michael Chesterman and Graham Greenleaf for their guidance, insight, suggestions and corrections, and to Dr Kathy Bowrey and Professor Jill McKeough for their constant encouragement. Thanks also to Mark Walters for his assistance with referencing.

ORIGINALITY STATEMENT

'I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.'

Signed .....

WORLD LEADER OR VILLAGE IDIOT?
AN EXAMINATION OF INTERNET CONTENT REGULATION IN AUSTRALIA.

Carolyn Penfold

PART 1: Putting internet content control into context.

PART 2: Passage, provisions, operation and effects of the internet content control regime.

PART 3: Evaluating and improving the internet content control regime.

PART ONE

PUTTING INTERNET CONTENT CONTROL INTO CONTEXT.

CHAPTER ONE: INTRODUCTION

This thesis examines the Australian scheme for internet content regulation. It details the context into which the scheme was introduced and the operation of the scheme, before evaluating its effectiveness and making suggestions for the future improvement of the scheme. The current chapter introduces some of the issues involved in the introduction and operation of that scheme, and then goes on to outline the structure of the thesis as a whole.

A. Background

Discussion surrounding internet censorship was not new when the Broadcasting Services Amendment (Online Services) Bill[1] was introduced to Parliament in April 1999, nor was it uniquely Australian. Technological, jurisdictional, political and social concerns regarding internet censorship had been raised and discussed in many parts of the world, and a number of countries had themselves introduced legislative or other schemes in attempts to control internet content. But the issues involved in internet censorship suddenly became more immediate, more important and more focused in Australia, with the introduction of the Online Services Bill.

The internet, a most innovative and exciting new communications phenomenon, had developed and changed at a rapid pace. Although at the time of the introduction of the Online Services Bill access to the internet had been available to the Australian public for a short time only, during that time there had been very significant developments in how, and how much, it was used. Access to the internet in Australia had initially been limited to research uses, but the policy changed in 1993 to allow a 'user-pays, anything-goes environment.'[2] A

[1] Broadcasting Services Amendment (Online Service) Bill 1999 (Cth). Known, and hereafter referred to as the Online Services Bill, and then as the *Online Services Act*. Where reference is made to specific clauses of the Broadcasting Services Amendment (Online Service) Bill 1999 (Cth), these refer to clauses in schedule 5 of the final version of the Bill, unless otherwise stated.
[2] Attributed to Hugh Irvine, founder of Connect.com.au by Jenny Sinclair, 'Everybody's gone surfin', *The Age,* 19 June 1999.

subsequent explosion occurred in internet use.[3] A total of less than 12 internet service providers (ISPs) in Australia at the end of 1993 grew to 130 by the end of 1995, by which stage the number of internet-linked computers was increasing by 50% per annum.[4] By the time of the introduction of the Online Services Bill, the number of ISPs in Australia had risen to an estimated 650.[5] Internet access was becoming readily available in many businesses and other places of employment, in schools and other educational institutions, in public libraries, in cafes, and in homes. In fact, such was the saturation of internet access that by mid 1999, with the Online Services Bill before Parliament, it was claimed that Australia had the 'highest percentage of internet usage in the world' after the USA.[6]

Citing community concern, generated apparently by the growth of the medium, the material available on it, and the risk to children of exposure to inappropriate content, the Government decided to legislate to regulate the internet.[7] Cynics suggested the real motivation was instead the government's need to woo arch-conservative Senator Harridine's support to pass other – unrelated – legislation.[8] While this need could not be seen as the genesis of internet regulation, given that that had been on the Government's agenda since at least 1995, it may have helped

---

[3] The early 1990's had seen the introduction of the World Wide Web, at first in a limited form, but expanding hugely as browsers developed to offer Unix, Mac and PC users uniform interfaces for access. 'Explosive growth' of the Web began in 1994, followed by an explosive growth of the internet. Roger Clarke, *Origins and Nature of the Internet in Australia* (2004) Principal, Xamax Consultancy Pty Ltd, Canberra <http://www.anu.edu.au/people/Roger.Clarke/II/OzI04.html > at 16 June 2004).

[4] Australian Broadcasting Authority, *Investigation into the Content of Online Services, Issues Paper*, (Dec 1995) 14. Note conflict with *A history of AARnet*, accessed at AARnet site <http://www.aarnet.edu.au/about/history.html> at 17 June 2004 which states that there were over 300 commercial ISPs by June 1995.

[5] Broadcasting Services Amendment (Online Service) Bill 1999, Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 21 April 1999, 3957, 3958 (Senator Ian Campbell, Parliamentary Secretary to Senator Alston, Minister for Communications, Information Technology and the Arts).

[6] Nadine Strossen, President of American Council for Civil Liberties, quoted in 'Australia urged to repeal law', *Sydney Morning Herald* (Business section), 24 August 1999. It is difficult to know whether this was precisely true. In 1996 Australia was said to be 'the fifth largest user of the Internet.' *Internet Australasia* (May 1996) 98, quoted in Australian Broadcasting Authority, *Investigation into the Content of Online Services, Report to the Minister for Communications & the Arts* (1996) 35. According to Nua surveys 30.5% of the Australian population were online as at May 1999, compared to 37% of the US population. It is possible though that some Scandinavian countries had higher proportions of internet users. See Nua Surveys, *How Many Online?* (2002) <http://www.nua.com/surveys/how_many_online/index.html> at 22 June 2004

[7] Senator Ian Campbell, above n 5, 3957.

[8] See for example David Marr, *The High Price of Heaven.* (1999) 114. This is discussed further in Chapter 7 below.

to explain the haste with which it was drafted, introduced and passed, despite serious concern and criticism.

In April 1999 the Online Services Bill was introduced to Australia's federal Parliament, with the objects of

> a) providing a means for addressing complaints about certain Internet content,
>
> b) restricting access to certain Internet content likely to cause offence to a reasonable adult, and
>
> c) protecting children from exposure to Internet content that is unsuitable for children.[9]

The regulation was intended to occur in a manner which did not impose unnecessary financial or administrative burdens on the internet industry, readily accommodated technological change, and encouraged the development of technology and the provision of services.[10]

B. Response to the Bill

The legislation was met by howls of derision on the one hand, and by delight on the other. It was said to be 'a largely ineffective and wasteful piece of legislation' which exemplified symbolic politics.[11] It was argued that a 'unilateral national response is destined to be unsuccessful, given the global and elusive nature of the medium.'[12] Claims were also made that the legislation would prove Australia the 'global village idiot' of the internet world.[13]

---

[9] Broadcasting Services Amendment (Online Service) Bill 1999 (Cth) (schedule 1) cl 2, now incorporated as *Broadcasting Services Act 1992* (Cth) s 3(1)(k),(l)&(m).

[10] Ibid (schedule 1) cl 4, now incorporated as *Broadcasting Services Act 1992* (Cth) s 4(3).

[11] Peter Chen, 'Pornography, Protection, Prevarication: The Politics of Internet Censorship,' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 18, 18.

[12] Ibid 22.

[13] Strossen, above n 6, referring to a comment by Danny Yee of Electronic Frontiers Australia: 'The government has turned Australia into the global village idiot.' EFA Media Release 26th May 1999. <http://www.efa.org.au/Publish/PR990526.html> at 22 July 2004.

Countering these claims were suggestions that 'the village idiot usually turns out to be the wisest member of the community.'[14] Some argued that the legislation ought to be 'applauded [as representing] a serious attempt to address the availability to children of material on the Internet that the Australian community has already decided should not be readily available to children.'[15]

While such strong reactions were being voiced both for and against the legislation, it was also suggested that the apparently flawed legislation was in fact a result of these conflicting arguments themselves. One lawyer wrote:

> Talking about Internet censorship is like discussing abortion; the debate is confused, emotive and polarised. The protagonists mark out their territory based on flawed assumptions and a passionate belief in the absolute truth of their principles. Conservative groups preach family values, industry focuses on e-commerce, and civil libertarians obsess with free speech. It is a collision of values and interests, without room for compromise, pragmatism and discretion. The result? The *Broadcasting Services Amendment:* ... confused, ill-conceived, and very difficult to implement in practice.[16]

C. Arguments against the Bill

Arguments put against the Online Services Bill included arguments against censorship per se, arguments against censorship of the internet specifically, arguments that internet censorship was technically impossible, and arguments against the specific scheme proposed.

Arguments against censorship or content regulation itself, or against censorship of the internet specifically,[17] were used to challenge the Online Services legislation, but were given short shrift by the Government. The Government saw no need to

---

[14] Melinda Jones, 'Free Speech and the 'Village Idiot.'' (March 2000) 6(1) *UNSWLJ Forum*, (*Internet Content Control)* 43, 43.
[15] Elizabeth Handsley & Barbara Biggins, 'The Sheriff Rides into Town: A Day of Rejoicing for Innocent Westerners.' (March 2000) 6(1) *UNSWLJ Forum*, (*Internet Content Control)* 35, 38.
[16] Niranjan Arasaratnam, 'Brave New (Online) World.' (March 2000) 6(1) *UNSWLJ Forum*, (*Internet Content Control)* 10, 10.
[17] See for example John Perry Barlow, *Declaration of Independence in Cyberspace*. (1996) <http://www.eff.org/barlow/Declaration-Final.html> at 16 June 2004, and the discussion in D Post & D Johnson, 'Law and Borders – The Rise of Law in Cyberspace,' (1996) 48 *Stanford Law Review*, 1367.

re-examine its existing censorship regime, and rejected arguments that the internet as a medium required a different or special regulatory framework. While willing to look at the differences in medium which required differing *methods* of regulation, the Government was not willing to countenance a regime different in *substance* to that existing for other media. In the view of Senator Alston, the Minister for Communications, Information Technology and the Arts, it was simply not 'acceptable that standards applicable to conventional media do not also apply to the internet.'[18]

Technical arguments were also used to suggest that the government had misunderstood its subject. It was claimed that censoring the internet, whether desirable or not, was technically impossible. Traffic on the internet could circumvent blocks, content could be encrypted to travel without detection, users could protect themselves with anonymity, content could be hosted anywhere in the world. Blocking or even removing content from one server would not stop access to the same content from other servers, and other jurisdictions.[19] Again the government rejected the arguments, acknowledging that it would be *technically* difficult to control internet content, but denying that this would make the regulation worthless. '...There are technical difficulties with blocking... [but] where it is technically feasible and cost-effective ... this should be done. It is not acceptable to make no attempt at all on the basis that it may be difficult.'[20] While the technical difficulties were thus taken into account in shaping the legislation, they would not affect the decision on whether or not to legislate.

The details of the proposed scheme also led to concern and argument. The government claimed internet censorship was to be in line with the existing classification scheme which was 'based on contemporary community standards... well understood and accepted within our society.'[21] Senator Alston regarded it as

[18] Senator Alston, 'The Government's Regulatory Framework for Internet Content', (March 2000) 6(1) *UNSWLJ Forum*, (*Internet Content Control*) 4, 6.
[19] See for example Kimberley Heitman, 'Vapours and Mirrors' (March 2000) 6(1) *UNSWLJ Forum*, (*Internet Content Control*) 30; Peter Coroneos, 'Internet Content Control in Australia: Attempting the impossible?' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 26.
[20] Senator Ian Campbell, above n 5, 3963.
[21] Senator Alston, above n 18, 4.

a 'logical step to legislate to extend the classification system to the internet.'[22] However, due to the sheer quantity of internet content, the classification scheme as used in other media was not a real option. There was simply too much material to classify. Furthermore, the existing classification scheme required restriction of certain content. If content on the internet were to be restricted, it was likely that it would need to be done at the level of internet content hosts (ICHs) and ISPs. It was argued that placing such a burden on the industry would be unjustified (like asking Australia Post to restrict mail deliveries on the basis of content) and financially onerous.[23] It may thus cripple the industry's potential for growth and expansion.

There was also concern that the quantity of internet content meant that any monitoring or blocking would need to be automated, and as such would require the use of filtering software. Filtering software was reported to over-block, under-block, take a broad-brush approach, to be biased at times, and was not Australian.[24] It was argued that no filtering could effectively restrict content in line with Australia's 'contemporary community standards.'[25] Further, internet content regulation raised freedom of speech concerns. Not only may filters block more than required, but who would know what they blocked and on what basis? Requiring ISPs and ICHs to monitor or block content would introduce private censorship,[26] and the real possibility of over-censorship by industry to avoid potential breaches.

---

[22] Ibid.
[23] Coroneos, above n 19.
[24] Many such reports were available, especially from the USA. These included for example Electronic Privacy Information Center (Epic), *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* (December 1997) < http://www.epic.org/reports/filter_report.html > at 16 June 2004; Gay and Lesbian Alliance against Defamation (GLAAD) *Access Denied, The Impact of Internet Filtering Software on the Lesbian and Gay Lesbian Community,* (December 1997). <http://www.glaad.org/documents/media/AccessDenied1.pdf> at 16 June 2004 and numerous studies into the operation of individual filters carried out by Peacefire. See <http://www.peacefire.org> at 16 June 2004.
[25] See for example Irene Graham, *Comments on IIA Approved Filters and CSIRO Filter Evaluation Report* (Jan 2000), <http://libertus.net/liberty/rdocs/apprfilters0001.html> at 22 July 2004 and reports listed therein, and note Australian Broadcasting Authority, above n 6, 151.
[26] See for example Heitman, above n 19, 30.

Other details of the scheme also suggested that the control of internet content would not be in line with control of content in other media. For example, all internet content was to be classified as film,[27] even when it bore no resemblance to film, and even where the content in question was simple text. Furthermore, X-rated material on Australian servers was to be prohibited,[28] although it was not illegal to possess X-rated material in Australia, nor to sell or distribute it within and from the Australian Territories. R-rated material hosted in Australia was also to be prohibited unless hosted with restricted access,[29] while no provision at all was made relating to overseas hosted R-rated content.

D. Government response to criticism of the Bill

Between the introduction to Parliament of the Online Services Bill and the *Act's* commencement, it was very unclear what the legislation's effect would actually be. If internet content was really to be controlled like content in other media, the internet industry would have a great deal of work on its hands to ensure that prohibited content was neither hosted in Australia nor carried in from overseas. However, the concern to control content without overly burdening industry was clear in Government statements on the issue,[30] and the objects of the legislation were specifically qualified with a statement that the regulation was to occur in a manner that 'does not impose unnecessary financial and administrative burdens on Internet content hosts and Internet service providers...'[31]

In fact, while the Government claimed to be legislating so that control of internet content would mirror control of content in other media, it was eventually convinced of the technical difficulties of achieving this aim. It thus introduced a general legislative framework which detailed procedures to deal with Australian-hosted content, but which lacked detail regarding how overseas-hosted content was to be controlled. It left the internet industry itself to decide the appropriate

[27] Broadcasting Services Amendment (Online Service) Bill 1999 (Cth) cl 12&13.
[28] Ibid cl 10.
[29] Ibid.
[30] See for example Senator Ian Campbell, above n 5.
[31] Broadcasting Services Amendment (Online Service) Bill 1999 (Cth) (schedule 1) cl 4.

way of carrying out such control. Under the legislation, the internet industry was to draft and register with the ABA Industry Codes of Practice which specified, amongst other things, the action industry would be required to take in response to notices issued by the ABA.[32] If such codes were not registered, the ABA was authorised to write industry standards itself.[33] It was not until a fortnight before that *Act* commenced that the Internet Industry Codes of Practice were registered with the ABA, and the industry, the public, and internet users began to discover more detail about how the content control regime was likely to work.

UNANSWERED QUESTIONS.

The establishment of a scheme for controlling internet content in Australia gave rise to, and left unanswered, a number of important questions. What effect, if any, would the *Act* have? Would it meet its aims? Would it stifle free speech? Would it cripple the internet industry? Would it be valuable in any way? Would it have any impact outside Australia? Could it be improved upon?

In an attempt to answer such questions, this thesis examines the internet content regime, evaluates the effect which it has had over the last four years, and makes suggestions for possible improvements to the regime. To help understand the regime and the *Online Services Act*, the thesis begins by discussing in Part One the context within which the enactment was made. Chapters Two and Three thus focus on the internet itself, the distinctions between this medium and others which the Government was familiar with censoring and regulating, and the technical methods which might be employed in attempts to control internet content. Chapter Four outlines prior overseas attempts to regulate internet content, which helped inform the Government as to what regulation would be possible and appropriate in Australia. Chapter Five examines the system of censorship and classification which existed in Australia prior to the enactment of the *Online Services Act*, and also discusses the protections for freedom of speech in Australian law, in particular to distinguish these from the better known US

[32] Broadcasting Services Amendment (Online Service) Bill 1999 (Cth) cl 60 - 61.
[33] Ibid cl 68 - 71.

protections. Chapter Six examines the development of industry regulation in Australia, and the models used to regulate other parts of the information and communications industries. This Chapter also includes discussion of recommendations made for regulation of Bulletin Board Systems, a precursor to the internet as it is now commonly known. These chapters form Part One of the thesis, and are intended to situate the scheme for internet content control and the *Online Services Act* within the context existing at the time of its formulation.

Part Two of the thesis looks in detail at the *Online Services Act,* and the operation of the scheme for online content control. Chapter Seven discusses the introduction to Parliament of the Online Services Bill, the political environment, the enquiries conducted, and the *Act's* eventual passage, before looking at the provisions of the *Act* itself. The thesis then moves on to look at the operation of the scheme, commencing in Chapter Eight with the drafting and registration of the Internet Industry Codes of Practice. Chapter Nine examines the regime established under the *Act* to receive complaints about prohibited internet content, and discusses the operations of this complaints process. Chapter Ten deals with community education, a part of the scheme concerned not with the regulation of content, but with assisting the community to understand the dangers of the internet, and to learn strategies to better protect themselves, and those in their care, from exposure to inappropriate internet content. Chapter Eleven looks at State and Territory legislative provisions relating to internet content. While such provisions are not directly part of the *Online Services Act,* they were acknowledged as a mainstay of the federal internet content regime, and as a necessary adjunct to the *Online Services Act* itself. Finally, Chapter Twelve looks at data from studies on the topic, and submissions made to the Review of the *Online Services Act,* which shed light on the perceptions a number of key participants have of the *Act* and the scheme more broadly. This Chapter also examines the findings of the Review.

Part Three of the thesis attempts to evaluate the effects of the content control scheme and the *Online Service Act.* Chapter Thirteen measures the effects of the *Act* against its own stated aims. The thesis then moves on to look at relevant overseas efforts in content control, and to see whether the Australian scheme has

influenced overseas practice (Chapter Fourteen). On the basis of Australian and overseas experiences, Chapter Fifteen then suggests changes which may improve the Australian scheme. While it is clear that there is no way to 'fix the problem' of internet content control, there are a number of possible approaches which may minimize the impact of problematic internet content, without overly burdening internet users or the internet industry. Chapter Sixteen concludes that the *Online Services Act* has been nowhere near as repressive, nor as burdensome to industry, as many anticipated prior to its enactment.[34] It appears also to have been largely ineffective in terms of achievement of its stated aims, although it may have been somewhat effective in addressing other, unstated objectives of the Government. The thesis concludes overall that Australia is probably neither world leader nor village idiot in the sphere of content control, but rather is just one more country trying to bring a new, amorphous and technically difficult medium into line with its existing regimes for industry regulation and content control.

It should be noted that this thesis confines itself to an examination of the Australian internet content control regime, and does not engage with arguments relating to the Australian censorship regime overall, the rights and wrongs of classification categories, and larger issues of government policy (or lack thereof) relating to telecommunications and new media generally. While each of these is related to the topic at hand, the Government chose to introduce its content control regime largely in isolation from these matters, and it is this content control regime which is the subject of this thesis.

The thesis is current to the 1st of June 2004. Since that date internet content control has once again become a source of conflict and debate, with press headlines talking of a 'Labor bid to block net porn'[35] in the lead up to the next federal election. While the thesis does not discuss these most recent

---

[34] Particular concerns of, for example, Electronic Frontiers Australia, and the Internet Industry Association.

[35] Emma-Kate Symons, 'Labor bid to block net porn,' *The Australian,* IT Section, (16 August 2004). While there has been something of a flurry in the press, no new policy has actually been announced. Rather, Labor is said to have shown a 'strong interest' in the Australia Institute's claims that ISP blocking of pornography is technically feasible, a claim the Australia Institute has based on the 2004 Report of the Review of the *Online Services Act.* This Report is discussed below in Chapter 12: Statistics and Perceptions.

developments, the author notes that the Australian scheme for internet content control may well become contentious again in the near future. It will be worth watching for resulting changes to the scheme and to policy on the topic.

CHAPTER TWO: THE INTERNET

No legislation is ever made in a vacuum; it is always dependent on context. A legislature's ability to enact new laws will depend on its domestic environment and powers, and often also on international developments. It will depend upon social, political, legal, historical, and in some cases technological factors.

In enacting the *Online Services Act*, it is clear that the ability of the Government to devise a scheme for internet content control was both informed, and limited, by all of these factors. The newness and uniqueness of the medium, the regulatory structures under which Australian industry operated, the existing classification and censorship scheme, the legal system, and overseas developments, all had a role in the government's decisions regarding internet content control and the *Online Services Act.*

To understand the debate surrounding regulation of the internet, it is necessary firstly to understand something of the internet itself. The design of the internet, the governance of the internet, the uniqueness of internet content, and the way it was produced and used, posed special challenges in terms of regulation. It is worthwhile looking firstly at these issues.

A. *History and design of the internetwork.*

For most Australians there was little awareness of the internet's gradual evolution, and of it slowly being adapted to more and more uses, until the 1990s. Although the early internet was being developed in the USA from the late 1960s, only spasmodic connections to it were made by Australians during the 1970s.[1] The early 1980s saw the first permanent email connection between Australia and the

[1] Roger Clarke, *Origins and Nature of the Internet in Australia* (2004) Principal, Xamax Consultancy Pty Ltd, Canberra <http://www.anu.edu.au/people/Roger.Clarke/II/OzI04.html > at 16 June 2004.

USA,[2] and the Australian Academic and Research Network (AARNET) commenced operation in 1990.[3] As the name suggests this network was mainly limited to research and academic uses, but it also carried a small amount of commercial traffic for organizations closely associated with research and the tertiary education sector.[4] However, it was not until after the development in 1993 of Mosaic, a World Wide Web browser which allowed one interface to be used on Macs, PCs and UNIX work stations,[5] that internet use amongst the general community boomed,[6] and commercial ISPs began to spring up in Australia.[7] In fact, numbers rose from virtually no commercial ISPs in 1993, to an estimated 130 or more by the end of 1995.[8] While nearly all traffic prior to 1993 had been AARNET related, by 1995 Australian use of the internet by non-AARNET users already accounted for about 20% of total traffic.[9]

The seemingly sudden growth of the internet belies an understanding however of the internet's real history, which is important in understanding the discussion and debate which has surrounded the regulation of internet content. While the internet and World Wide Web burst onto the Australian scene in a user-friendly form in the early 1990s, development work to this point had been enormous. The initial ideas which led finally to the internet as we now know it were developed in the

---

[2] Ibid.

[3] Ibid, and see also ASTEC (Australian Science and Technology Council), *The Networked Nation* (1994) 13, and Robert Hobbes Zakon, *'Hobbes' Internet Timeline* (1993-2004), Zakon Group LLC <http://www.zakon.org/robert/internet/timeline> at 16 June 2004.

[4] *A history of AARnet*, accessed at AARnet site <http://www.aarnet.edu.au/about/history.html> at 17 June 2004.

[5] Clarke, above n 1, and Zakon, above n 3.

[6] In 1993, with the release of Mosaic, World Wide Web traffic had an annual growth rate of 341,634%! Zakon, above n 3.

[7] According to Roger Clarke, Australia's first formal commercial ISP (connect.com.au) operated from May 1994. Note that there are many arguments about when and who was in fact the first ISP in Australia, which follow from arguments relating to what an ISP is. A number of organisations earlier ran 'store and forward operations' to support applications such as FIDO and bulletin board systems, and some may also have provided 'connectivity' via dial up connections. However, the first Value Added Reseller program was introduced by AARnet in 1994, with connect.com.au being the first organisation registered as a value added reseller. Clarke, above n 1. According to Australian Broadcasting Authority, *Investigation into the Content of Online Services, Issues Paper*, (Dec 1995) 14, there were 'less than a dozen 'organisations offering on-line services in Australia' at the end of 1993, which had grown to 'an estimated "more than 130" by December 1995.'

[8] Australian Broadcasting Authority, *Investigation into the Content of Online Services, Issues Paper*, (Dec 1995) 14. According to AARnet the 2 commercial ISPs in 1992 grew to over 300 by June 1995 *A history of AARnet*, above n 4.

[9] *A history of AARnet*, above n 4.

early 1960s by a number of researchers, working together and apart, working for government and the private sector, and working in both the USA and the UK. The internet was not the brain child of an individual, nor did its development rest upon a single motivation.[10]

For some of the internet pioneers the motivation was military; [11] a desire 'to develop a military research network which could survive a nuclear strike, decentralized so that if particular US cities were attacked, the military could still have control of nuclear arms for a counter-attack.'[12] On the other hand, the Department of Defense's Advanced Research Projects Agency (ARPA) which commissioned the building of the initial network, was said to have developed the network in a 'climate of pure research...'[13] But it was the combination of both which led to the internet's development. 'The project reflected the command economy of military procurement, where specialized performance is everything and money is no object, and the research ethos of the university, where experimental interest and technical elegance take precedence over commercial application.'[14] The individuals involved also had varying motivations. Some wished to develop computers to a point where they would be seen not simply as the machinery to perform arithmetic calculations, but rather as partners which could assist humans to solve problems and develop ideas.[15] Others were interested for example in the networking side of things; how computers could be made to interact with one another.[16] But far from an individual design or motivation, the ideas of many people with differing motivations and varied emphases came together in the ARPANET, the forerunner of what we now know as the internet.[17]

---

[10] For an excellent discussion of pre-internet developments see Katie Hafner and Matthew Lyon, *Where Wizards Stay up Late: The Origins of the Internet* (1996).

[11] Paul Baran for example 'had developed an interest in the survivability of communications systems under nuclear attack. He was motivated primarily by the hovering tensions of the cold war, not the engineering challenges involved.' Hafner and Lyon, Ibid 11.

[12] Dave Kristula, *The History of the Internet* (1997) <http://www.davesite.com/webstation/net-history.shtml> at 17 June 2004, and see Janet Abbate, *Inventing the Internet* (1999) Ch 1.

[13] Michael Hauben, *The "Open" History of the ARPANET / Internet.* <http://www.dei.isep.ipp.pt/docs/arpa.html> at 17 June 2004

[14] Abbate, above n 12, 145.

[15] For example JCR Licklider. Hafner and Lyon, above n 10, 33-35, and Hauben, above n 13.

[16] For example Larry Roberts & Donald Davies. Hafner and Lyon, above n 10, Ch 2.

[17] BM Leiner, VG Cerf, DD Clark, RE Kahn, L Kleinrock, DC Lynch, J Postel, LG Roberts, S Wolff, *A Brief History of the Internet.* <http://www.isoc.org/internet/history/brief.shtml> at 26/7/2004

It may be that the military goals of networking - that is the need for security of information and an ability to overcome outages – led to its major design features; packet switching and a distributed network. However, it appears that individual scientists working both with and without military motivations both came up with roughly the same ideas for such a network, although developing their ideas in ignorance of one another.[18] Thus, at least some of the features of the internet which now ensure against interception and blockage undoubtedly suited military purposes, but were also the best way to build a stable, reliable computer network.[19] These features are highly relevant in any discussion of internet content control or censorship.

Firstly, to ensure that large messages or pieces of data did not tie up communications systems, a protocol was developed which did not involve all data in a message traveling together. While a whole message was readable when it reached its final destination, during transmission through the network the data was broken into packets (internet protocol (IP) packets).[20] Whole messages were sent and received, but during transfer only disjointed parts of messages could be accessed. Individual packets could also travel independently of one another, taking many different routes to the same destination so that the chance of losing or intercepting the whole of any message was remote. A checksum was attached to messages, to ensure that the whole of a message was received, and to allow re-sending of any part which had not reached its destination.[21]

Secondly, to ensure that messages did reach their intended destinations, the transfer protocol which was developed involved the ability for messages to route and re-route until they reached their addressee. Rather than traveling the shortest possible route, packets would be sent where there was capacity to carry them, and

[18] Paul Baran in USA, and Donald Davies in UK. Hafner and Lyon, above n 10, Ch 2.
[19] "Baran's system had many elements that were specifically adapted to the Cold War threat, including very high levels of redundancy, location of nodes away from population centres, , and integration of cryptographic possibilities... None of these features were adopted by Davies or Roberts, neither of whom was concerned with survivability." Abbate, above n 12, 39.
[20] Ed Krol, *The Whole Internet: User's Guide & Catalog* (Academic ed 1996) 28-30.
[21] Ibid, and see McCrea, Smart and Andrews, CSIRO, *Blocking Content on the Internet: A Technical Perspective* (June 1998) 11-13.

good connections. If one part of a network was damaged or destroyed, a message could travel another route and another route and another route until reaching its final destination. A malfunction in some part of the network would not stop a message reaching its destination so long as there were functioning parts of the network capable of carrying the data.[22]

From the original ARPANET the internet grew, but not as a single, nor even an integrated, development. Rather, the understanding of networking, and the practical demonstration of it, allowed and encouraged the growth of other computer networks. By the early 1980s very many networks had developed both in the USA and overseas.[23] The growth was not confined to government nor even scientific communities, and numerous networks were being set up for commercial, community, and other applications. In fact, the explosive growth of the internet in the late 1980s has been attributed not to the expansion of ARPANET itself, but to the number of networks connecting to it.[24]

Although the internet as we now know it was very much developed and trialed in the USA, during the 1970s other countries were also beginning to introduce internetworking capabilities, based on the knowledge and technical protocols developed in the experimental ARPANET. In the United Kingdom JANET, or the Joint Academic Network, had provided the academic community with networking services since 1979.[25] Canada too had introduced a network for the advancement of Research, Industry and Education, known as CANARIE.[26] Australia had a number of research networks, starting in the mid 1970s with CSIRONET, before AARNET, the Australian Academic Research Network, began in 1990, with the help of funding from the Australian Research Council.[27] These and other networks were linked internationally also, allowing the development of what is now known globally as the internet.

---

[22] Krol, above n 20, 15.
[23] Neil Randall, *The Soul of the Internet ; Net Gods, Netizens, and the Wiring of the World* (1997) especially Ch 6 and 7.
[24] Abbate, above note 12, 186.
[25] ASTEC above n 3, 11
[26] Ibid.
[27] Ibid 13-17.

Although these networks existed, it was not until the development of the World Wide Web that internet use became popular, and wide-spread amongst the broader community. Prior to the World Wide Web, those with internet access had been able to use the network to gather information if they knew what that information was and where it was stored. Gradual developments made this slightly easier, when programs such as Gopher and WAIS introduced searchable indexes, and allowed files to be found based on content rather than location.[28]

But it was not until the invention of the World Wide Web, followed by a user friendly web browser, Mosaic, in 1993,[29] that internet use exploded.[30]

> The Web would fundamentally change the internet, not by expanding its infrastructure or underlying protocols, but by providing an application which would lure millions of new users. The Web also changed people's perception of the internet. Instead of being seen as a research tool or even a conduit for messages between people, the network took on new roles as an entertainment medium, a shop window, and a vehicle for presenting one's persona to the world.[31]

In April 1993 there were 62 web servers in existence, by May 1994 there were 1298.[32] Web site numbers increased from 130 in June 1993 to 2,738 in June 1994, 23,500 by June 1995, and an estimated 230,000 in June 1996.[33] In 1994 the Australian Vice-Chancellors Committee also introduced an open access policy for use of AARnet.[34] Spurring and spurred by a great growth in ISP numbers, Australians were now able to access the internet readily, and in a user-friendly, easy to navigate form.

---

[28] Abbate, above note 12, 213.
[29] Tim Berners-Lee, *Weaving the Web* (1999) 69.
[30] Ibid 80. 'In March 1993 Web connections had accounted for only 0.1% of Internet traffic. This had risen to 1% by September, and 2.5% by December. Such growth was unprecedented in Internet Circles.'
[31] Abbate, above n 12, 213-214.
[32] Ibid 217.
[33] *Web Growth Summary* (1996), accessed at <http://www.mit.edu/people/mkgray/net/web-growth-summary.html> at 17 June 2004.
[34] ASTEC, above n 3, 13.

B. *Governance*

A most important factor limiting internet regulation is the absence of a central governing body, or national governmental control. 'What is unique about the internet is not that it is ungoverned; it is that its regulation has emerged from the bottom up and not the top down.'[35] Early development of internet standards and protocols was generally the result of 'rough consensus' amongst members of various bodies. The bodies were open to anyone interested, and anyone could put forward proposals and air their ideas.[36] While the Internet is not governed by any nation, nor by any single entity, a number of bodies take responsibility for its development and administration.[37] The fact that no single body governs internet development and administration does not however mean that the internet itself is anarchic or chaotic. In technical terms the internet is in fact highly organized and structured, and there are a great many bodies involved in its administration and development.[38]

Firstly there is the Internet Society (ISOC) whose mission is 'to ensure the open development, evolution and use of the internet for the benefit of all people throughout the world.'[39] This body appoints the Internet Architecture Board (IAB) responsible for architectural oversight of Internet Engineering Task Force (IETF) activities, and for oversight of and appeals from internet standards processes.[40] The IETF is a volunteer group which meets regularly to discuss operational and near-term technical problems,[41] and it includes 'network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.'[42] Smaller working parties of this group are sometimes established, which produce reports and make recommendations for

---

[35] Edward McBride, 'Regulating the Internet: The Consensus Machine,' *The Economist*, 10-16 June 2000, 77.
[36] Ibid.
[37] A Froomkin, 'An Introduction to the "governance" of the internet: Towards a critical theory of cyberspace.' Extracted in B Fitzgerald & A Fitzgerald, *Cyberlaw* (2002) 94 - 97.
[38] M Capore, 'The Self-governing Internet: Coordination by Design.' Extracted in Fitzgerald & Fitzgerald, above n 37, 94.
[39] Internet Society, *Mission Statement* <http://www.isoc.org/isoc/mission/> at 17 June 2004.
[40] Internet Architecture Board home page <http://www.iab.org/> at 17 June 2004.
[41] Internet Engineering Task Force home page <http://www.ietf.org/overview.html> at 17 June 2004
[42] Ibid.

solutions to particular problems. There is also the World Wide Web Consortium (W3C) which specifies web standards,[43] and the Internet Corporation for Assigned Names and Numbers (ICANN), which is an 'internationally organized, non-profit corporation [with] responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic and country code Top-Level Domain name system management, and root server system management functions.'[44]

In addition to the plethora of bodies involved in internet governance and development, the internet lacks 'ownership' in a controllable sense. Computers are owned by individuals, governments, corporations, schools etc, and linked to networks. These networks link to other networks to form an internetwork. It is not ownership, but the use of particular protocols and links which allow these networks to join the larger internetwork. This lack of ownership creates further difficulty for those wishing to assert control over the internet.

C. *Jurisdiction*

Another feature militating against easy control is what has been termed the 'seamless' nature of the world wide web. This refers to the ability of those using the web to send and receive content to and from sites located anywhere in the world, without knowledge of that site's location.[45] There is no wait to access a site in another country, there is no customs stop, no visible sign at all. A site across the globe can be accessed as quickly as a site across the road. Internet surfers can move around the world without even being aware that they are doing so.

Because it is irrelevant on the net where content is housed or stored, stopping the hosting of material in one jurisdiction may not stop access to the material even

---

[43] World Wide Web Consortium home page <http://www.w3.org/>. For an interesting view of the early W3C see Berners-Lee, above n 29, Ch 8 and 9.
[44] ICANN home Page, *ICANN information* <http://www.icann.org/general/> and see Mcbride, above n 35.
[45] UNESCO, *The Internet and some international regulatory issues relating to content.* (September 1997) 12.

within that jurisdiction. Content initially hosted in one jurisdiction will often be copied or 'mirrored'[46] on a site in another jurisdiction, so that even when content is removed from one site in one jurisdiction, it will still be accessible to users in the first jurisdiction.[47] For internet users, it is irrelevant whether or not the site they access is local; the availability of the information is the same either way.

While the Australian Government clearly had jurisdiction over users, ISPs, ICHs and content providers in Australia, it had no jurisdiction over those located overseas. Thus in choosing a regulatory scheme it needed to take account of the fact that internet content outside Australia may be readily available within Australia, even when the content was prohibited here. These jurisdictional issues placed serious limits on the ability of one government effectively to control content within its own territory.

D. *Technology.*

Many technical factors have been referred to above in the discussion of the development of the internet. Internet protocols involving packet switching and a distributed network are important in ensuring that information can be transmitted and received regardless of disruption to the system. Just as important however is the type of content which this new technology makes possible. Pre-internet technologies allowed a diverse range of media, such as text, video, audio, graphics, film, and many distribution channels such as print, radio, free to air, cable TV, etc. Current technology allows all these media to be transmitted via the internet, and moreover, it allows amalgamation and integration of many of these.[48] In terms of internet censorship this technological wizardry is extremely important. It raises questions, for example, of whether an amalgamation of various forms of media is a new form of media, requiring new ideas and new, different, and

---

[46] McCrea, Smart and Andrews, CSIRO, above n 21, 16-17.
[47] Jon Casimir, *A Boy and His Mouse; More Postcards from the Net* (1997) 159.
[48] Australian Broadcasting Authority, *Investigation into the Content of Online Services, Report to the Minister for Communications & the Arts* (1996) 36-38, and McCrea, Smart and Andrews, CSIRO above n 21, 9.

specifically focused censorship regimes, or whether the new forms of media can appropriately be equated with pre-existing forms of media. There is nothing in the technology to tell us the answer; technically these new forms of material could be characterised as the same as or different from those previously known. Thus judgment about characterising internet material needs to be made on bases other than technical.

Further, an 'Internet user requires a PC, a modem, and a contract with an ISP to connect to the Internet.'[49] While radio or television transmissions, and even print, require specialised and expensive equipment, making content available on the net is simple and cheap, and it is easy to move around both the content and the means of transmission. These factors create particular difficulties for those seeking to regulate internet content.

E. *Social Aspects of the Internet*

The internet has social aspects which are not seen in any other medium. While these social aspects were not decisive of what could or could not be done to regulate the internet, they were certainly relevant to argument surrounding that regulation. The real involvement of many people with the internet, not simply as a medium but as a way of life, heightened the willingness of many to fight against internet regulation, and thus heightened the level of conflict in which the legislation was drafted and enacted.

The internet has been described as 'potentially the most empowering, the most enlightening, the most liberating tool for individual self-realisation, as well as for democratisation.'[50] By 'allowing anyone to participate, online services are, after

[49] McCrea, Smart and Andrews, CSIRO, above n 21, 14.
[50] Nadine Strossen, President of American Council for Civil Liberties, quoted in 'Australia urged to repeal law', *Sydney Morning Herald* (Business section), 24 August 1999.

speech itself, the most free and democratic form of human communication yet devised...These services constitute a new form of human interaction...'[51]

Many early users of the internet thought of it as 'a place where borders were not to be boundaries; access was to be open and free; people could enter and engage without revealing who they were ...Its essence was captured in the irreverence of a mouse: With a click one could flash just about anywhere. The very design of cyberspace was (in the period of its infancy) in contrast to the world that had constructed it.'[52] Because of these unique features, many users feared *any* restriction of the medium.[53]

There are many factors which make the net special, and socially different from any other medium. Firstly there is the ability of the net to overcome the isolation of an individual. Many people would think that meeting and interacting with someone they do not know, can not see and are never likely to meet would be a boring and somewhat weird pastime, but for those who may have been long isolated such is not the case. Net users report a great sense of connection brought about by their ability to make contact through the web with people they would not meet in real life. And this is not confined to computer 'nerds and geeks' meeting up with other 'nerds and geeks;' it appears to be a far broader phenomenon which covers countless instances of those isolated in their own communities.[54]

Secondly, the net allows meetings to occur across geographical borders, and across distances both large and small. It may allow for example those isolated in a school environment to contact similar students in other schools, and those isolated in their broader communities to meet those outside. And conversely, the net

---

[51] Australian Broadcasting Authority, above n 48, 59; quoting from the submission of Gillian Appleton.
[52] Lawrence Lessig, 'Reading the Constitution in Cyberspace.' (1996) 45(3) *Emory Law Journal* 869, 887.
[53] 'Socially, the fundamental purpose of the Internet is the sharing of information, so censorship is nothing less than a crime - or, when carried out by a government, an act of war. Censorship on the scale proposed will, quite literally, start a war - with the Australian government on one side and the Net's hackers, cypherpunks, and civil libertarians on the other.' Danny Yee, 'Internet Censorship.' Speech delivered to Aussie.ISP 8th April 1999 found at <http://danny.oz.au/freedom/AISP.html> at 21 June 2004.
[54] M Hauben & R Hauben, *Netizens, On the History and Impact of Usenet and the Internet* (1997).

allows next-door neighbours to meet up, even with no knowledge of one another's physical proximity. It is a place where common interests and common needs can bring people together, rather than geography, community or introductions.[55] Further, the speed with which material can travel on the net greatly increases opportunities for interactivity, and is another factor making the net socially unique. The ability to exchange information in 'real time' with someone across the world, or indeed with many people in many parts of the world, cheaply, is a new and powerful phenomenon.

This interactivity is significant in making the net both popular and unique. A huge amount of information is on the net, but a huge amount of information was already available on TV, in newspapers, films and magazines. On the net however, recipients of information are not solely recipients; they can be participants also. The net allows people to interact with the material they access, to reply to others, to put up material of their own. The net allows information to move in many directions, no longer just outward from providers to recipients.

Another factor unique to the web and its social life is the ability of participants or net users to remain both anonymous and 'bodyless'. 'On the internet, the old joke goes, no-one knows you're a dog.'[56] Net participants are not tied in any way to their 'real life' personas; they can be who they will when they will. They can change views, change agendas, even change genders, without the constraints imposed by the physical world. 'We are all anonymous online, disembodied voices wrapped in whatever personalities we choose. There are no rules to follow in the creation of our virtual persona, no boundaries or restrictions.'[57]

The breadth of content available is another factor unique to the internet, described by Justice Dalzell in the US District Court as 'the most participatory form of mass speech yet developed ... it is no exaggeration to conclude that content on the

---

[55] Ibid.
[56] From cartoon by Peter Steiner published in The New Yorker 5/7/1993, referred to in Casimir, above n 47, 202.
[57] Casimir, above n 47.

internet is as diverse as human thought.'[58] The net allows those from non-mainstream groups to voice their ideas and concerns and to discuss them with others. Many people would not share ideas in a society where they feel their ideas are unfashionable, unpopular, or politically incorrect, but the net allows a forum for discussion of unpopular or minority views. While this may encourage or at least allow the development of anti-social viewpoints, it also gives an opportunity to discuss ideas that are not so much anti-social, as reflective of minority interests.

Tied to all this is the ability of those using the net to have a say in what information is available in the public domain. The net empowers users to *make* news, or to be a source of information in one's own right, rather than a passive recipient of information, or 'subject' of news. While newspapers, radio, magazines and television are the main sources of information, through them it can be difficult to disseminate unpopular or minority views. When unpopular views *are* reported in the mainstream media, they are often accompanied by journalistic derision and negative editorialising.

The net on the other hand allows individuals to decide not only to publish information, but to decide how that information should be presented, when it should be made available, and whether it should be linked to other information. Not only can those providing the information have a say in its publication, but recipient internet users now have alternative and less 'establishment' sources of information. 'The top down model of information being distributed by a few for mass consumption is no longer the only news. ... People now have the ability to broadcast their observations or questions around the world and have other people respond.'[59] 'The common people have a unique voice that is now being aired in a new way.'[60]

An excellent local example of the power of the net as a news source can be found in the publication of a story about an assisted suicide in the Northern Territory. By

---

[58] *ACLU v Reno*, 929 F Supp. 824, 835 842; quoted in *Reno v ACLU* 117 S Ct 2329, 2340 2335 (1997)
[59] Hauben & Hauben, above n 54, 4.
[60] Ibid 10.

publishing information about the death only on the internet, the doctor involved ensured that 'the net-connected part of the public could read exactly what he wanted it to read, instead of a filtered or edited version... The media is no longer just something that is done to him; it is something he *does*.'[61]

F. *Conclusions.*

The technology of the internet, the lack of centralised or national control, the opportunity for social empowerment, and the uniqueness of the medium, all featured in arguments relating both to what could and could not be done, and to what should or should not be done. Thus even where the Government claimed only to be bringing the internet into line with other media, it was argued that the internet could not and should not be treated like other media. This in itself raised the profile of the proposed scheme, increased the level of opposition, and forced the government to act in a context of heightened conflict.

Moreover, to regulate the content available on the internet, the Australian Government needed to establish a regulatory framework capable of dealing with many factors which had not previously been within its regulatory knowledge or competence. In doing so, the Government needed to take account of the features of the internet discussed above, the methods available for its regulation, the censorship and regulation of content in other media in Australia; internet content regulation in place in other countries; and the regulatory frameworks already in place in similar industries in Australia. Each of these will be discussed in the following chapters.

[61] Casimir, above n 47, 81-83.

CHAPTER THREE: METHODS OF INTERNET CONTENT CONTROL

By 1999 the internet was highly developed technologically, readily accessible in Australia, heavily used, and brimming with content of all types. It was the availability of that content which concerned the Australian Government. While many nations were interested in controlling internet content[1] no one method had shown itself to be particularly effective or appropriate for controlling access to content in a democratic society. This chapter examines the possibilities for internet content regulation existing prior to the enactment of the *Online Services Act*. It should be noted that this chapter, and this thesis generally, refer to the control of web based internet content, and not to all content distributed or accessed via the internet.

A. *Internet content control generally.*

It is necessary firstly to distinguish degree of control, location of control, and methods of control. 'Degree of control' refers here to the amount of control desired or achieved. 'Location of control' refers to where that control will be asserted, while 'method of control' refers to the way in which the control will be carried out. Of course these factors overlap and intertwine. For example, the degree of control or location of control will be influenced by available methods of control; the choice of location of control will depend on the desired degree of control and so forth. However, it is worth looking at the three separately to help clarify the options available to the Australian Government prior to the enactment of the *Online Services Act*.

1. Degrees of control.

A government may wish totally to control its citizens' access to content, may not wish to control it at all, may wish to control access to some content only, or may wish to control access for some citizens only. It may wish only to improve

[1] Discussed in more detail in Chapter Four: Overseas content control prior to the *Online Services Act*.

controls available to users themselves. Where total control is desired, in an extreme case a government may stop its citizens from accessing computers, or stop its citizens from accessing the internet.[2] Where these methods are not an option, a government may still exert a high degree of control over access to internet content, for example by allowing access to approved content only. In this case, content may be provided and hosted locally, subject to approval only, and foreign content may also be accessible, again subject to approval. Criteria for approval may be broad or narrow, depending on the aims of the regulation. This may be referred to as a closed or controlled environment, where internet content is not available unless approved.

Lesser control may also be achieved using the opposite approach, whereby access to all internet content is available, unless the content is excluded or blocked. There may be attempts to exclude some content entirely, or to exclude certain content for some users and not for others. The approach taken at this initial phase will significantly alter the degree of control possible over internet content.

It must be remembered also that control over access to internet content will not necessarily come from a central government. Control may be exercised not only upon citizens but by them also. Government may for example mandate systems whereby users have greater control over their own selection of content, where ISPs offer differentiated services, where content providers label their content, where service providers such as schools or libraries must or may control content to which they provide access. Furthermore, demands for such control may not come from government at all; user needs and thus market demand may for example result in the development of filters to operate at user level, in the labeling of content, in ISPs offering differentiated or 'family friendly' services, or in libraries offering access to controlled environments only.

[2] Countries for example such as Myanmar or Cuba, discussed further in Chapter Four: Overseas content control prior to the *Online Services Act*.

2. Location of control.

Location of control refers to the actual location at which control will occur, and there are a variety of points which may be used to achieve greater or lesser degrees of control. For example, foreign-hosted internet content may be blocked or approved at a national gateway, at ISP level, by third party proxy servers, or at user level. The higher the point of control, the more uniform the regulation will be, and the greater control can be achieved. For local content, restrictions could occur again at ISP or proxy server lever, and / or at content provider or host level. Published criteria could define for providers and hosts content which may or may not be hosted, or content may even require approval prior to hosting.

In addition to these points of control, control may be exerted over users of the internet themselves, and other providers of internet access such as internet café proprietors, libraries, schools, universities, and workplaces. A combination of points of control is likely to achieve the greatest control; top level pre-approval ensuring as far as possible that only approved content is available, and restrictions at lower levels and upon individuals to discourage circumvention of these controls.

Controls exercised at gateways, ISPs or proxy servers are often referred to as 'upstream' controls, while those closest to users are referred to as 'downstream' controls. While controls located higher in the chain, or further upstream, would give greater control and more uniformity, the converse is also true. The lower the location of control, or the more downstream it is, the more control can be tailored to suit the user. Filtering at ISP level for example may be set to specific criteria for 'families,' while at the user lever the filtering may be set to reflect the wishes of the individual family using it.

3. Method of control.

It is necessary to distinguish human methods of control from automated methods of control. Human control involves persons checking internet content to decide whether the content meets criteria for inclusion or hosting, or for exclusion. This can be done prior to content being made available on the internet, or when content

is requested, or simply by selection of suitable content. If done in response to requests a human may actually allow or refuse access to the content requested, but more often human checking is used as a way of compiling lists of content to be included (white-lists) or excluded (black-lists), which is then carried out using automated methods. Labeling of content to identify category or type of content may also be done by humans; possibly a content provider, host, government body, or other organization set up for the purpose.[3]

Computer software (filters) can be programmed to allow access only to content contained on a white-list, to allow access to any content not contained in a black-list, or to allow or reject access to content carrying specified labels or tags. This filtering can occur at any location, from national gateway to ISP, proxy, or user. Additionally, filters based on an exclusionary approach may combine the use of black-lists with a number of other methods of exclusion.

Zoning is another method of enabling automated control of internet content. Zoning requires sites or users to be identified in terms of content hosted, user credentials etc, and either sites themselves, or user's filters, would use this information as a basis for allowing or denying access. The advantages and disadvantages of filtering, labeling, and zoning are discussed below.

B. *Filtering*

Many commercial filter products were already available prior to the enactment of the *Online Services Act*, and many were known by this time to have serious flaws.[4] The following section discusses the methods used to filter access to

[3] Labeling is discussed in more depth below, this Chapter.

[4] Studies had repeatedly shown serious flaws in content filters. Cyber-Rights and Cyber-Liberties (UK) Reports, 'Who Watches the Watchmen: Internet Content Rating Systems and Privatised Censorship' Nov 1997, 'Who Watches the Watchmen Part II – Accountability and Effective Self-Regulation in the Information Age' Sept 1998, Electronic Privacy Information Centre, 'Faulty Filters, How content filters block access to Kid-Friendly information on the Internet' Dec 1997, along with Peacefire's analysis of CyberSitter, Smart Gear, I filter, X-Stop, NetNanny, WebSense, Cyber Patrol and Bess, and the EFA's report on Clairview Internet Sheriff, were all available and well publicised prior to the enactment of the *Online Services Act.*

internet content, and gives examples of some of the problems seen in the use of different techniques. References in this section are drawn from the period prior to the *Online Services Act,* and from more recent reports on filtering products, to illustrate both that the problems were apparent prior to the government's introduction of the *Act*, and that the problems continued.

1. White-lists, inclusion filtering, or controlled environments.

White-lists are lists of internet addresses which do not contain offending material. They allow automated inclusion filtering, whereby a filter denies access to any but the listed addresses, rather than excluding offending sites. The use of filtering by inclusion or white-lists creates for a user a controlled or closed environment.

White-lists need to be compiled by humans, as there is no other sufficiently reliable method of ensuring that inappropriate material is not accessible. While filters based on properly compiled 'white' or inclusion lists will thus be highly reliable in ensuring that users see only non-objectionable material, a major drawback with the use of inclusion or white-lists is the paucity of material to which a user will have access. For example, in February 1999, while the *Online Services Act* was being drafted, the publicly indexable web was estimated to contain about 800 million pages.[5] At the same time a well-known publicly available inclusion list, Yahooligans, included only about 3000 web addresses, a tiny proportion of the internet proper.[6] Because most material on the internet *will not* be objectionable, one would expect a reasonably comprehensive inclusion list would contain some millions of sites. However, given the size and growth of the internet,[7] and the need to check sites individually for inclusion, it is unlikely that an inclusion list sufficiently broad for general use could ever be compiled.

This was recognized prior to the enactment of the *Online Services Act,* with the ABA reporting that 'maintenance of the quality and appropriateness of material

---

[5] P Greenfield, P McRea, S Ran, CSIRO, *Access Prevention Techniques for Internet Content Filtering* (December 1999) 6, prepared for the National Office of the Information Economy.
[6] Ibid.
[7] By January 1997 there were already an estimated 650,000 web sites available. Matthew Gray, *Web Growth Summary* <http://mit.edu/people/mkgray/net/web-growth-summary.html> at June 20 2004.

... was seen as a practical difficulty in the implementation of a controlled environment. However, the major drawback was the danger of so limiting the available material that its educational or other usefulness was significantly diminished.'[8] While the use of white-list filtering may be appropriate for small children to whom quantity of information is unimportant, white-list filtering is unlikely to be appropriate for anyone else. When one of the biggest attractions of the internet for older children and adults is the ability to connect widely with many people, and to gather a breadth of information from anywhere in the world on any given topic, white-lists stymie much of this attraction.

2. Black-lists and exclusion filtering.

Exclusion filtering allows access to any content unless it is excluded. It may be excluded by being placed on a black-list, a list of addresses from which content will not be retrieved. Such lists may be generated by people checking content randomly, or in response to complaints or concerns; may be generated automatically; or may be generated by a combination of these means. Filters using black-lists may rely on filtering by universal resource locator (URL) or packet filtering. Packet filtering relies on routers, which steer material from place to place, blocking 'packets' (a piece of information) which originate at prohibited IP (internet protocol) addresses.[9] An IP address specifies a particular computer, so that blocking in this way blocks anything coming from a particular computer, although that computer may of course host material both offensive and inoffensive. It is a particularly coarse method of filtering.[10] URL filtering on the other hand allows for more specific blocking. Rather than blocking everything which originates in a given computer, it reads the address of specific content (the URL) and can therefore filter more carefully, differentiating right down to individual pages.[11] However, the more specific the filtering, the more addresses will need to be included in the filters, and so the system may become unwieldy.

---

[8] Australian Broadcasting Authority, *Investigation into the Content of Online Services, Report to the Minister for Communications & the Arts* (1996) 35, 160.

[9] P McRae, B Smart & M Andrews, CSIRO, *Blocking Content on the Internet: A Technical Perspective* (June 1998) 6-7 and part 5, 32-38, prepared for the National Office of the Information Economy.

[10] Greenfield, McRea, Ran, above n 5, 7

[11] Ibid 7-8.

Furthermore, as internet material is frequently reorganized and relocated, it is a mammoth task to keep such URL lists current.[12]

Instead of, or more often in addition to, the initial exclusion of black-listed content, filters may examine content requested or retrieved and measure it against further criteria before it is allowed or rejected. There are a number of techniques used in filters for this purpose. Keyword filtering automatically measures requests sent or content loading against a list of prohibited words. Requests containing such words will not be sent, retrieved material containing these words will not be displayed.[13] Keyword filtering can block material containing individual prohibited words or combinations or strings of such words.

Profile filtering looks at the 'characteristics' of the content received by a computer, characteristics such as the ratio of pictures to text in requested material. A considerable amount of content needs to be received to enable a profile check as this filtering is done on the receiver's computer, and that material may be displayed on the monitor in the meantime.[14] Another method is image analysis filtering, which 'relies on techniques such as the detection of skin tone, or indeed on the analysis of images themselves.'[15] Like profile filtering, image analysis also requires material to be received before analysis and so may allow display of objectionable material.

Exclusion filtering using only black-lists is likely to be less reliable than white-list or inclusion filtering, as 'unrated sites are presumed to be innocent,' and access to all sites is therefore allowed unless they are excluded.[16] Thus where white-lists tend to under-include, black-lists tend to under-exclude. Black-lists used in combination with a variety of other filtering techniques may be more effective than black-lists alone in excluding problematic material, but all of these techniques of exclusion have flaws.

---

[12] Ibid.
[13] Ibid 7.
[14] Ibid 8.
[15] Ibid.
[16] Ibid 6.

3. Flaws in filters.

Exclusion or black-lists often involve blocking far too large for the problem at hand. 'Deja News' for example was entirely blocked by some filters, as some of its news groups carried offending material,[17] although many thousands did not. The job of identifying individual offending pages or even groups may be too large and can lead therefore to extremely broad-brush filtering. Some filter products add to this problem by giving users little choice. Net Nanny for example required users to employ the whole of its black-list, or none of it. Had the list been broken down into categories, users could have had much more say into their filtering; for example by setting the product to use some black-list categories but not others.[18]

The difficulty of monitoring sites for addition to or removal from black-lists leads to many filter providers using exclusion lists in combination with word, image or profile checking of material requested or received, but these techniques have their own problems.

There are countless examples of problems with keyword, word combination or word string filtering.[19] The White House web site was reportedly blocked by a filter responding to the word 'couple,'[20] while a high school student was unable to access his own school web site from his school library when a filter responded to the word 'high.'[21] In using word detection CyberSentinel blocked an entry page with the message '"This site contains no pornography. It contains no pictures of male or female genitals," presumably because the words pornography and genitals appeared on the screen.'[22] The blocking of breast cancer information through the filtering of the word 'breast' has been a commonly used example, but filter

---

[17] The Censorware Project, *Cyber Patrol and Deja News, Censorware product blocks an important research resource* (1998) < http://censorware.net/reports/dejanews/> at 4 August 2004.
[18] CSIRO, *Effectiveness of Internet Software Filtering Products* (Sept 2001).
[19] Greenfield, McRea, Ran, above n 5, 7.
[20] Australian Broadcasting Authority, above n 8, 152.
[21] Digital Freedom Network, *Foil the Filters Contest* (2000) <http://dfn.org/Alerts/contest.htm> at 10 October 2000 (this page no longer exists), but reference can be found at Open Source Roundtable <http://www.linuxdevcenter.com/pub/a/linux/2000/09/29/rt.html > at 1 August 2004.
[22] CSIRO, above n 18.

providers now claim that context is examined to some degree, by blocking offending words only when it is likely that they are used in an offending way.[23]

However, keyword filtering may be problematic even when combined with 'contextual' analysis. Filters blocking violent language are likely to filter out news reports, filters blocking sexually explicit language may well filter out censorship information.

> Software that uses keyword blocking to block the word "Nazi" will block out history sites about the Holocaust as well. Even the tools that work only when certain words appear together or near each other are likely to block out sites like the Simon Wiesenthal Center's page on the growth of hate groups online, or an article on white supremacist activity on the Southern Poverty Law Center site.[24]

Filters using image analysis techniques also have problems. In one product at least,[25] where skin tones appeared to be the primary trigger for denial of access, black and white nude photos escaped detection, while pictures with fleshy tones, even of faces or desert scenes, were wrongly classified as pornography, and rejected.[26]

The enormity of the work involved in compiling comprehensive black-lists, given the quantity of content on the internet, and the fluidity with which it may be moved, removed, adjusted or modified, coupled with the problems of automated filtering and blocking techniques, suggest that the use of filters to restrict access to content may be partially effective at best. These may not however be the worst of filterware's problems.

---

[23] Ovum, *Internet Content Filtering: A Report to DCITA.* (April 2003) 17.
[24] GetNetWise, *Tools for Families* <http://www.getnetwise.org/tools/index.php3?definition=blockhate> at 20 June 2004. For a review of a filter which uses key word and string blocking see for example Benet Hasselton, *Sites Blocked by Cyber Sentinel* <http://peacefire.org/censorware/Cyber_Sentinel/cyber-sentinel-blocked.html> at 20 June 2004.
[25] Eyeguard.
[26] CSIRO, above n 18, 55.

4. Non-technical flaws in filtering.

Prior to the enactment of the *Online Services Act*, Senator Stott-Despoja told the Senate: 'It is crucial that the operation of content control in a liberal democracy is open and accountable. We certainly need to ensure that the value systems and the decisions made in blocking content are explicit.'[27] Unfortunately, numerous examples suggested that commercially available filter products may not be sufficiently transparent.

(a) Bias

A significant problem with the use of filters for internet content regulation is the opportunity for bias within products. For commercial purposes the exclusion lists and filter techniques used by commercial filter products are often kept secret, and are highly protected. For example, when the 'CyberNot'[28] code was cracked and published, a law-suit ensued to stop dissemination of the information.[29] Thus those whose searches are subject to filtering may not know just what content is and is not being blocked. This need not matter if users are able to rely on filter providers to have the same understanding of filtering categories as the user does, and if filter makers can be relied upon to stick faithfully to those categories. Unfortunately, many examples show that these conditions do not exist.

America Online (AOL) for example provided a filter to protect children by restricting them to 'kids only' web sites. When used, children could access the web site of the Republican National Committee, but not of the Democratic National Committee; could see the web sites of the Conservative Party and Libertarian Party, but not of the Green Party or Reform Party.[30] AOL's 'young teens' filter, less restrictive than 'kids only,' allowed access to sites promoting gun use, but blocked gun safety organizations such as Coalition to Stop Gun

---

[27] Cth, *Parliamentary Debates*, Senate, 11 May 1999, 4743. Quoting from Democrat (minority) Report of Senate Select Committee on Information Technology, tabled 11 May 1999.

[28] Cyber Patrol's black-list.

[29] *Microsystems Software Inc and Mattel Inc v Scandanavia Online AB, Islandnet.com, Eddy L O Jansson, and Matthew Skala*, 98 F. Supp. 2d 74; 2000 U.S Dist (D. Mass. March. 28, 2000) For links to news articles and comments on the case see <http://www.politechbot.com/cyberpatrol/> at 20 June 2004.

[30] Brian Livingstone, *AOL's youth filters protect kids from Democrats* (2000) Wired Watchdog News.com < http://news.com.com/2010-1071-281304.html> 4 August 2004.

Violence.[31] According to a study which searched for over 100 sites over a number of days, AOL's filters repeatedly allowed the viewing of far more conservative sites than democratic or liberal sites, and these results were consistent throughout the testing period.[32]

Material on individual's web sites has been blocked by filters although the material was copied directly from large conservative websites not blocked by the same software. It has been suggested that filter makers may be hesitant to block the sites of large conservative groups as they are in fact market allies with similar goals. Large conservative organizations are those pushing hardest for the introduction of filtering software in homes, schools and libraries, and filter makers have a lot to lose, economically, by getting such organizations off-side.[33]

Further examples of bias can be seen in the blocking of the sites of Electronic Frontiers Australia (a non-profit national organisation formed to protect and promote the civil liberties of users and operators of computer based communications systems)[34] and Peacefire (created to represent the interests of people under 18 in the debate over freedom of speech on the Internet, a 'people for young people's freedom of speech' organization)[35] by a number of filter products. Peacefire's anti-censorware site was listed as offending every non reserved category of Cyber Patrol's 'CyberNot' list; it was blocked in the categories 'Violence / Profanity / Partial Nudity, Full Nudity, Sexual Acts / Text, Gross Depictions / Text, Intolerance, Satanic or Cult, Drugs / Drug Culture, Militant / Extremist, Sex Education, Questionable / Illegal & Gambling, Alcohol & Tobacco!'[36]

The web site of Electronic Frontiers Australia was blocked by Surf Watch as 'sexually explicit' although EFA's site did not contain any sexually explicit

---

[31] Ibid.
[32] Ibid.
[33] Declan McCulloch, *Filters Kowtowing to Hate* (27 May 2000) Wired News <http://www.wired.com/news/print/0,1294,36621,00.htm> at 20 June 2004.
[34] <http://www.efa.org.au/AboutEFA/Welcome.html#intro> at 20 June 2004.
[35] <http://peacefire.org/info/about-peacefire.shtml> at 20 June 2004.
[36] Eddy L O Jansson & Matthew Skala, *The Breaking of Cyber Patrol* <http://www.snark.freeserve.co.uk/censorware/cp4break.html> at 4 August 2004.

material.[37] It did however contain considerable criticism of filtering software. The web site of the South Australian division of the Liberal Party was also blocked by Surf Watch, after the South Australian Liberal Party Council resolved that 'the federal government should revoke its recently introduced Internet Censorship legislation as it is unworkable.'[38]

(b) Differing Standards

Many filter products specify the basis on which they filter, and some allow users to select for themselves which categories they would like to be able to access, and which should be unavailable.[39] Categories include things like violence, sex, offensive language, hate, crime etc. Problems may arise however from the fuzzy nature of the categories, and disagreement over boundaries.

Take, for example, a picture of a naked woman. Her body parts are labeled using scientific names. Take the same woman, take away the names, and add a black bra pushed up and black pants pushed down. Take the same women, painted by Reubens. Take the same woman lying on a bed reading the Wizard of Oz. Take the same woman lying on a bed reading PlayBoy. Which of these are inappropriate for children? Which are explicit? Which are too explicit? The appropriateness of nudity, sex, pornography etc has always been an area of dispute, with different individuals, different families, and different communities taking different perspectives.[40]

(c) Broad brush blocking

Filter providers need sometimes to make decisions about whether to possibly under-block or over-block internet content. The blocking of 'Deja news,' a huge archive of Usenet messages, and a serious research resource used by many professionals, illustrated this problem. A small portion of the text sought to be

---

[37] Electronic Frontiers Australia, 'Government Approved Net Filters Attempt to Silence Critics.' (press release, 29 June 2000)
[38] Ibid.
[39] CSIRO, above n 18, 6.
[40] Hate speech is another good example of the difficulty of categorization. It appears that some filter products classify particular content as hate depending not only on what is said, but on who is saying it. McCulloch, above n 33.

blocked by Cyber Patrol had sexual content, but to block this over 300 gigabytes of data, representing 250 million messages, was black-listed, or added to the 'CyberNot' list.[41] As many public libraries used the software, criticism of the blocking was huge. It was said that 'blocking library patrons from using Deja news because some of the newsgroups have sexual content is the equivalent of refusing to carry the Encyclopaedia Brittanica because some of the articles cover sexual topics.'[42] There have been at least two other similar occurrences of Cyber Patrol using extremely broad brush blocking; 50,000 pages in the West Hollywood pages of Geocities, and over a million pages at members.tripod.com. Both of these were unblocked after adverse publicity.[43]

Internet Sheriff has also been accused of similar over-blocking problems. It has been found to apply 'an exceptionally broad brush in deciding, not only what it deems pornographic, but also in blocking entire sites.'[44] Bess (sold as ifilter in Australia) has caused similar complaints; filter users can choose to ban all free homesite pages, or let them all through. Bess's makers say individual home pages are too difficult to monitor as their content changes so frequently, and therefore users must choose to allow all or nothing.[45]

(d) Errors

Honest errors may be of less concern than intentional bias, but high error rates may raise questions regarding the usefulness of filter products. In a study which involved de-crypting I-Gear's list of blocked sites, of the first fifty sites decrypted, twenty eight (56%) were found to be obvious errors, ten (20%) marginal errors, and twelve (24%) correctly blocked.[46] Even leaving aside marginal errors, the obvious error rate was clearly too high for the filter to be relied upon.

---

[41] The Censorware Project, above n 17.
[42] Ibid.
[43] Ibid.
[44] Electronic Frontiers Australia, *Report: Clairview Internet Sheriff, An Independent Review* (1999) <http://www.efa.org.au/Publish/report_isheriff.html> at 20 June 2004.
[45] The Censorware Project, *Passing Porn, Banning the Bible* (undated) <http://censorware.net/reports/bess/> at 27 July 2004.
[46] Peacefire, *IGDecode: I-Gear list codebreaker* <http://peacefire.org/censorware/I-Gear/igdecode/> at 20 June 2004.

A similar study was done using the Surf Watch filter. Working alphabetically, attempts were made to access the first thousand .com domains, using the Surf Watch filter set to exclude only 'Sexually Explicit' material. 147 of the first thousand were found to be blocked as sexually explicit, although 96 of those were pages 'under construction.' Of the remaining 51 blocked sites nine were sexually explicit, while 42 did not contain sexually explicit material and were blocked in error.[47]

In tests of hundreds of images the BAIR filter 'incorrectly blocked dozens of photographs including portraits, landscapes, animals and street scenes. It banned readers from viewing news photos at time.com and newsweek.com, but rated images of oral sex, group sex, and masturbation as acceptable for youngsters.'[48] I-Gear 3.5 seems also to have given bizarre results. With the filter set to block pornography / erotica about 98% of such content was blocked. However, when the filter was set to allow such content, more art / photography was allowed through, but about 98% of pornography / erotica was still blocked![49]

Most analyses of filter products occurred in response to fears that the use of such products would be mandated, and thus were mainly carried out between about 1997 and 2000. In 2001 NetAlert and the ABA jointly commissioned research into filter effectiveness[50] which showed extremely variable results, many of which are referred to above. Problems were still being documented in 2001 and 2002; and a 2003 report to DCITA on internet content filtering states that 'it is no more practical to use complex analysis techniques such as textual and image analysis to automatically filter web content in 2003 than in 2000. There have been no major developments in technology.'[51] The report goes on to state that while the techniques of artificial intelligence have been refined during this time and have

---

[47] Bennett Haselton, *SurfWatch error rate for first 1,000 .com domains* (2000) <http://peacefire.org/censorware/SurfWatch/first-1000-com-domains.html> at 20 June 2004.
[48] Declan McCullagh, *Smut Filter Blocks All But Smut* (20 June 2000) Wired News <http://www.wired.com/news/print/0,1294,36923.00.htm> at 20 June 2004.
[49] CSIRO, above n 18, 66-67.
[50] Ibid.
[51] Ovum, above n 23, 5. See also National Coalition against Censorship, *Internet Filters, A public policy research* (written by Marjorie Heins & Christina Cho) Fall 2001, and Henry J Kaiser Family Foundation Report *See no evil: How internet filters affect the search for online health information* Dec 2002.

increased accuracy, such techniques demand considerable computing power and thus cause significant delays.[52] The same report suggests that there may have been improvements in the ability of filters to carry out more granular or better defined filtering of URL and IP indices,[53] although the problems (referred to above) of creating such indices remain.

C. *Labeling*

Labeling involves a tag or label being attached to internet content by a provider, host, government body, or third party, which identifies the type or category of content. A number of labels may be assigned to an individual page to allow more specific information as to what kind of content the page or site includes. Filter software then reads these tags as a basis for allowing or rejecting relevant internet content.[54]

Labeling allows multiple classifications, so that one page may be tagged for example sex/health/education, another violence/news, and another cult/religion. Such classifications could even be combined with ratings, for example sex1/health3/education3, another violence4/news2 and another cult3/religion5. No choices would be made at the labeling level as to what content was desirable, appropriate, dangerous, permitted or prohibited; the material would simply be classified and rated. Users could then set filters to allow selection on the basis of labels.

However, even with established criteria, what one person may rate as sex3 another may rate as art1. Further, the more people assigning the labels the more variety there would be in the classification, and the less useful the scheme would be. Thus if content providers determined for themselves how content was to be rated, labels may be of little general value. Labeling by a centralized body or other third party

---

[52] Ibid 23. It is not clear whether this increased accuracy makes the technique nearly accurate, or even acceptably accurate, or just more accurate than previously. The report gives no references to source material.
[53] Ovum, above n 23, 23.
[54] Platform for Internet Content Selection. <http://www.w3.org/PICS/> at 20 June 2004

may overcome this problem. Currently the Internet Content Ratings Association (ICRA) for example, in issuing labels, asks content providers a number of specific questions about their content. Labels are assigned on the basis of their responses, and the ICRA criteria for assigning labels to content is transparent and freely available.

As mentioned above, the assignment of labels does not denote what content is suitable, appropriate, dangerous, etc. Rather, filters on a user's computer are set to select content on the basis of the labels it carries. Filters could be set up by individuals, or alternatively templates could be developed by third parties, such as the OFLC, businesses, or even community groups. For example, the OFLC may design an 'under 15s' template, which would exclude all content carrying labels which suggest to the OFLC that the content is unsuitable for younger persons. A school education department may create a template which allows access only to content labeled to suggest it has educational value. So long as the technical protocols for labeling and content selection were uniform, users could take responsibility for themselves selecting appropriate content, or could choose for themselves to use templates best reflecting their own views.

In the late 1990s there was a strong movement internationally toward the development of such schemes for content labeling and selection, the best known of which were Platform for Internet Content Selection (PICS), Recreational Software Advisory Council for the Internet (RSACi), and later the Internet Contents Ratings Association (ICRA). Prior to the *Online Services Act* the ABA had concluded[55] that the Government should support further development of such systems, which would allow - or could require - labeling of content by owners and providers, or by third parties.[56] These could then be used as the basis for internet users themselves to decide which categories of material they wished to access or

[55] Australian Broadcasting Authority, above n 8, 158.
[56] Any third parties could be used. Labeling could be done by a body such as the OFLC, or by independent ratings agencies, churches, education groups etc.

restrict.[57] The ABA's 1996 report listed many advantages of labeling, and went on to strongly support it as the preferred method of regulating internet content.[58]

> 'It seems to offer parents and supervisors a method of protecting minors from material which may be inappropriate for them, allows adults themselves to be shielded from material which they do not wish to view, whilst at the same time maximising freedom of speech and choice for ... users who do not want to have their access to Internet content unduly limited.'[59]

Such schemes have the potential to offer a more refined basis for content selection, and to allow users more responsibility in this sphere. Senator Alston said in 1998 that the government was 'pursuing international collaboration to establish content labeling and filtering standards worldwide. These standards will give all users, and particularly parents, the power to identify and control the type of material to which they have access on the internet.'[60] The benefits of labeling continued to be promoted, with the ABA noting in an early report on the online regulatory scheme that a rating system had been launched 'which can be adapted to different national, cultural and individual needs.'[61]

However, while the idea of content labeling looked to offer real possibilities for user choice in content selection, it had drawbacks also. Firstly, there would need to be agreement, at government or industry level, on a scheme or schemes to be used. A protocol such as PICS would allow content selection based on labels. Labeling according to more than one scheme would be possible, but too many schemes may make labeled content difficult to filter. Labeling would not be a very effective method for content selection if some filters could read the tags of some schemes and not others.

---

[57] The best known of such systems is PICS, or Platform for Internet Content Selection, but other such labelling schemes are also in development. For a critique of such systems see Electronic Frontiers Australia <http://www.efa.org.au/Issues/Censor/cens2.html#filter> at 20 June 2004.
[58] Australian Broadcasting Authority, above n 8, 156-158.
[59] Karen Koomen 'Freedom of Speech and the Internet in Australia' (Speech delivered at the Communications Law Centre Conference on 'Free Speech in Australia', Sydney, 10 September 1997) 16.
[60] Senator Alston, 'Regulatory Challenges in Cyberspace' (Speech delivered at Interactive Kids '98, Sydney, 18 May 1998).
[61] Second *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2000* Tabled in Senate by the Minister for Communications, Technology and the Arts (April 2001).

Secondly, labeling would be most beneficial if there were a 'critical mass' of labeled material,[62] even if a great deal of material remained unlabelled. Once sufficient material was labeled, filters could be used to exclude unlabelled material, which would provide an incentive for others to label. It was recognized prior to the *Online Services Act* however that to get sufficient material labeled initially, labeling would probably need to be mandated in at least some of the major content providing nations, or some incentive offered to encourage labeling. Further, if labels were to be used in content control, they would need to be applied by third parties, or there would need to be some sanction for wrongly labeling.

Labeling clearly held some promise, although with difficulties to be overcome. However, while the idea of labeling had initially been heralded as a method of empowering users to take control of their own access to internet content, by 1997 there was considerable concern that filtering using such schemes may be imposed at higher levels. It was argued that while the schemes themselves were value-neutral, the development of schemes such as PICS 'makes censorship easy because it embeds the tools of censorship into the root architecture of online publishing.'[63] It was said that 'technology which empowers parents to control the access of their children, equally empowers governments to control the access of their adult citizens ... Many of the original PICS advocates have become alarmed by the extent to which PICS makes the Web censor friendly.'[64] 'Blocking software is bad enough ... PICS is the devil.'[65]

This new perspective on labeling schemes took the gloss off somewhat. While in Europe labeling and rating is still heavily promoted,[66] it is estimated that about

---

[62] Greenfield, McRea, Ran, above n 5, 23.
[63] L Lessig, *Tyranny in the Infrastructure* (July 1997) Wired News. http://www.wired.com/wired/5.07/cyber_rights.html
[64] Graham, Irene; *'The Net Labelling Delusion: Saviour or Devil?'* (undated), <http://libertus.net/liberty/label.html> at 20 June 2004 and see Bohorquez, FA, 'The Price of PICS: The Privatization of Internet Censorship.' (1999) 43 *New York Law School Law Review.* 523.
[65] Lessig, above n 63.
[66] Michael Rotert, President of Euro ISPA, 'The Response of the Internet Industry,' (Paper presented at the INHOPE Conference, The Internet 2004: Safe or Just Safer? Berlin, 20 November 2003). Stephen Balkam, CEO of ICRA, *Submission to Review of the operation of Schedule 5 to*

100,000 sites have applied to ICRA for labels since 2001, but it is not clear how many sites use them. Even if all 100,000 sites are labeled, this remains a small proportion of all internet content, which is estimated to include well over 8 billion web pages,[67] and 50 million sites in May 2004. [68]

D. *Zoning*

Prior to the enactment of the *Online Services Act*, there had also been discussion of the possibility of 'zoning the internet' as a method of restricting access to content. Zoning could occur in a great variety of ways, and thus zoning refers more to ideas of delineating internet spaces or users, than to particular methods of doing this. Zoning may also be operative at a number of different levels, and from inclusive or exclusive positions.

A requirement to zone, or agreement to zone, could result in providers and / or hosts of content identifiying sites or parts of sites as including certain content, or as not including certain content. In the US for example hosts may identify sites as including 'content harmful to minors' or alternatively identify sites as not including 'content harmful to minors.' In Australian parlance, sites could be identified as including R or X-rated content, or alternatively as including only G-rated content, G and M-rated content etc. At site level, access could be allowed or denied depending on the user's identity. Again this could be inclusive or exclusive; an adult site for example may reject all users not exhibiting an adult identity,[69] or may allow all users not exhibiting a child's identity. [70]

---

the Broadcasting Services Act 1992 (November 2002) and for earlier discussion of the scheme see David Kerr, Internet Watch Foundation, *Action Plan on Promoting Safer Use of the Internet, Preparatory Actions – Self Labelling and Filtering, Final Report-Executive Summary*, (April 2000).

[67] Google claims to search 4 billion web pages, *About Google: Google Web Search Features* <http://www.google.com.au/help/features.html> at 27 July 2004.

[68] NetCraft, *Web Server Survey* (May 2004). <http://news.netcraft.com/archives/web_server_survey.html> at 20 June 2004.

[69] The adult verification system in fact used for Australian hosted R-rated material under the *Online Services Act* is an example of such 'zoning.' This adult zoning however has been strongly criticised as unnecessarily cumbersome, and the alternative suggestion of child zoning has generally been preferred. <http://www.efa.org.au/Campaigns/99.html> at 20 June 2000.

[70] See for example Lawrence Lessig and Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model* (1999) <http://cyberlaw.stanford.edu/lessig/content/index.html> at 20 June 2004, and Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999)

Such zoning would require ways to identify users, with possible methods including for example passwords, digital signatures or certificates of authentication.[71] Such passwords, signatures or certificates would identify users either as specific persons, or as persons with particular attributes, being a certain age for example, or living in a particular country.[72] Government or quasi-government organisations could allocate passwords, signatures or certificates, or this could be done by private enterprise, who could take responsibility for verifying that a person was who they claimed to be, or had the attributes claimed.[73] When a user then tried to access a site, that site could be set up either to allow access only if a user could show that he or she was an adult, or alternatively to reject access if a user was identified as a child. To avoid the burden of needing constantly to prove identities while using the internet, software could allow computers to be set up with this information, so that within a family for example, a person logged in as user 1 or 2 may have unrestricted access to the internet, whereas users 3, 4 and 5 are identified on log in as having restricted access. [74]

Of course this type of identification of internet users may threaten anonymity. If an individual was required to identify his or herself to gain a certificate or password, that individual could then be identified when using the internet. It is not necessary for this to be the case however. For example, face to face transactions could be used to issue passwords, as most adults could be identified as adults without showing identification. Even if identification needed to be shown, there is no need to keep records of who is issued with which password or certificate. It would be necessary once to prove that someone is an adult, it would not be necessary to record details of that person, or the identity of those to whom passwords are issued. In that case, users could prove they were adults for the purpose of internet access, without needing to surrender their anonymity.[75]

---

[71] Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999) Ch 4, and especially 34-35
[72] Ibid.
[73] Ibid.
[74] See for example Lessig and Resnick, above n 70, Lessig, above n 71, 176.
[75] Note that approved restricted access systems in Australia require the applicant's name as mandatory information. *Restricted Access Systems Declaration* 1999 (No 1) made under the *Broadcasting Services Act* 1992 (Cth).

Alternative methods of zoning include IP or domain allocations. IP allocations could be made on the basis of content carried. For example, only sites containing content not harmful to minors, or G-rated, could be hosted at IP numbers 777.77.77.777 to 999.99.99.999.[76] Alternatively, such allocations could be made specifically for those hosting adult sites. If the latter, sites could reject users without adult certification, if the former, users could set filters to allow access to content hosted only at IP addresses within the given range. Similarly, specific domain allocations were mooted, such as .kids or .xxx.[77] Restrictions may limit what could be hosted in the former, the latter would be required to restrict access unless satisfied users were adults.

While in the US and Australia restricting access to pornographic content has been the focus of zoning discussion, zoning could equally be used to denote attributes other than child / adult users or content. Attributes such as citizenship or location could also be verified using passwords, certificates and signatures, and more recently it has also been suggested that country domains of ISPs could be used. For example, expert testimony to a French Court in the *Yahoo!* case[78] suggested that sites could be set up to reject access to users whose ISPs were located in a particular place, thus allowing (theoretically at least) for requirements that pro-Nazi and White Supremist sites be set up to reject access to users identified as French or German, or whose access originates with an ISP in that jurisdiction.[79]

While zoning has great attractions, and if effective could overcome many of the problems of regulating the internet, in common with other approaches it raises many difficulties. Firstly, as with labeling, there is the question of who will decide

---

[76] William H Clinger IV, 'Internet Protocol Numerical Address Zoning,' *Testimony for Commission on Online Child Protection.* August 2000.

[77] Both domains were applied for but rejected by ICANN in 2000. Patricia Jacobus, *ICANN staff opposes ".kids," ".xxx" domains.* (10 November 2000) CN News.com <http://news.com.com/2102-1023_3-248455.html?tag=st.util.print > at 21 June 2004. Another application for .xxx domain is currently before ICANN <http://www.icann.org/tlds/stld-apps-19mar04/xxx.htm> at 21 June 2004.

[78] *LICRA et UEJF vs Yahoo! Inc and Yahoo France* (20 November 2000) Tribunal de Grande Instance de Paris (Superior Court of Paris) <http://www.gigalaw.com/library/france-yahoo-2000-11-20.html> at 21 June 2004.

[79] George A Chidi, *Internet moves toward 'virtual zoning'* (December 15 2000) CNN.com <http://cnn.com/2000/TECH/computing/12/15/german.laws.on.web.idg/> at 21 June 2004.

whether or not content is harmful to minors, or G or M or R or X-rated? Secondly, who will mandate or agree to the zoning? Would it breach privacy and unnecessarily burden speech for adults to be required to prove they are adults? Who would ensure that a children's domain for example really did host only content suitable for children? Would those identifying as children have access to too little content? Is zoning too coarse an instrument? Who would issue certificates and what should they cost? Would the burdens placed on internet users and / or the internet industry outweigh the benefits?

Beyond these problems lies the problem of jurisdiction. So long as technology is available any country can mandate some form of zoning for material hosted therein, and for access to content of users present therein, but cannot reach outside the jurisdiction. Thus zoning within the jurisdiction would only be useful if access was restricted to the jurisdiction at least for some users. Otherwise users could still freely access unzoned content from other jurisdictions.[80]

Thus to be an effective method of content control, 'zoning' would still require agreement between governments, or within the internet industry itself, that sites, and / or users, be appropriately identified. Otherwise, while local sites may stop children entering, or may require adults to prove they are adults, overseas sites not so zoned would still be accessible to all.

---

[80] In fact this is exactly what occurs presently in Australia. R-rated Australian hosted content must be housed so as to deny access to any user unless that user is identified as adult. However, that same user has no restriction when accessing similar, or X-rated, or even RC content if hosted overseas. <http://www.efa.org.au/Campaigns/99.html> at 21 June 2004. Apart from ineffectiveness, the burdens of the Australian scheme have been criticised on many grounds, 'The proposals are administratively onerous to the extent that few Australian content hosts would be prepared to incur the costs involved in setting up the relevant systems. It would be far easier to simply set up sites offshore in a country where such regulatory burdens are not imposed... The proposed identification details are easily forged, demonstrating conventional wisdom that effective age-authentication systems are almost impossible to implement on the Internet.' Electronic Frontiers Australia, *Comments on Australian Broadcasting Authority (ABA) Consultation Paper on Restricted Access Systems* (1999) <http://www.efa.org.au/Publish/ABAresp9911.html#summ> at 22 June 2000.

E. *Conclusions.*

It can be seen from the above that technology placed serious limits on what the Australian Government could achieve in terms of internet content control. While some choices were available to the Government in terms of the degree of control it wished to exercise, the locations at which control would be exerted, and the methods used to effect that control, any control would be dependent upon the available technologies. While the filtering technologies and products discussed above, based on URL, IP, word, image or profile analysis clearly had major flaws; such technology could at least be applied by users themselves, at low cost, and without need for international agreements. While filtering from labels would have improved user choice, sufficient labeling to be useful would likely have required some form of international agreement. Zoning met the same difficulties.

The technology limited what government could do to control the internet, but technology was only one aspect that the Government needed to take into account. Of course, it would be influenced also by what was being done in this sphere overseas, control of content in other media in Australia, and regulation of other industry in Australia. Each of these will be examined in turn in the following chapters.

CHAPTER FOUR: OVERSEAS CONTENT CONTROL PRIOR TO THE *ONLINE SERVICES ACT.*

The online services regime attempts to regulate the Australian part of a global industry. To understand better the enactment of the Australian legislation it is necessary to look to the international context at the time. While there was as yet no international agreement relating to the regulation of internet content, many countries around the world were grappling with similar issues, and attempts to censor or regulate internet content were varied and complex.[1] A number of these attempts were familiar to the Australian Government prior to drafting the Australian legislation. In particular, methods of internet content regulation in the UK, Malaysia and Singapore had been the subject of a comparative study commissioned by UNESCO, and undertaken by the ABA.[2]

A. The UNESCO Report

At the time of the ABA undertaking the comparative study for UNESCO, Malaysia had not introduced laws specifically to regulate internet content, and had in fact stated that the internet in Malaysia would not be censored.[3] Malaysia was hoping to develop and profit from the creation of an uncensored 'multimedia super corridor' which it was hoped would bring investment and business into Malaysia.[4] The government thus preferred an international agreement 'as to what can and cannot go on [the internet] in response to pornographic content,'[5] to a national framework which may have been seen as limiting freedom on the internet in Malaysia specifically. However, the conditions of service laid down by Malaysia's two ISPs required subscribers not to use the network 'for any activities

---

[1] Current overseas schemes are discussed in more length in Chapter Fourteen: Comparative content control – current overseas regimes. Presently however, only the pre-1999 situation is discussed, to place the drafting and enactment of the *Online Services Act* in context.
[2] Australian Broadcasting Authority, *The Internet and Some International Regulatory Issues Relating to Content: A Pilot Comparative Study Prepared for UNESCO* (1997).
[3] Ibid 36.
[4] Ibid 29, and see Davidson, AD, 'I Want my Censored MTV,' 31 Vand. J. Transnat'l L. 97 January 1998.
[5] Australian Broadcasting Authority, above n 2, 36.

not allowed under any law of Malaysia;'[6] 'to comply with and not to contravene all applicable laws of Malaysia relating to the service, not to use the service for any unlawful purpose..., and not to use the service to send or receive any message which is offensive on moral, religious, racial or political grounds or of any anxiety to any person...'[7]

Conversely, Singapore had specifically extended its definition of broadcasting services to include internet services. As a result, under the *Singapore Broadcasting Authority Act 1994* the Singapore Broadcasting Authority was bound to ensure that nothing was included in any internet service which was against public interest or order, national harmony, or which offended against good taste or decency.[8] ISPs and content providers were required to be licensed under a 'deemed' class license scheme, whereby it was not necessary to register individually, but the SBA had authority to modify, place conditions upon, or even cancel licenses if Codes of Practice issued by the SBA were not complied with, or if any laws were contravened.[9] The aim of the class license scheme was to 'encourage responsible use of the internet while facilitating its healthy development.'[10] While ISPs and ICHs were not required actively to monitor websites, they were required to block access to certain websites notified to them by the SBA, and to use their best efforts to ensure nothing contrary to the *Broadcasting Act* was included in their internet services.[11] Blocking of around 100 pornographic websites was required as a symbolic gesture.[12] Singapore's Minister of Information likened the internet to a large city, where 'there are wholesome well-lit parts and there are dark alleys with dirt, sleaze and crime.'[13] It was the

---

[6] Ibid 37, referring to JARING Conditions of Service.
[7] Ibid referring to TMNet Terms and Conditions for Dial-up Access Service.
[8] *Singapore Broadcasting Authority Act* s 6(2)(c) referred to in Australian Broadcasting Authority, above n 2, 38.
[9] Ibid s 24 referred to in Australian Broadcasting Authority, above n 2, 39.
[10] Australian Broadcasting Authority, above n 2, 39.
[11] Ibid 42, 40.
[12] Arunachalam & Eddie Kuo, 'Governing the Internet Regime' (Paper presented at Internet Political Economy Forum, Singapore, 2001) 16.
[13] George Yeo, Singapore Minister of Information and the Arts, quoted in Amy Kroll, 'Any Which Way But Loose: Nations Regulate the Internet.' (Summer 1996) 4 *Tulane Journal of Comparative and International Law* 275, 7.

Government's job to 'help its citizens keep to the well-lit areas and not allow them to stray to the wrong side of the tracks.'[14]

The content regulatory regimes of the UK aimed to be technology neutral, and thus applied to content on the internet as to content in any other medium.[15] In the UK the internet industry, in concert with government, had been active in developing directions for regulation of internet content. By September 1996 negotiations between the Internet Service Providers Association, (ISPA), the London Internet Exchange, the Safety Net Foundation, the UK Dept of Trade and Industry, the Home Office, and the Metropolitan Police, had led to the development of the R3 Safety Net Proposal; a self regulatory scheme for the internet industry.[16] The main tenets of this scheme were encouraging **R**ating of material to allow users to choose content appropriately, establishing a system for **R**eporting of complaints regarding illegal internet content, and **R**esponsibility on both content providers in rating what they provide, and on ISPs to remove illegal content, or content persistently or deliberately mis-rated.[17] In the UK an industry code of practice had also been adopted which required members to use reasonable endeavours to ensure their services did not contain anything illegal or encourage illegal acts, but which also went considerably further. Under the heading 'Decency' members were required to use reasonable endeavours to ensure 'services and promotional material [did] not contain material inciting violence, sadism, cruelty or racial hatred,' and 'are not used to promote or facilitate prostitution.'[18]

B. The ABA Report

Other developments in content regulation overseas were also brought to the attention of the Australian government before the drafting of the Online Services

[14] Ibid.
[15] Australian Broadcasting Authority, above n 2, 42.
[16] Ibid.
[17] Ibid 43.
[18] Ibid 44-45.

Bill. An ABA report to the government in July 1998[19] identified some common themes in international regulatory developments, including

- 'a recognition of the role of industry self-regulation in the online environment...;
- interest in the potential role of filtering and labeling products and services...;
- support for the use of 'hotline services' for the reporting of illegal content, and in particular child pornography;
- a recognition of the importance of community education...;
- a recognition of the importance of international cooperation....'

These themes were identified by the ABA in monitoring developments and work in the USA, Japan, Singapore, the UK, the European Commission, UNESCO and the OECD.[20]

C. US attempts at content control

An attempt in the USA to regulate online content also had a high profile prior to the drafting and enactment of the *Online Services Act*. The US *Communications Decency Act 1996*, which criminalized the transmission of obscene or indecent material through a telecommunications device to a person under 18 years old, had been held unconstitutional in the USA shortly before the enactment of the Australian legislation.[21] Although the constitutionality issue was not relevant in the Australian setting, the challenges to and decisions about the *Communications Decency Act* inspired many arguments within Australia, as well as giving considerable insight into political, social, and technological aspects of internet content regulation.

[19] Australian Broadcasting Association, *Interim Online Services Report* (July 1998).
[20] Ibid.
[21] *Reno v ACLU* 117 S Ct 2329 (1997).

D. Other methods of control

Many differing methods of censorship and content regulation were being used in other countries also prior to the introduction of the *Online Services Amendment.* While most were not influential in the decisions of the Australian government regarding how and what to regulate, they are worth noting to give a better picture of the myriad methods being used at the time in attempts to achieve similar ends.

a) Strict regulation

Some countries controlled access to content through allowing only the trusted few to have access to computers and internet connections. In Myanmar (formally Burma) for example, it was forbidden to access the world wide web, unauthorized use of a modem was punishable by 7 to 15 years in jail, and email access was restricted to fewer than 1000 people close to the ruling party (SPDC).[22] In Cuba, although the number of Cubans using the internet had grown steadily, Drake, Kalathil and Boas observed that:

> the potential pace of growth is limited by public policy allowing internet access only through approved institutions – select universities and places of employment. This policy ensures that the internet is used mainly by the politically trustworthy, and only in environments where use can be informally monitored. There are still no Internet Cafes allowed in Cuba, and individual access is prohibited, beyond a few well connected individuals who work out of their homes. Essentially, internet diffusion in Cuba is determined by government policy rather than the market...[23]

Other countries required all information coming into the country by internet to be routed through a government monitored server, so that the government itself had direct control over monitoring and blocking material seen as problematic. The United Arab Emirates forced all internet traffic through a single gateway.[24] Saudi

---

[22] Sandy Barron, 'Myanmar Works Hard to Keep the Internet Out', *New York Times* 14 July 2000.
[23] William J. Drake, Shanthi Kalathil, Taylor C. Boas, 'Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba', *Information Impacts Magazine*, October 2000. Accessible at site of Carnegie Endowment for International Peace http://www.ceip.org/files/Publications/dictatorships_digital_age.asp?p=5&from=pubdate accessed 27 July 2004.
[24] Human Rights Watch, *The Internet in the MidEast and North Africa: Free Expression and Censorship* (June 1999) <http://www.hrw.org/advocacy/internet/mena/uae.htm> at 21 June 2004 and see Jennifer Lee, 'Punching Holes in Internet Walls' *New York Times*, 26 April 2001.

Arabia spent almost two years developing the technology necessary to filter almost all web data entering the country through a central server.[25] While there were many private ISPs, all content was filtered at one gateway.[26]

Still other countries allowed easy access to computers and to the internet, but allowed only licensed or registered ISPs to operate. Conditions for operating ISPs could be very strict, and some included requirements for monitoring and blocking material. For example, China required ISPs to be registered, and to keep records of all content which appeared on their web sites and of all users who dialled onto their servers. ISPs were held responsible for blocking vast categories of internet content.[27]

b) Use of general laws to control internet content

In other places general legislation was applied in attempts to control content on a freely accessible internet. The CompuServe case in Germany was one example, which involved the criminal trial and conviction of the Managing Director of a German ISP, on charges of 'facilitating access to violent, child or animal pornographic content,' under legislation regarding *Dissemination of Publications Morally Harmful to Youth.*[28] Although in this instance the conviction was later overturned[29] attempts to use general - not internet related - law to control internet

---

[25] Lee, above n 24.

[26] Human Rights Watch, above n 24.

[27] *China's Iron-Fisted Internet Regs* (16th Oct 2000) Wired News <http://www.wired.com/news/politics/0,1283,39192,00.html> at 21 June 2004, and see Kristina Reed, 'From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce.' (Fall 2000) 13 *Transnational Lawyer* 451, 458-463.

[28] Ulrich Sieber, *Commentary on the Conclusion of Proceedings in the "CompuServe Case" (Acquittal of Felix Somm) Moving Forward into the New Millennium - A New Culture of Responsibility on the Internet* (undated) <http://www.somm-case.de/> at 21 June 2004. In this case the Managing Director of a German ISP had passed on to its US parent company a Government request to remove a number of newsgroups carrying child pornography. The newsgroups were removed, and a later request to remove many more newsgroups was also passed on to and complied with by its US parent company. After some time however the parent company introduced a filter program which allowed subscribers to block content for themselves, and so the ISP stopped centrally blocking these newsgroups. This resulted in prosecution of the Managing Director of the German ISP.

[29] Appeal against the conviction was allowed as it was held that the accused was not technically able to remove the newsgroups, and had made reasonable efforts to request the removal of the newsgroups by the parent company, which could technically have carried it out. B Frydman & I Rorive, 'Regulating Internet Content through Intermediaries in Europe and the USA.' (2002) *Zeitschrift fur Rechtssoziologie* 23 Heft 1 41, 45-46.

content have also been seen more recently in France, Germany and Norway.[30] In each case however it has been clear that such laws can influence only content originating within the jurisdiction, and will have no effect on the same or equivalent content housed beyond the jurisdiction, but accessible within it.

c) Non-governmental approaches

Another approach used in some countries prior to the *Online Services Act* was the setting up of hotlines which could take complaints about allegedly illegal material online, and then act as conduits for channeling that information on to police and other law enforcement agencies. These hotlines, which aim 'to prevent illegal activity and abuse of children,' were common in Europe by the late 1990s, such that INHOPE (Internet Hotline Providers of Europe) was established in 1999 with support from the European Commission to provide a forum for hotline providers to share their experiences and concerns.[31] Such a hotline also operated in the USA (Cybertipline),[32] and aimed to encourage the reporting of trafficking of child pornography and online solicitation of children, and to allow that information to be passed on to various international law enforcement agencies. The various hotlines drew some funding from government but were supported also by funding from the private sector. They have not required legislative backing; the hotlines are concerned about material and behaviour which is illegal anyway, not simply because it is on the internet.

CONCLUSIONS

At the time of the drafting and enactment of the *Online Services Act*, although many states appeared to recognize that internet content regulation required international agreement to be effective, no such agreement had been reached. It is clear nevertheless that many countries were grappling individually with concerns about internet content and its restriction, and that attempts to control internet

[30] These more recent attempts to apply general content laws to internet content are discussed further below in Chapter Fourteen: Comparative content control.
[31] <http://www.inhope.org/> at 21 June 2004.
[32] <http://www.missingkids.com/cybertip/> at 21 June 2004.

content were in no way confined to non-democratic countries, nor to those without respect for citizen's rights. All over the world the question of how to control internet content was being raised, but different countries had answered the question in different ways. Naturally, what content was illegal differed from country to country, as did views about what material was harmful, or even objectionable. In Australia, a great deal of content was not illegal per se, but was illegal to distribute to those under 18 for example, and could be seen as harmful to minors although legal to own. Each country had its own views, and its own rules, regarding what content should be controlled and how.

There was thus no successful general 'model' for the Australian Government to copy, but it can be seen that the scheme it enacted incorporated aspects of many of the schemes already in place around the world; such as the use of industry codes of practice, systems for reporting and investigating complaints, requirements for content blocking by ISPs, and regulation of locally hosted content.

More current approaches to internet content control are discussed further in Chapter Fourteen below, where overseas activity is examined in the light of the operation of the Australian scheme. Presently however, to continue exploring the context of the enactment of the *Online Services Act,* it is necessary to look to the situation regarding censorship and free speech in Australia at that time.

CHAPTER FIVE: CENSORSHIP AND FREE SPEECH IN AUSTRALIA.

In preparing to regulate access to content on the internet, the Federal Government found itself faced with a genuinely new technology, with novel social and cultural aspects not found in any other medium. While these were new, censorship and classification were not. A highly structured system to regulate content already existed in Australia, and the Government was thus placed in a position where, if it were to regulate internet content, it needed either to adjust an old scheme to a new medium, or to come up with a new scheme. The history of the existing scheme shows the long road Australian Governments had traveled to finally reach a reasonably uniform national scheme for censorship and classification, and helps to explain the Government's keen desire to fit the new technology into that existing scheme.

Further, because the debate over Australia's internet regulation was played out in the wake of the US case of *Reno v ACLU*,[1] free speech arguments commonly used to support an anti-censorship stance in the USA were used also in attempts to resist content regulation in Australia. However, Australian free speech protections vary greatly from those in the USA, and it is necessary to distinguish between the two to understand the powers of the Australian Government in terms of content regulation. A discussion of Australia's free speech protections follows a discussion of the classification and censorship system.

A. *Classification and Censorship in Australia*

Classification and censorship in Australia is, and has for some years, been 'managed' under a central classification system, which is a combination of Federal, State and Territory law. Laws passed by the Commonwealth allow the Office of Film and Literature Classification to make decisions on behalf of the

[1] *Reno v ACLU* 117 S Ct 2329 (1997).

Commonwealth, States and Territories, but these decisions rely for enforcement upon other Commonwealth, State and Territory legislation.

The Commonwealth has always been involved in censorship through its power to regulate interstate[2] and overseas trade,[3] and through its power of law making for the Territories,[4] but more recently the Commonwealth has also claimed legislative competence under the corporations power, the external affairs power, and the postal and telecommunications power.[5] Conversely the States have full power to make laws in this area.[6] While the current centralised classification regime looks neat and administratively sensible, this current structure belies the history of classification and censorship in Australia.

B. *A Brief History of Censorship in Australia*

From the beginning of white settlement[7] Australia has had censorship. British law, both statute and common law, was 'received' into the various colonies of Australia upon settlement.[8] Even when the colonies, and later the States and the Commonwealth, began making their own laws, censorship law continued to align closely with that of England. While British censorship had initially focused mainly on the supression of religious and political dissent,[9] from the late 18th century social change meant that censorship became more concerned with sexual

---

[2] This power is subject to *Australian Constitution* s 92.
[3] *Australian Constitution* s 51(i) and see Australian Law Reform Commission, *Censorship Procedure*, Report No 55, (Canberra 1991) 2.
[4] *Australian Constitution*, s 122.
[5] Bills Digest, Classification (Publications, Films and Computer Games) Bill 1995 (ACT), 2. *Australian Constitution* s 51(xx), (xxix), and (v) respectively.
[6] While the Commonwealth is a government of specific powers, states hold residual power to legislate over any matter not exclusively given to the Commonwealth. See for example *Constitution Act* 1902 (NSW), s 5: 'The Legislature shall, subject to the provisions of the Commonwealth of Australia Constitution Act, have power to make laws for the peace, welfare, and good government of New South Wales in all cases whatsoever...'
[7] The author acknowledges that argument exists over whether Australia was ever really 'settled' in legal terms. For the purpose of this paper however the term settled is preferred, as it is generally used to explain the reception of British law by the Australian colonies.
[8] Blackstone, *Commentaries on the Laws of England*, (11th Ed, 1791) Vol 1, 108, referred to in Cook, Creyke, Geddes and Holloway, *Laying Down the Law* (5th Ed, 2001) 33-34.
[9] D Lindsay, *Censoring the Internet: The Australian Approach to Regulating Internet Content*. Research Paper No 9, Nov 1999 (University of Melbourne, Centre for Media, Communications and Information Technology Law) 42.

material, and obscenity.[10] In Australia, material the tendency of which was to 'deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall,'[11] was censored as obscene. A much stricter test of obscenity was adopted by the Customs Department in 1930, summarized as 'whether the average householder would accept the book in question as reading matter for his family.'[12]

As most literature and films were imported into, rather than produced in, Australia, the Commonwealth government played a pivotal role in censorship, refusing to allow the importation of certain material,[13] even though censorship was not one of its specified powers.[14] Often however, this level of censorship was only the beginning, and material which was allowed past the Commonwealth customs and censorship officers was then subject to re-examination by censors in individual States. States did not surrender their censorship power in favour of the Commonwealth, and so this dual classification system (federal decision followed by state decision), continued to operate for a considerable time. There was no uniformity of decisions between the various States, and no uniformity between States and the Commonwealth.

It is not necessary to list the various censorship regimes which applied in Australia from time to time, but until the late 1900s the main features of censorship in Australia were arbitrariness, secrecy, confusion, lack of uniformity, and strictness. The basis of many censorship decisions was unclear, and decisions were often made on the basis of an individual's opinion by customs officers, police or politicians.

While this censorship system lasted a long time, so did opposition to it. Coleman, in a forward to the second edition of his book '*Obscenity, Blasphemy, Sedition;*

---

[10] Ibid 43.
[11] Justice Cockburn in *R v Hicklin* (1868) LR 3 QB 360, 373.
[12] P Coleman, *Obscenity, Blasphemy and Sedition; 100 Years of Censorship in Australia* (2nd ed 1974) 14.
[13] G Griffith, *Censorship: Law and Administration* (1993) 1.
[14] As discussed above. Commonwealth legislative powers are specified in the Commonwealth Constitution, and do not include powers to legislate for censorship, but a number of other powers have been used by the Commonwealth in this area.

100 years of Censorship in Australia'[15] discusses an 80 year 'crusade' against censorship in Australia, in which the *dramatis personae* were 'church groups, women's groups, moralists, booksellers, publishers, free-thinkers, revolutionaries, journalists, pornographers, sex reformers, muck-rakers, religious bigots, race cranks, politicians, lawyers, judges, magistrates, customs officers, postal officials, and policemen.'[16] Coleman adds that '...The basic fact about Australian censorship ... until recent years is that it was a long series of almost entirely indefensible prohibitions and prosecutions...'[17]

Criticism of the censorship regime as anachronistic and repressive in nature[18] came to a head in the 1960s, with the Film Censorship Board criticised as 'a law unto itself, working in secret, free of judicial and political control.'[19] Of literature censorship it was said that 'despite the appearance of a legal framework, the Commonwealth system of censorship is merely a façade to cloak the reality of censorship by the minister and his departmental officials.'[20]

During this decade many now famous censorship decisions were made, including the Commonwealth Censor's decision to ban horror films as 'undesirable in the public interest,' the banning of an ever growing list of authors including JD Salinger, DH Lawrence and Mary McCarthy, and the prosecution of those involved in the production of the Oz magazine in New South Wales.[21] Each of these decisions fueled the already simmering criticism of the operation of the censorship regime in Australia.

---

[15] (2nd ed, 1974).
[16] Coleman, above n 12, Prologue. (To this list one could now add the IT industry, nerds and geeks and netizens.)
[17] Ibid
[18] Griffith, above n 13, 5
[19] Ibid 6.
[20] E Campbell and H Whitmore, *Freedom in Australia*, (1966) 152 quoted in Griffith, above n 13, 6.
[21] Griffith, above n 13, 5. The latter prosecution, where the decision of a Magistrate was then overturned on appeal by a Judge, led in NSW to the re-introduction of jury trials for obscenity cases, which had been abolished in 1880. Coleman, above n 12, 45-46.

'*Australia's Censorship Crisis,*'[22] a collection of essays published in 1970, claimed to be 'the crystallization of an urgent public feeling that censorship procedures...do not accord with the 'community standards' now held by the young and yet mature majority of Australians.'[23] However, these essays argued less against censorship per se and more against arbitrary and secret censorship;

> policemen, magistrates and judges are incompetent to decide... ...this book is a recognition that the community – not policemen, politicians or magistrates – have the basic and fundamental right to determine and assert what are 'community standards.'... Secret and illiterate film censorship, book banning by anonymous decision, the whole decrepit apparatus is and must be subject to responsible and adult scrutiny ... The average reasonable mature Australian citizen is entitled to examine the idiotic, inconsistent, incomprehensible moral judgments and bannings made in his name by confused legal functionaries or anonymous public servants.[24]

As a result of the continuing public criticism of both individual censorship decisions, and of the censorship system itself, changes began to creep in. Articulating for the Federal Government a shifting attitude to censorship, Don Chipp, as Federal Minister for Customs and Excise, and therefore responsible for censorship, said:

> ...It is a monstrous thing...that there is one man...who can say to you as an adult: 'I say you cannot read this or see this or hear it.' It is an evil concept... People should censor more and more... The individual, the bookseller, should have a responsibility, the television station, the radio station, the parent, the individual; government should censor less and less, move more and more out of the field and leave it to individual choice.[25]

During Chipp's term as Minister he instituted a reporting mechanism requiring the Film Censorship Board to report on which films it had cut or banned, and a Film Board of Review was established to replace the earlier system of review by a single appeal Censor. [26] The Membership of the Film Censorship Board was also overhauled, and along with the Chief and Deputy Chief Censor, seven other Board members were appointed, to move the function of the board away from the role of

---

[22] G Dutton & M Harris (eds), *Australia's Censorship Crisis* (1970).
[23] Ibid 6.
[24] Ibid 6-7.
[25] Coleman, above n 12, 24.
[26] Griffith, above n 13, 6.

experts and toward the role of jury, making informed decisions on the basis of reasonableness.[27] Annual reports of the Board even began to include the Board members' curricula vitae so that the public could see who were making the decisions. All of this was intended to indicate a move away 'from a 'closed' model and toward an 'open' model of censorship.'[28]

To assist in achieving uniformity in literature censorship, a National Literature Board was also established in 1967, with 5 of the 9 Board members nominees of the states.[29] However, the Board's recommendations were advisory only,[30] and could be, and often were, overridden by the Federal Minister. Most states continued with their own literature censorship, although they too were attempting to move toward less arbitrary models, which focused on classification rather than censorship per se,[31] and which allowed review and appeal mechanisms. The process of decision making at the federal level, even with the establishment of the National Literature Board, remained obscure, and was substantially beyond public scrutiny and understanding.[32] As a result the Board became redundant and was abolished in 1977, and the states continued independently to censor and classify literature.[33]

While the censorship and classification system had been 'modernised' to some extent, it was still extremely fragmentary. The Commonwealth made film censorship and classification decisions for all states, but some states continued to have their own review mechanisms. Literature censorship was still carried out at both the federal and state levels.

As a result, in 1984, a legislative scheme aimed at bringing Australian classification and censorship regimes into a unitary national system was put into

---

[27] Ibid 7.
[28] Ibid.
[29] Coleman, above n 12, 24.
[30] Griffith, above n 13, 8.
[31] Ibid 9.
[32] Ibid.
[33] Ibid 8.

place.[34] While the Commonwealth had no general power over censorship, it amended its customs regulations, and enacted legislation for the ACT under its territories power,[35] intending that this legislation would be mirrored in all states and the Northern Territory.[36] The principles behind the legislation were agreed to by the Ministers of the Commonwealth, States and Territories, and were:

- Adults are entitled to read, hear and see what they wish in private and in public;
- People should not be exposed to unsolicited material offensive to them;
- Children must be adequately protected from material likely to harm or disturb them.[37]

The aim of the legislation was to establish a national classification system under which all films and publications could be classified, and to provide for restricting and prohibiting that material which ought not, under the classification guidelines, be freely available, or available at all. However, the scheme failed in this objective as the legislation was not in fact picked up in all the States and Territories, so that while the 'national' scheme operated effectively in some places, censorship and classification in Australia remained, in reality, somewhat fragmented and piecemeal.[38]

Due to the failure of the scheme, in 1990 the Commonwealth Attorney General referred the matter of film and literature censorship procedure to the Australian Law Reform Commission (ALRC). The reference stated that while the Commonwealth, States and Territories were in broad agreement as to policy, it was difficult to administer the area as the laws were unnecessarily complicated and not uniform. The ALRC was asked to report on 'how the laws relating to censorship... can be simplified and made more uniform and efficient while giving

---

[34] Australian Law Reform Commission, *Censorship Procedure*, Report No 55, (Canberra 1991) 3.
[35] Ibid.
[36] Ibid.
[37] Ibid, and see Griffith, above n 13, 7.
[38] Australian Law Reform Commission, above n 34, 6.

effect to the policy agreed....' The ALRC were also asked to draft model legislation.

After agreement between Commonwealth, State and Territory ministers, new classification legislation came into effect in January 1996.[39] The Commonwealth Government again enacted legislation for the ACT, which was to 'form a basis for a joint Commonwealth – State scheme for the classification of [publications, films, and computer games].'[40] It was again expected that each State and Territory would enact identical legislation to result in a uniform national scheme. According to the Bills Digest to the ACT legislation, 'although the issue of classification has always been an important issue for governments, the recent concern about unclassified video games and computer technology, and the availability of X-rated videos in certain states only has led to a push for a more uniform regime.'[41]

C. *The Classification Scheme at the drafting of the Online Services Act.*

Classification of films, computer games, and publications is now carried out by the (national) Classification Board, which is part of the Office of Film and Literature Classification. In making classifications the Board is required to reflect contemporary community standards and to apply criteria set out in the National Classification Code,[42] which forms a schedule to the *Act*. The Code contains the general principles to be taken into account in classification decisions, but is to be applied in conjunction with Classification Guidelines which give more detail about the nature of the various categories, and the scope and limits of material

---

[39] *Classification (Publications, Films and Computer Games) Act* 1995 (ACT) s 3: The purpose of this Act is to provide for the classification of publications, films and computer games for the Australian Capital Territory. This Act is intended to form part of a Commonwealth/State/Territory scheme for the classification of publications, films and computer games and for the enforcement of those classifications. Note: Provisions dealing with the consequences of not having material classified and the enforcement of classification decisions are to be found in complementary laws of the States and Territories.

[40] Bills Digest, above n 5, 1.

[41] Ibid 2.

[42] *Classification (Publications, Films and Computer Games) Act 1995* (Cth) s 9.

suitable for classification within each category.[43] Both the Code and the Guidelines are agreed to by the various Commonwealth, State and Territory ministers responsible for censorship in their various jurisdictions, and can be altered only by their unanimous decision.[44] The Code and Guidelines are both publicly available.[45]

Material to be broadcast on television and radio is not classified under this code. It is regulated instead by the *Broadcasting Services Act* 1992 (Cth), and various industry codes; and censorship and classification are dealt with also in broadcast license conditions.[46] Programs are classified in accordance with the National Classification Code, but additional restrictions apply, such as the times at which differently rated programs can be broadcast.[47]

Classification regimes are slightly different depending on the medium. All films and videos must be classified before they can be sold, hired, or shown publicly in Australia.[48] Computer games must be classified before they can be sold, hired or demonstrated.[49] Conversely, not all printed publications require classification,

---

[43] *Classification (Publications, Films and Computer Games) Act 1995* (Cth) s 12, and Office of Film and Literature Classification, *Guidelines for the Classification of Computer Games (Amendment No.1)* (1999) 4.

[44] *Classification (Publications, Films and Computer Games) Act 1995* (Cth) s 6 re Code amendment, and s 12 re amendment of Guidelines.

[45] The National Classification Code is a schedule to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). Guidelines are tabled in parliament and gazetted. Current guidelines are included with this thesis at appendix 2, and can be found on the OFLC website at <http://www.oflc.gov.au/resource.html?resource=62&filename=62.pdf> for film and computer games and at < http://www.oflc.gov.au/resource.html?resource=63&filename=63.pdf> for publications. Accessed 27 July 2004.

[46] See Sally Walker, *Media Law. Commentary and Materials* (2000) for further discussion of this.

[47] Lindsay, above n 9, 55-57.

[48] Office of Film and Literature Classification, *Guidelines for the Classification of Films and Videotapes (Amendment No.2)* (1999) 2. Separate Guidelines for film and computer games were in force prior to the enactment of the *Online Services Act.* Now however there is one set of guidelines covering classification of both films and computer games, which states that both films and computer games must be classified before they are 'released or advertised.' As the intent of this section is to illustrate the context into which the *Online Services Act* was enacted, the Guidelines in force at that time are referred to in the remainder of this chapter.

[49] Office of Film and Literature Classification, *Guidelines for the Classification of Computer Games (Amendment No.1)* (1999) 1. Note that these are now "Guidelines for the Classification of Films and Computer Games (2003) Refer above n 48.

only those likely to warrant restriction (submittable publications) must be submitted to and classified by the Board.[50]

The basic principles behind classification are the same regardless of medium. The National Classification Code includes the principles enunciated in 1984:

> Classification decisions are to give effect, as far as possible, to the following principles:
>
> (a) adults should be able to read, hear and see what they want;
>
> (b) minors should be protected from material likely to harm or disturb them;
>
> (c) everyone should be protected from exposure to unsolicited material that they find offensive;
>
> and a further principle added more recently;
>
> (d) the need to take account of community concerns about:
>
> (i) depictions that condone or incite violence, particularly sexual violence; and
>
> (ii) the portrayal of persons in a demeaning manner.[51]

The Code then goes on to specify how each kind of material is to be classified.[52] Film classifications include G for general exhibition, PG for material requiring parental guidance, M for material that cannot be recommended for persons under 15, MA for material that cannot be recommended for persons under 15 without the guidance of their parents or guardians, R for material that is unsuitable for a minor to see, and RC (Refused Classification) for material likely to cause offence to a reasonable adult and unsuitable for a minor to see. Classification for computer games is slightly different. There is no PG or R classification, and there is a G (8+) classification for games which may not be suitable for children under 8.

For publications there are four classifications only, Unrestricted, Category 1- Restricted for material unsuited to those under 18, and which may offend some

---

[50] Office of Film and Literature Classification, *Guidelines for the Classification of Publications*, (1999) 7.

[51] *Classification (Publications, Films and Computer Games) Act 1995* (Cth) Schedule Section 5, National Classification Code. Point (d) has been added more recently than (a) – (c).

[52] The code is annexed as Appendix 1.

adults also, Category 2-Restricted which is similar to the previous category but with more sex, nudity or adult themes, and RC for material refused Classification.

Classifications made by the National Classification Board are given effect through legislation enacted by the various States and Territories,[53] which provide for enforcement of the scheme.[54] The Commonwealth legislation interacts therefore with offence provisions enacted in each State and Territory in relation to the possession, publication or distribution of certain material. [55]

However, because States and Territories have not all introduced the same offence and enforcement provisions, censorship and classification is still not really uniform in Australia. For example, it is prohibited in every state to sell or hire X-rated videos, while this is allowed in the Territories. Further, while the Classification Board classifies publications on behalf of New South Wales, Victoria, South Australia, Queensland and the Territories, WA and Tasmania operate their own schemes.[56] So while censorship and classification in Australia is probably closer to uniform than ever before, there are still considerable differences and inconsistencies which may never be overcome.

After all this work toward a national classification and censorship scheme, internet content came along. By the late 1990s, regulatory provisions for the control of internet content in various states and territories was already creating fragmented, uncertain and inconsistent legislative frameworks.[57] In the context of

---

[53] In NSW, ACT, NT, SA, TAS, Vic the legislation is: *Classification (Publications, Films and Computer Games) Enforcement Act* 1995. In Qld the legislation *is Classification of Computer Games and Images Act* 1995, *Classification of Films Act* 1991, *Classification of Publications Act* 1991. In WA the relevant legislation is the *Censorship Act* 1996.

[54] John Dickie, *Classification and Community Attitudes,* Research Paper No 5 (Jan 1998) 2 (University of Melbourne, Centre for Media, Communications and Information Technology Law).

[55] The Commonwealth / State / Territory agreement 'relating to a revised co-operative scheme for censorship in Australia' can be found online via the OFLC website at <http://www.oflc.gov.au/resource.html?resource=215&filename=215.pdf> 28 July 2004.

[56] Griffith, above n 13, 11.

[57] Prior to the enactment of the *Online Services Act*, some States and Territories had enacted legislation aimed at control of internet content. The Commonwealth Government was concerned by this 'possible regulatory fragmentation of differing State/Territory legislation and the possible adverse effect on the development of the online industry.' Broadcasting Services Amendment (Online Service) Bill 1999, Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 21 April 1999, 3957, 3958 (Senator Ian Campbell, Parliamentary Secretary to Senator Alston, Minister for

earlier attempts at centralizing content control for other media, the Government was aware of how difficult it would be to create a uniform national scheme once States and Territories had already entrenched their own regimes. The Federal Government was thus understandably keen to avoid the establishment of another fragmented censorship scheme. It therefore moved toward the creation of a new scheme to cover internet content, which required the government to look also to freedom of speech concerns.

D. *Freedom of speech.*

Many arguments against the introduction of the *Online Services Act* were based on freedom of speech. Some arguments were based on a general desire not to have speech regulated or restricted, and some based on a desire not to have the internet regulated. Commonly however, arguments made on the grounds of free speech failed to distinguish between generally applicable *concepts* of free speech, and the specific protections for free speech existing in Australia or in the US.

It was not surprising that this was so, firstly as there had been little focus on freedom of speech in Australian politics or law, and secondly because free speech protections in the USA had just been successfully used to impeach the *Communications Decency Act,* the USA's first federal attempt at internet censorship.[58] However, it is necessary in any discussion of free speech in Australia to understand what rights to freedom of speech exist in Australia, and to understand just how limited such rights are. Once this is understood, it is easy to see why classification and censorship in Australia has not led to the problems encountered in places such as the USA where laws attempting to censor or restrict communications have infringed against protections for freedom of speech.

Communications, Information Technology and the Arts). State and Territory regulation of internet content both before and after the enactment of the *Online Services Act* is discussed in depth in Chapter 10: State and Territory legislative provisions.

[58] *Reno v ACLU* 117 S Ct 2329 (1997).

In the United States, unlike Australia, speech is protected from restriction, except in some narrow and well defined categories. The unequivocal text of the First Amendment to the US Constitution - 'Congress shall make no law ... abridging the freedom of speech' - places the burden on government to justify its encroachments on free expression.[59] Although the test has been stated in various ways, 'the question has always been whether there is a sufficient justification for legislative restriction of the guaranteed right.'[60] In Australia on the other hand, although freedom of speech ideals often influenced both the judiciary and the legislature, it was treated as a 'residual liberty' rather than an essential and central one. Such freedom only existed 'to the extent that legislation or common law rules did not restrict it.'[61]

The source of such protections differs also. In the USA and many other countries, rights to freedom of speech (amongst other things) are explicitly granted by a constitution or other document.[62] In Australia, although there have been many arguments made in favour of such explicit enactments,[63] moves to introduce such a document have not come to fruition. [64] As a result, in order to identify protection for freedom of speech in Australia it is necessary to look not to one document but to various possible sources. These include the general or common law, international law or conventions, and the Australian Constitution. It is worth examining each of these.

1. *Free speech and the general law in Australia.*

In Australia a general right to free speech has never been recognised. Such a right was not recognised in the UK prior to the reception of English law into the

[59] R Smolla, *Free Speech in an Open Society* (1992) 5.
[60] Murray Wilcox. *An Australian Charter of Rights?* (1993) 27.
[61] Sally Walker, *Media Law, Commentary and Materials* (2000) 13.
[62] For example First Amendment to United States Constitution, Canadian Charter of Rights and Freedoms, New Zealand Bill of Rights Act, South African Bill of Rights, European Convention for the Protection of Human Rights and Fundamental Freedoms; all referred to in Sally Walker, *Media Law, Commentary and Materials* (2000) 6-8, and see also discussion on the former two in Wilcox, above n 59.
[63] See for example Wilcox, above n 60.
[64] Ibid.

colonies of Australia, and the continuous development of common law in the Australian environment has not produced such a right.

It is true that there has been recognised a general freedom to do anything not restricted by law. But the right to freedom of speech only exists therefore where there is nothing to prevent its exercise,[65] and as a result 'free speech does not mean free speech, it means speech hedged in by all the laws of defamation, blasphemy, sedition and so forth, it means freedom governed by the law.'[66]

There have also been more recent pronouncements by the High Court on the general law in relation to freedom of speech. Although there may generally be a freedom to speak, that freedom will not necessarily prevail over other interests.[67] 'Freedoms or immunities recognised by the common law are, generally speaking, liable to impairment or abrogation by legislation.'[68] It is clear then that the general law would not restrict the legislative powers of the government with regard to censorship legislation.

2. *Free Speech and international conventions.*

A second possible source of rights to freedom of speech is international law and conventions. However, unless enacted into Australian domestic law, these will directly bind neither parliament nor the courts. Although Australia is a party to the *International Covenant on Civil and Political Rights*, (ICCPR)[69] it is not bound in domestic law to apply that convention.[70] Its importance lies rather in the fact that

---

[65] *Australian Capital Television Pty Limited v The Commonwealth* (1992) 177 CLR 106, 182 per Dawson J.

[66] *James v Cth* (1936) 55 CLR 1 per Lord Wright, PC.

[67] *Australian Capital Television Pty. Limited v The Commonwealth* (1992) 177 CLR 106, 142 per Mason CJ, 159 per Brennan J.

[68] *Nationwide News Pty. Limited v Wills* (1992) 177 CLR 1, 48 per Brennan J.

[69] New York, 19 Dec 1966, *Aust Treaty Series* 1980 No 23. With regard to Australia's reservations to that Covenant see ICCPR with notes re ratifications and reservations. <http://www.clea.org.uk/treaties/Iccpr.htm> at 21 June 2004.

[70] The ICCPR is included as a schedule to the *Human Rights and Equal Opportunity Commission Act* 1996 (Cth). According to s 11 the functions of HREOC include examining enactments to ascertain whether they are, or would be, inconsistent with or contrary to any human right, inquiring into any act or practice that may be inconsistent with or contrary to any human right, promoting an understanding and acceptance, and the public discussion, of human rights in Australia; and undertaking research and educational programs and other programs for the purpose

it may indirectly influence the courts 'to have greater regard to the ICCPR as a source of fundamental rights norms...'[71] While courts have held that a judicial interpretation which does not conflict with such a convention will be preferred to one which does,[72] parliament still has a right to enact legislation without regard to and even in conflict with international conventions which have not been enacted into domestic law.[73]

However, Australia is also a party to the First Optional Protocol of the ICCPR, which allows an individual to petition the United Nations Human Rights Committee once all domestic avenues of obtaining a remedy have been exhausted.[74] Thus in theory, even without the ICCPR being enacted as Australian law, legislation which cut across rights protected by the convention could be challenged by an individual before the Human Rights Committee. While Australia has been a signatory to the protocol since 1991, only one successful challenge to Australia's laws has been made under this protocol.[75]

Whether enacted domestically or enforced under the First Optional Protocol, it is unlikely that the ICCPR would stymie the *Online Services Amendment.* Article 19 of the ICCPR makes quite clear that the rights it proclaims to freedom of expression are rights which need balancing against other rights, and are not to be construed as absolute rights. Article 19 states:

(1) everyone shall have the right to hold opinions without interference;

(2) everyone shall have the right to freedom of expression, which includes the freedom to seek, receive and impart information...

---

of promoting human rights... In the *Act* 'human rights' refers to rights and freedoms recognized by the Covenant (amongst other things), read as a reference to the rights and freedoms recognised by the Covenant 'as it applies to Australia' (s 3).

[71] Sally Walker. *Media Law: Commentary and Materials* (2000) 70.

[72] *Minister of State for Immigration and Ethnic Affairs v Ah Hin Teoh* (1995) 183 CLR 273.

[73] See also Sir Anthony Mason, Centre for International and Public Law, ANU Law Faculty, *Human Rights and Australian Judges*, Law and Policy Paper No 3 (1996).

[74] First Optional Protocol to the ICCPR, Articles 1&2 <http://www.unhchr.ch/html/menu3/b/a_opt.htm> at 21 June 2004, in force for Australia 25 Dec 1991.

[75] *Toonen v Australia*, Communication No 488/1992, Un Doc CCPR/C/50/D/488/1992 (1994) found at <http://www.unhchr.ch/tbs/doc.nsf/0/d22a00bcd1320c9c80256724005e60d5?Opendocument> at 25 June 2004.

(3) [the above rights carry with them] special duties and responsibilities ... and may therefore be subject to certain restrictions ...

(b) for the protection of national security, public health or morals.

It appears that the terms of the ICCPR are sufficiently broad to allow the type of censorship legislation enacted by the Commonwealth, States and Territories. Furthermore, the types of expression which international bodies have dealt with regarding freedom of expression suggest that any speech stifled by the *Online Services Act* is not that most likely to be protected by the Covenant.[76]

3. *Free speech and the Australian Constitution.*

A further possible source of free speech rights or protections is the Commonwealth Constitution, which restricts the extent to which governments can limit communication on political and governmental matters. Prior to 1992, although freedom of speech was valued and did influence the judiciary to some extent,[77] no constitutional protection for freedom of speech had been recognised. More recently however, a number of High Court cases have held that such constitutional protections do exist.[78]

(a) The source of the freedom.

An implied freedom to communicate on government and political matters is found by the High Court to arise from the entrenchment in the Australian Constitution of

---

[76] 'Cases before international judicial bodies have established key safeguards for freedom of expression. These include the principle that a free press is of cardinal importance to democracy, the obligation on governments to allow private broadcasters, the principle that politicians must tolerate a greater degree of criticism under defamation and related laws than ordinary citizens, the importance of protecting the confidentiality of journalists sources, the illegitimacy of requiring journalists to obtain licenses and the right of military personnel to criticise the military.' *Legal and constitutional guarantees of freedom of expression.* <http://www.unesco.org/op/eng/3may98/art-19.htm> at 21 June 2004.

[77] Sally Walker above n 71, 13-14.

[78] *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1, *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106, *Theophanous v Herald and Weekly Times Ltd* (1994) 182 CLR 104, *Stephens v West Australian Newspapers Ltd* (1994) 182 CLR 211, *Cunliffe v Commonwealth* (1994) CLR 272, *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, *Levy v State of Victoria and Others* (1997) 189 CLR 579. For discussion of the development of the law in this area see Michael Chesterman, *Freedom of Speech in Australian Law, a Delicate Plant* (2000) particularly ch 2.

a governmental system based on representative democracy. The entrenched representative democracy requires a government directly chosen by the people, which in turn requires free elections. Free elections require real choice, and to have real choice there must be an ability to communicate on relevant matters. 'Freedom of communication on matters of government and politics is an indispensable incident of that system of representative government which the Constitution creates...'[79]

A string of High Court cases in the 1990s had all held that an implied constitutional freedom of communication existed,[80] but the decisions and individual judgments within them differed markedly. In an attempt to clarify the basis and the scope of the freedoms implied in the Constitution, the High Court in *Lange*[81] brought down a unanimous decision. The court was very careful in this case to confine its implication of freedoms to the specific text of the Constitution. While some earlier judgements,[82] had implied rights and freedoms from the nature of the polity or from the Constitution generally, the court in *Lange* rejected this approach, holding that 'under the Constitution the relevant question is not "What is required by representative and responsible government?" but rather "What do the *terms* and *structure* [italics added] of the Constitution prohibit, authorise or require?"'[83] In *Lange* the Court found that sections '7 and 24 and the related sections of the Constitution necessarily protect the freedom of communication ... concerning political or governmental matters which enable the people to exercise a free and informed choice as electors.'[84]

(b) Individual rights to free speech.

The High Court was very clear that the freedom to communicate which required protection under the Constitution could not be characterised as an individual's

---

[79] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 559.
[80] See list of cases above n 78.
[81] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
[82] Particularly those of Justice Murphy. See *Australian Capital Television Pty. Limited v The Commonwealth* (1992) 177 CLR 106, 185ff per Dawson J, discussing cases where Murphy J had sought to imply freedoms of movement, speech, and other communication, using implications based 'not upon the text of the constitution, but upon the nature of our society.' Dawson J then went on to discuss the various judgements in which Murphy J's views are rejected.
[83] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 567.
[84] Ibid 560.

right to free communication. The sections of the Constitution giving rise to protection for freedom of communications 'do not confer personal rights on individuals. Rather, they preclude the curtailment of the protected freedom.'[85] 'They are a limitation or confinement of laws and powers which give rise to an immunity rather than a right in the strict sense.'[86]

It is important to note also that in most of the 'free speech' cases the High Court examined aspects of the rights and restrictions on power which arise under the First Amendment to the US Constitution. The High Court found that although US jurisprudence was helpful in its analysis, the Australian position differs markedly and is clearly distinguishable from that of the US. The framers of the Australian Constitution had examined and specifically rejected the US model prior to the enactment of the Australian Constitution, and there is therefore no case for the import of US free speech notions in interpreting the Australian Constitution.

(c) The scope of the freedom.

In relation to internet content regulation or censorship, the scope of this freedom is its most important aspect. While the freedom implied by the Australian Constitution effectively limits government power in some instances, it is clear that the freedom is confined. What is less clear is the extent of its confinement.

According to *Lange*,[87] to determine whether a law is invalid due to inconsistency with the Constitutionally implied freedom, a two-stepped approach is necessary. 'First, does the law effectively burden freedom of communication about government or political matters either in its terms, operation or effect? Second, if the law effectively burdens that freedom, is the law reasonably appropriate and adapted to serve a legitimate end the fulfillment of which is compatible with the maintenance of the constitutionally prescribed system of representative and

[85] Ibid.
[86] Ibid, quoting Deane J in *Theophanous v The Herald and Weekly Times and Another* (1994) 182 CLR 104, 168.
[87] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

responsible government ...? If the first question is answered "yes" and the second is answered "no" the law is invalid.'[88]

Consequently, it is necessary firstly to determine what communications could be said to be 'communications about government or political matters.' It is clear that 'communication' may extend beyond speech, but less clear what is 'government or political.' Since the unanimous decision in the *Lange* case[89] it appears that protected communications may include communications not only about parliament and its members and potential members, but also about the conduct of government ministers and their departments, public servants, public utilities and statutory authorities.[90] The protection may also extend to what appears to be discrete State or Territory issues due to the 'increasing integration of social, economic and political matters in Australia.'[91] Furthermore, the protection is not confined to communications occurring during election periods.[92]

Where communication is clearly political or governmental less problems arise, but in some situations defining 'political or governmental' has been more difficult. Since *Lange*,[93] decisions in the cases of *Levy*,[94] *Brown*[95] and *Coleman*[96] have illustrated some of the kinds of communication which might be covered by the implied freedoms. It was successfully argued before the High Court in *Levy* for example that a non-verbal protest against duck shooting could be seen as political communication, and its legislative restriction therefore subject to the implied freedom. Similarly in *Coleman,* the Queensland Court of Appeal accepted that oral statements such as 'This is Constable [P], a corrupt police officer,' and

---

[88] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 567-568.
[89] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
[90] Michael Chesterman, *Freedom of Speech in Australian Law, a Delicate Plant* (2000), particularly ch 2, 18, referring to *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 558-9, 561.
[91] Chesterman, above n 90, 18-19, referring to *Levy v State of Victoria and Others* (1997) 189 CLR 579, 596.
[92] Chesterman, above n 90, 19, referring to *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561.
[93] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
[94] *Levy v State of Victoria and Others* (1997) 189 CLR 579.
[95] *Brown v Members of the Classification Review Board of the Office of Film and Literature Classification* (1998) 154 ALR 67.
[96] *Coleman v P and Anor* (2001) 189 ALR 341.

distribution of written material entreating readers to 'Get to know your local corrupt type coppers' may well fall into the category of communications about government or political matters.[97]

In *Brown* on the other hand, an argument that shoplifting instructions were political speech failed to win majority support.[98] In that case, an article containing shoplifting instructions was published in 'Rabelais', a university student newspaper. After investigation by the Commonwealth Office of Film and Literature Classification, the article was refused classification under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth), on the basis that it instructed in matters of crime. Once refused classification, distribution of the article became an offence under equivalent Victorian legislation. The Federal Court heard an appeal against the refusal of the OFLC to classify the publication.[99]

Justice French thought it arguable that the text in question fell within the protected category, stating that 'political matters are not limited to matters concerning the functioning of government. They may include broad discussion about the social and economic organisation of society as well as about its laws and proposals for their change.'[100] He thought that there were many arguments against the article being seen as political discussion, but found nonetheless that 'inelegant, awkward and unconvincing as is its attempt to justify its practical message about shoplifting by reference to the evils of capitalism, it is arguable that in some aspects it would fall within a broad understanding of political discussion.'[101]

---

[97] *Coleman v P and Anor* (2001) 189 ALR 341. Justice McMurdo noted that as the Solicitor General, on behalf of the Attorney, had conceded that these were communications about political or governmental matters, he could jump straight to the second limb of the *Lange* test, 342-3. Justice Davies did not canvass this, while Justice Thomas found it unnecessary to decide this point, as a decision that the law was invalid would make 'characterisation of [the Appelant's] conduct or language... unnecessary,' 354.

[98] *Brown v Members of the Classification Review Board of the Office of Film and Literature Classification* (1998) 154 ALR 67.

[99] Ibid.

[100] Ibid per French J at 80.

[101] *Brown v Members of the Classification Review Board of the Office of Film and Literature Classification* (1998) 82 FCR 225, per French J at 238.

The other justices disagreed however, with Justice Heerey stating that the article did not concern political or government matters. In response to submissions that encouragement of theft may be seen as an expression of political dissent or incitement to social change, he noted that the:

> author is not advocating the repeal of the law of theft, either generally or in respect of theft from shops owned by large corporations. The article says nothing, expressly or by implication, about the conduct of holders of elected or appointed public office or the policies which should be followed by them. The article is not addressed to readers in their capacity as fellow-citizens and voters. The article does not even advocate breaking one law as a means of securing the repeal of another law perceived as bad...[102]

Having rejected that argument Justice Heerey went on to state that 'all this may be in one sense politics, but the constitutional freedom of political communication assumes – indeed exists to support, foster and protect - representative democracy and the rule of law. The advocacy of law breaking falls outside this protection and is antithetical to it.'[103]

It appears from the decision in *Brown* that, if the shoplifting instructions had been used there as a way of advocating changes in the law, they may have been seen as 'political speech' subject to constitutional protection. Is it possible then that content restricted or prohibited by the *Online Services Act* would also fit within that category? If content which would be prohibited or R-rated is used to make a political point, as for example in the Tharunka publication of the 1970s,[104] might it be successfully argued that the *Online Services Act* is unconstitutional?

It appears possible, but unlikely. Although more decisions based on differing fact situations will help over time to answer the question of what communication does and does not fall within the confines of the constitutional protection, the majority of High Court Justices, in a range of cases, have tended toward confining the

---

[102] *Brown v Members of the Classification Review Board of the Office of Film and Literature Classification* (1998) 154 ALR 67 per Justice Heerey at 87.

[103] Ibid 87-88.

[104] *Reg. v Bacon* [1973] 1 NSWLR 87, [1977] 2 NSWLR 507.

ambit of the implied constitutional freedom.[105] The High Court is expected shortly to hand down its appeal decision in the *Coleman* case,[106] which itself may give better definition to the communications covered by the implied constitutional freedom. If the confined interpretation continues, it is unlikely to be a relevant constraint on the *Online Services Act.*

Further, even where legislation does burden communication within the governmental / political sphere, the implied freedom will not invalidate a law enacted to satisfy a legitimate end if 'the object of the law is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government... [and] ...the law is reasonably appropriate and adapted to achieving that legitimate object or end.'[107] It is unclear however, when a law will be so adapted. Since *Lange* there have been a number of judicial formulations as to how 'reasonably appropriate and adapted' is to be measured. The court may look to whether the restriction on communication is itself intentional, or is merely incidental to some other purpose, whether the restriction is proportionate with the competing public interest which the law is designed to serve, and whether there were alternative or less restrictive methods of achieving the same or similar ends.[108] Each of these enquiries may be given more or less prominence in individual cases, and it remains unclear what test will be used to determine the circumstances in which restrictions will or will not invalidate legislation.

Decided cases help illustrate the confines of the freedom in this regard. In *Levy* for example it was held that even though the protest action being restricted was political, a law stopping the protest was in fact necessary to protect the safety of duck shooters and protesters. The legislation was aimed at a legitimate end with appropriate restrictions only.[109] In *Brown,* Justice French found that although the speech may have been political, the Classification Code under which the

---

[105] For discussion of these developments see Chesterman, above n 91, Ch 2, and especially 44-55.
[106] *Coleman v P*, High Court, B98 of 2002 heard October 2003, judgement reserved (29 June 2004).
[107] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 562.
[108] Elisa Arcioni, 'Politics, Police and Proportionality, An Opportunity to Explore the Lange Test: Coleman v Power' [2003] *Sydney Law Review* 17, 5-7, and for further discussion of this see Chesterman, above n 90, Ch 2, 69-72.
[109] *Levy v State of Victoria and Others* (1997) 189 CLR 579.

publication was classified sought 'by reasonable and appropriate means to protect the rule of law which is of the essence of democratic society with representative and responsible government' and consequently would not be invalidated by the implied freedom. [110]

CONCLUSIONS

It can be seen from the above that the law relating to freedom of speech in Australia is unlikely to create a barrier for a Government wishing to restrict access to material refused classification, or classified R or X, whether that material is on the internet or in any other medium.[111] The general law, and probably international conventions also, will not be seen to limit the Government's ability to restrict such material. Further, given the reasonably narrow interpretation of communications subject to the implied constitutional protections, little content restricted by the *Classifications Act,* and thus by the *Online Services Act*, is likely to invoke this protection. The *Online Services Act* as it relates to internet content regulation is thus unlikely to be challenged or avoided on the basis of freedom of speech.

[110] *Brown v Members of the Classification Review Board of the Office of Film and Literature Classification* (1998) 82 FCR 225, per French J at 239.
[111] Unless that content could be classified as 'political' material. This is however unlikely, as restriction of political material tends not to be the aim or the result of this type of restriction.

CHAPTER SIX: REGULATORY BACKGROUND

To understand Australia's co-regulatory scheme for internet content regulation, it is necessary to have an understanding of the Australian regulatory framework which preceded the introduction of the *Online Services Act.* This chapter will thus deal briefly with the pre-existing regulation in similar industries, before looking at the background to regulation of the computer industry and the content it carries.

Unlike the Australian States, which have a general power to make laws for the peace, welfare, and good government of their territory,[1] the Commonwealth can enact legislation only if it falls within a head of power specifically conferred by the Constitution. Since the enactment of the Commonwealth Constitution in 1900 however, many powers specified by the Constitution have been interpreted broadly by the High Court to take into account social and technological change. Although what is now commonly referred to as the 'telecommunications power,' is in fact worded only as a power to pass laws with respect to 'postal, telegraphic, telephonic, and other like services;' the power has been more broadly interpreted by the court to allow the Commonwealth to legislate over many new technological developments.[2] Radio broadcasting, and by analogy television broadcasting, have been held by the High Court to be covered by s51(v),[3] and although there has been

---

[1] *Constitution Act 1902* (NSW) s 5 'The legislature shall...have power to make laws for the peace, welfare, and good government of New South Wales in all cases whatsoever.' Different States use different words, but basically all give similarly broad powers.

[2] For further discussion see Geraldine Chin, 'Technological Change and The Australian Constitution' (2000) 24 (3) *Melbourne University Law Review* 609.

[3] *R v Brislan: Ex Parte Williams* (1935) 54 CLR 262. This case decided by a 4:1 majority that 'broadcasting' could be regulated by the federal government exercising its powers under s 51(v) of the Constitution. Interestingly, it appears that Dixon J, who dissented in that case, may well have held that internet services did fit within s 51(v) although he held that broadcasting did not. He found the section's reference to post, telegraphic, telephonic and other like services covered services which 'consist in an established system organized for the purpose of performing a function to satisfy the demands of the members of the community. The demand they go to satisfy in common is for means of interchanging intelligence at a distance. The primary requirement of the community they fulfil is for a method by which an individual who desires to communicate with another at a distance may dispatch and have delivered to him his message, or establish direct oral communication with him. No doubt the need of receiving communications, if sent, is an important want of a community. The two things are mutual. But the ability of the individual to originate the communication received is the first condition. The expression "other like services" covers, I should think, every system or organized process of furnishing means of individual inter-communication...' 292, 293. Dixon J held that broadcasting was not similar in that it relied on one

no court decision directly on the matter, regulation of the internet would likely also be included.[4]

Some form of federal regulation of internet content in Australia had been anticipated since at least 1993, when the Federal Government ordered an enquiry into Computer Bulletin Boards.[5] From that time on 'governments of Australia [had] been attempting to develop laws to regulate transmissions over computer networks, with a particular focus on restricting the availability of pornographic material...'[6]

To some extent it was foreseeable also that internet regulation, when it came, should take the form it did, not in terms of detail but in terms of a broadly 'self- or co-regulatory' scheme established by legislation, and overseen by the Australian Broadcasting Authority. Since 1982, when the *Broadcasting Services Act* was introduced, it had been clear that in this sector[7] a 'soft-touch, self- or co-regulatory' approach was preferred by government.[8]

---

receiving information transmitted outward from a central point with 'no inter-communication; no means is provided by which one individual can originate a message or establish communication with another...' 293. R v Brislan held 51(v) to cover radio broadcasting, more recently *Jones v Commonwealth* (No 2) (1965) 112 CLR 206 held that this power extended also to television broadcasting.

[4] The Commonwealth government is not obliged to state the power under which it is legislating. Thus it is only where the legislation is challenged in the High Court as beyond government power that the Commonwealth would need to specify a particular head of power. Furthermore, the government need not specify one head of power, it may rely on a number of heads of power for one piece of legislation, here for example 51(v) telecommunications is the most obvious, but powers such as s 51(i) trade and commerce, and s 51(xx) corporations may also be invoked to support any particular piece of legislation.

[5] Computer Bulletin Board Systems Task Force, *Regulation of Computer Bulletin Board Services* (1995).

[6] Kimberley Heitman, 'Vapours and Mirrors' (March 2000) 6(1) *UNSWLJ Forum, Internet Content Control* 30, 30.

[7] Although there have been and still are arguments about the correctness of grouping internet with broadcasting, similarities can certainly be seen in terms of the service comprising the transmission of content and information to the public at large.

[8] The terms co-regulation, self regulation, and enforced self-regulation are all used to describe varying degrees of regulation, by industry itself and backed by government sanctions or the threat of them. Self-regulation is likely to be the most industry driven of these regimes, with enforced self regulation or co-regulation placing increased emphasis on the role of government in the regulatory regime. While co-regulation suggests government and industry acting in concert to regulate an industry, self-regulation more often denotes an industry regulating itself, but within (or even without) a legislative framework. In truth however the various terms are not necessarily descriptive of only one circumstance, and often more than one term could be used to describe a particular regulatory structure. What is clear however is that in such a case regulation will not be

A. *Regulation of industry*

In the years prior to the passage of the *Online Services Act*, governments, both in Australia and elsewhere, had been moving away from government-centred regulation, but also away from no-regulation. Unregulated industries, especially industries important to the economy overall, providing public goods, or serving the public interest, were seen as problematic when unregulated, causing concern for governments and consumers alike.[9] On the other hand, over-regulation and heavy government regulation was said to tie up industry, often subverting market forces, and inhibiting economic growth and progress. The 1980s and 1990s thus saw increasing moves in developed nations toward the middle road of legislatively backed self or co-regulation,[10] which was increasingly viewed as a more desirable method of ensuring an appropriate degree of regulation, while not overly burdening the relevant industry.

The advantages of co-regulation and self-regulation are said to be many. Firstly higher levels of expertise and technical knowledge are likely to be found within the industry itself than within any government regulator. Further, experts within an industry are likely to have a better understanding of what the industry would see as reasonable and useful in terms of regulation. Efficiency is another benefit said to arise from self or co-regulation. Those within an industry have easier access to the industry, and therefore experience lower costs in acquiring the necessary information to formulate and set standards. This inside involvement ought also to lead to lower monitoring and enforcement costs, partly as those within industry are able to act more informally and enjoy the trust of the industry itself which outside or governmental regulators would not. Further, in a regime of self or co-regulation the industry itself is likely to bear more of the cost, whereas

---

exclusively governmental, but the degrees to which industry takes responsibility for regulating itself may vary considerably.

[9] Anthony I Ogus, *Regulation: Legal Form and Economic Theory* (1994) Ch 3.

[10] For further discussion of legislatively backed self-regulation see Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (1992) especially Ch 4 'Enforced Self-Regulation.' See also Karen Yeung, 'Negotiated Compliance Strategies: The quest for effectiveness and the importance of constitutional principles,' (Unpublished, paper presented at ALRC conference, Sydney, June 2000).

with governmental or external regulators a great deal at least of the costs of regulation are likely to be borne by government and therefore by tax payers.[11]

Moves toward co and self-regulation had been evident in a great many industries in Australia, and could clearly be seen in the media and telecommunications industries. Print media, television, radio, and telecommunications were all subject to varying degrees of self and co-regulation.[12] For some industries legislation required that the industry largely regulate itself, so as to be more responsive to the needs of consumers and society, to ensure that better products or services were available to consumers, but also to encourage efficiency and competitiveness in the industry itself.[13] On the other hand, without legislation, the print media had itself set up the Australian Press Council to regulate concerns about publications.[14]

An ABA Issues Paper preceding the investigation into the regulation of online services alluded to the many advantages of codes of practice,[15] and industry codes of practice were becoming a standard structural part of much regulation. For example, under the *Broadcasting Services Act* 1992 there are separate codes of practice regulating commercial television, commercial radio, community radio, subscription broadcasters, and narrowcasters. There was an ABC Code of Practice made under the *Australian Broadcasting Corporation Act* 1983, and an SBS Code

---

[11] See R Baldwin & M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999) Ch 10. And see Australian Broadcasting Authority, *Investigation into the Content of On-line Services, Issues Paper* (December 1995) 24.

[12] The regulation of these industries is discussed in Senate Select Committee on Information Technologies, Cth, *In the Public Interest: Monitoring Australia's Media* (April 2000).

[13] See for example *Broadcasting Services Act 1992* (Cth) s 3.

[14] Australian Press Council Home Page, http://www.presscouncil.org.au/ at 20 August 2004, and note particularly 'About the Press Council - Benefits of Self Regulation,' http://www.presscouncil.org.au/pcsite/about/benefits.html at 20 August 2004.

[15] Australian Broadcasting Authority, *Investigation into the Content of On-line Services, Issues Paper* (December 1995) 24.

of Practice made under the *Special Broadcasting Service Act* 1991.[16] A code of practice for the telecommunications industry was being developed.[17]

The responsibilities resting upon each group or industry varied considerably. For the Press the scheme was clearly self-regulatory. For commercial broadcasters there was extensive legislative prescription of the industry's roles, which would be better described as co-regulation. Other industries lay between the two. The responsibility for developing codes of practice, for deciding what should or should not be included in the codes, for dealing with complaints, monitoring code compliance, and for imposing sanctions, varied considerably, but all these other industries had or were developing regulatory schemes, generally somewhere on the spectrum between self-regulation and co-regulation.

However, the internet industry remained relatively unregulated.[18] Although it had spend a great deal of time drafting codes it had not yet finalised one, and no federal regulatory scheme dealt specifically with the internet or internet content. Some content offences were covered by state legislation,[19] but this was seen as an

---

[16] How prescriptive the relevant legislation is for each body or group, and how much responsibility the body or industry itself has in drafting Codes of Practice varies. While full responsibility for developing codes may lie with industry, legislation may prescribe to a greater or lesser extent what those codes must, may or may not cover.

[17] Senate Select Committee on Information Technologies, Cth, *In the Public Interest: Monitoring Australia's Media* (April 2000).

[18] Content control was not the only regulation being pursued however. Between 1997 and 2001 other major regulatory changes were also made in terms of privacy: *Privacy Amendment (Private Sector) Act 2000* (Cth) which enacted 10 privacy principles for dealing with data, Office of Federal Privacy Commissioner <http://www.privacy.gov.au/publications/npps01.html> at 23 June 2004 and copyright: *Copyright Amendment (Digital Agenda) Act 2000* (Cth) which introduced 'the most comprehensive reforms to Australian copyright in 30 years. In essence, the Act updated the *Copyright Act 1968* to take account of technological developments such as the Internet...' Australian Government, Department of Communications, Information Technology and the Arts, *Guide to the Copyright Amendment (Digital Agenda) Act 2000* <http://www.dcita.gov.au/Article/0,,0_1-2_1-4_13287,00.html> at 23 June 2004

[19] Queensland had enacted the *Classification of Computer Games and Images Act* in 1995. Victoria in 1995 and WA and the Northern Territory in 1996 enacted legislation specifically regulating online content. The NSW government in 1996 drafted for discussion a bill to regulate online services, with a view to its adoption also by other states and territories. The ACT in 1999 proposed amendments to its own Classification Act to include regulation of internet content. The role of the states in censorship and classification is discussed in more detail in Chapter 4: Censorship and Free Speech, and more recent state and territory legislation is discussed in more detail in Chapter Ten: State and Territory legislative provisions.

unsatisfactory and fragmentary way to regulate what was a global - or at the very least a federal – problem.[20]

The internet was becoming more widely accessible and a more mainstream source of information and 'content,' and the internet industry had not managed to develop any scheme to regulate itself. In the light of the regulation of the industries mentioned above, it was not surprising then that the internet would be further regulated by the Government. But, because of the different structures and technologies involved, along with the different history and social aspects of the internet, it was not easy for government simply to replicate for the internet the regulatory models in force in other industries.

A. *Regulation of computer networks*

By 1992 computer networks were recognized as a method of distributing 'content' globally, but recognized also as requiring a different and perhaps distinct form of regulation from content distributed through other media. The first Government sponsored enquiry to look specifically at the regulation of content accessible over computer networks came in 1992, with the Federal Government ordering an enquiry into Computer Bulletin Boards.[21] The initiation of the Bulletin Board Task Force was closely tied to attempts to regulate adult and illegal content in computer games. While censorship ministers were looking to change computer games classifications to allow them to contain only content suitable for children, it became clear that such regulation could apply only to computer games physically distributed, and would not reach the games accessed via bulletin boards. Thus the Censorship Ministers excluded content available on BBS from the general

[20] The Commonwealth Government was concerned by 'possible regulatory fragmentation of differing State/Territory legislation and the possible adverse effect on the development of the online industry.' Broadcasting Services Amendment (Online Service) Bill 1999, Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 21 April 1999, 3957, 3958 (Senator Ian Campbell, Parliamentary Secretary to Senator Alston, Minister for Communications, Information Technology and the Arts).

[21] Computer Bulletin Board Systems Task Force, above n 5.

classification scheme, but created the BBS Task Force to look further into its regulation.[22]

Apart from concerns about unregulated computer games, content on BBS more generally also led to 'community concern.' As the emergence of many new technologies - including film, television, video, and cable TV - had likewise led to community concern about the corruption of society,[23] it was not surprising that 'community concern' should again arise with the advent of Bulletin Boards. Although the Task Force noted that it was this concern which fuelled the government's investigation of possible regulation, when the Task Force was formed and commissioned by the government to

> 'consider options for developing a system of regulation of BBS that would allow users, parents and guardians to make informed entertainment choices for themselves and those in their care, and
> provide adequate protection to children from material that might otherwise harm and disturb,'

less than 4% of Australian homes were thought to have a computer and a modem, necessary to gain access to bulletin boards. Furthermore, on calling for submissions from the public, the Task Force did not receive a single submission 'from persons complaining that they or their children had gained access to offensive material posted on BBS.'[24]

---

[22] Ibid. 'On 4th November 1993 Commonwealth, State and Territory Censorship Ministers agreed that regulation for a regulatory scheme for computer games or images offered for sale...be drafted as a matter of priority....The computer game scheme will only apply to 'over the counter' sales of computer games and images. It is clear that games and other material that might otherwise come within the new classification regime is freely available over the telephone network on BBS. Due to the need to act swiftly and the legal and technical aspects involved in the regulation of BBS, that material was excluded from the proposal. However, in view of the concerns expressed by many in the community at the prospect of children gaining access to violent or sexually explicit material through home computers, it was agreed that a task force be created specifically to look at ways in which the content of material available on bulletin boards could be regulated.': at 11.

[23] 'History shows that every important innovation in communications technology has caused a moral panic.' D Lindsay, University of Melbourne, Centre for Media, Communications and Information Technology Law, *Censoring the Internet: The Australian Approach to Regulating Internet Content*. Research Paper No 9 (Nov 1999) 55-57. Note also Peter Chen, Australia's Online Censorship Regime: The Advocacy Coalition Framework and Governance Compared (PhD Thesis, ANU, 2000) 103.

[24] Computer Bulletin Board Systems Task Force, above n 5, 4.

The BBS Task Force recognised that regulatory problems arising on BBS were likely to be far broader than pornography concerns, and included concerns about unauthorised copying and distribution of copied material, distribution of stolen credit card and phone numbers, distribution of confidential and defamatory information, and racial vilification. The Task Force noted however that 'community attention to date has focussed on the manufacture and distribution of computerised pornography.'[25]

The Task Force identified four options for regulation of BBS, in addition to the 'do-nothing' option.[26] 'Doing nothing' it did not recommend, as although BBS saturation was at that point minimal, it anticipated substantial growth in usage which could make later regulation more difficult. Furthermore, the Task Force believed that a 'do-nothing' approach could 'be interpreted by a segment of the community ... as an admission of impotence by the government.'[27]

The Task Force recommended what it called 'Option A,' that the BBS community be required to regulate itself by drafting 'best practice guidelines' (industry codes of practice) with which BBS operators would be required to comply.[28] Along with these guidelines, complaints could be made to the OFLC regarding specific content, which could then be classified and its removal by BBS operators ordered. The Task Force acknowledged possible difficulties with code compliance being enforced by a non-government body such as an industry association,[29] but thought nonetheless that true self-regulation for BBS operators could be introduced immediately, with no lead time and minimal cost, allowing the Government time to monitor and assess its effectiveness, and to assess the other options.

The Task Force however foresaw that government may not welcome this option, writing 'The Task Force recommends that as an immediate response, the Government adopt Option A. *If Option A is not accepted,* the second preference is

[25] Ibid 14.
[26] Do nothing is Option D.
[27] Computer Bulletin Board Systems Task Force, above n 5, 9.
[28] Ibid, 36 & 28.
[29] Ibid, 36 & 38-30.

for option B1...'[30] Government desire to take greater action to control BBS was also noted in a response to the report of the BBS Task force: 'The report presented no evidence of harm, but its authors obviously felt obliged to recommend new controls.'[31]

The second option (B1) recommended by the Task Force was to require the above mentioned self-regulation, and additionally to introduce legislation specifically prohibiting transmission (or obtaining or acquiring), advertising as available for transmission, or possessing for transmission, objectionable material.[32] Objectionable material was that refused classification, or in the case of a computer game, any game unsuitable for a minor. No other BBS material would require classification nor restriction, and under this scheme it would be a defence to have taken all reasonable steps, in the circumstances, to avoid contravention.

Option B2 escalated Options A and B1, by additionally including as objectionable material 'anything which is unsuitable for a minor to see or play.'[33] Thus rather than restricting only Refused Classification material or adult computer games, all material unsuitable for minors would have been restricted under this option.

Finally, Option C was to require compulsory classification of all material on BBS, and for BBS material then to be regulated as films and computer games were regulated. The Task Force noted however that 'the costs of enforcing any comprehensive regulatory scheme are likely to be prohibitive.'[34]

The Report on the Regulation of BBS is particularly interesting not because of any regulation which arose from it, but because even in 1993/1994, with so few of Australia's population having any connection to or interest in bulletin board systems or computer networks, the Task Force was already able to identify almost

---

[30] Ibid 10, italics added.
[31] Public Policy Assessment Society Inc, *Response to Consultation Paper on the Regulation of On-line Information Services*, (1995) 1.
[32] Computer Bulletin Board Systems Task Force, above n 5, 36 & 30-32.
[33] Ibid, 9.
[34] Ibid, 17.

every concern and difficulty which would arise regarding the regulation of 'ephemeral' content' transmitted via computer networks.

Firstly, even at this early stage, the Task Force foresaw the potential for growth, and change, in both the technology itself, and in the take-up of the developing technologies. It thus recommended the formulation of principles which could be applied to the regulation of industries across a broad spectrum, understanding that regulation relevant only to BBS would be too narrow and short sighted. The BBS Report noted that

> any Task Force recommendation accepted by government will obviously have implications for the regulation of broadband services. There is a clear need for co-ordination in the formulation of communications and technology policy, including on questions of content regulation. Access to offensive or disturbing material can be provided by an increasing number of sources, of which BBS is just one... Any regulatory scheme introduced for a service, such as that offered by BBS, needs to be reasonably consistent with government regulatory policy for other electronically accessed or delivered communications.[35] [36]

Further, the Task Force was aware of the need for any regulation to isolate issues relating to medium from issues relating to content, and then to distinguish between various content issues. It noted thus that copyright, fraud and other criminal offences should be dealt with in isolation from other 'content' regulation.[37] Further, it noted the different focuses required to regulate content on bulletin boards: one focus 'essentially on content of bulletin boards and on censorship issues, the other on bulletin boards as a medium, and on general law enforcement issues associated with the new technologies.'[38]

The Task Force also engaged with the issue more recently dubbed 'media equivalence,' and the possibility that identical content in different media may be regulated differently. One emotive submission to the Task Force noted that it

---

[35] Ibid, 10.
[36] An investigation into 'broadband services' (Broadband Services Expert Group Inquiry into New Communications Services) commenced during the term of the BBS Task Force, and was due to report in Dec 1994. Computer Bulletin Board Systems Task Force, above n 5, 9-10.
[37] Computer Bulletin Board Systems Task Force, above n 5, 3.
[38] Ibid.

would be 'a travesty of justice' if material were legal in one medium but not another.'[39] The Report itself stated that a ban on X and R-rated material on bulletin boards would be 'attacked as being inconsistent and unwarranted in view of R and X rated material in other media...'[40] Questions also arose as to what would be the appropriate equivalent classification, and even at this stage it was suggested that text may be classified as film.[41]

Relative to 2003, in 1993/1994 computer transmissions were few, users were few, and content was minimal. However, even then the Task Force found that the sheer quantity of content on BBS made it impossible to pre-classify, or to subject all content to checking by BBS operators.[42] Even if content could be checked, enforcement against individual content-posters would be nearly impossible, as once a user gained access rights to a bulletin board it was possible to post anonymously or as another person. Here arose two of the major problems of regulating internet content, the decentralised nature of providers, and the fact that any user could post material. With earlier technologies, content had been distributed from a central source.

The inconsistency of State and Territory classification enforcement schemes was also recognised by the BBS Task Force, which found that although s85ZE of the Commonwealth *Crimes Act* may sometimes be used to enforce classification and censorship controls (if the matter in question fell within Commonwealth power), generally such controls relied on a mish-mash of State and Territory regulation, which decreased any chance of enforcement at other than the Commonwealth level. Even with better thought-out and more consistent legislation, the nature of the technology would make detection of offences a huge problem.

The Task Force also recognised that only very small quantities of BBS content were problematic, but that these quantities were likely to grow with the growth of accessibility of the medium, and that the material which was problematic could be

[39] Ibid 15.
[40] Ibid 25.
[41] Ibid 26, 27.
[42] Ibid 16.

extremely problematic, even to the extent of including child pornography and paedophile contacts. The Task Force noted concerns however that greater regulation of BBS could serve to move more problematic BBS groups underground, where increased security would add to the difficulties of detection.

As with the more recent debate on the topic, there was consideration in the BBS report of the role of and need for parental supervision, and the usefulness or otherwise of 'technologies'[43] to 'reject defamatory or obscene information.'[44] It was recognised that such technologies would be costly in terms of time and effort, and could anyway ultimately be circumvented.[45]

The investigation conducted by the BBS Task Force was thorough and considered, and gave government a number of options for implementing varying degrees of BBS content regulation, whilst also not down-playing the difficulties likely to be involved in any such regulation. However, by the time the BBS Task Force reported, bulletin board systems were fast losing importance. 'Those interested in personal computer networking had already begun to explore seriously a new development in public computer networks, a technology that utilised simplified graphical browsing, hypertext, and provided the user with a greater access to material on a global scale: the World Wide Web had arrived in Australia.'[46]

While the BBS Task Force had noted that in 1994 less than 4% of Australians had access to a computer and modem from home, by 1995 the number of Australian computers connected to online services was increasing at a rate of over 50% per year.[47] Numbers of service providers for example had increased from less than a dozen in 1993, to over 130 in 1995.[48]

---

[43] Now generally known as 'filters'.
[44] Computer Bulletin Board Systems Task Force, above n 5,16.
[45] Ibid.
[46] Chen, above n 23, 101.
[47] Australian Broadcasting Authority, above n 15, 14.
[48] Ibid.

Although the report of the BBS Task Force was too late to be usefully implemented, it had both anticipated the difficulties, and identified the possibilities, in relation to regulation of 'that kind' of media. In fact, the BBS Report could be seen in many ways as a blueprint for the OSA, with findings and recommendations simply stretched to fit the newly developed internet.

Taking the findings of the BBS Task Force, along with those of the Broadband Expert Group,[49] in July 1995 the Attorney General's Department and the Department of Communications and the Arts jointly published a consultation paper proposing a regulatory framework which built upon the work of the BBS Task Force, but in relation to a wider range of services.[50] The paper began: 'There is community concern over the availability of offensive material from on-line information systems...'[51] The paper stressed that 'no Government, Commonwealth, State or Territory has made a decision on the matter.'[52] However, the consultation paper proposed a strategy which would incorporate

- an effective self-regulatory scheme including a code of practice and complaints procedure;
- a comprehensive education strategy; and
- the introduction of appropriate offence provisions.[53]

The 'self-regulatory scheme' proposed was actually already moving toward the co-regulation end of the spectrum, with the consultation paper stating that 'a self-regulatory scheme is proposed, reinforced by an education program and legislative sanctions to enhance its effectiveness.'[54]

Further, by 1995 the government had already conceded that the objectives of such regulation were potentially contradictory, as they needed to:

---

[49] The Broadband Services Expert Group reported in *Networking Australia's Future* (Dec 1994). That Report looked at the development of network infrastructure and the encouragement of the use of broadband technologies generally. While it did not look specifically at content control issues, it did note the need to ensure that any such controls were consistent across technologies. Chapter 4.
[50] Consultation paper issued jointly by Attorney General's Department and Department for Communications and the Arts (7 July 1995).
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Ibid.

- protect freedom of expression, especially with regard to private communications between adults;
- limit children's exposure to harmful or unsuitable material;
- support the development of new services that enhance Australia's competitiveness;
- ensure that emerging service industries are not burdened with unnecessary costs; and
- align censorship regimes for new services with the regimes that have been adopted for other media.[55]

In August 1995 the task of investigating an appropriate regulatory regime for online services was handed over to the ABA.[56] Questions of content regulation were also the subject of an ongoing Senate Enquiry,[57] although this enquiry focused more on the need for the regulation of content than on the technical issues involved. The Senate Committee's second report noted that it had 'directed its attention solely at the key issue of the regulation of obscene, offensive or other undesirable material available through on-line services.'[58] That committee recommended strict offence provisions, including for transmitting, obtaining, demonstrating, or advertising via a computer network RC, X or R rated material. It also recommended requiring age and identification verification for the issue of online accounts, and a system of community education to assist users to deal with restricted material available despite regulations.[59]

The following ABA enquiry took a broad view of online regulation, and examined in more detail both how such a regulatory scheme could work, and many

---

[55] Ibid.
[56] Australian Broadcasting Authority, above n 15, 14.
[57] Senate Select Committee on Community Standards Relevant to Information Technologies, Cth, *Report on Regulation of Computer On-Line Services* Part 1 (Sept 1995), Part 2 (Nov 1995) Part 3 (1997).
[58] Ibid Pt 2 Ch 3 Summary 3.94.
[59] Ibid Pt 2 Recommendations. Its 3rd report went further, suggesting heavy fines for breach of codes of practice; consistent state, territory and cth legn; random checks for restricted content; investigation of labeling schemes, phone and fax hotlines for complaints. Senate Select Committee on Community Standards Relevant to Information Technologies Part 3, Recommendations, above n 52.

associated issues.[60] The ABA report closely examined for example the existence and further potential development of technologies such as content filters, of systems such as the platform for internet content selection (PICS), of closed networks for specific groups, especially children, and of the usefulness of ancillary functions such as community education programs, hotlines and complaints handling functions. Its enquiry was much wider-ranging than any of those undertaken by the Senate committees, and offered the government a more holistic view of the issues involved in online regulation. The ABA report recommended what it termed 'a substantially self-regulatory regime'[61] for online service providers in Australia, the main thrust of which was the development of codes of practice by industry groups, with the codes then registered and monitored by the ABA.[62]

The whole question of regulating online content was now firmly on the agenda, but not everyone was looking at it from the same perspective. There were those most concerned about restricting children's (and adults') access to inappropriate content, those most concerned with protecting freedom of speech on the internet, others concerned about the technical aspects of any such restriction, and yet others concerned to ensure that the demand for online services in Australia continued to grow. By July 1996 Senator Alston was 'mindful of the dangers of heavy-handed regulation discouraging innovative content and access providers' and mindful also of 'the complexity of the issue, both technically and morally.'[63] The conflicts inherent in internet regulation were becoming more clear.

In July 1997 the government released its 'Principles for a Regulatory Framework for On-Line Services in the Broadcasting Services Act 1992' which proposed 'effective industry self-regulation ... supervised by the ABA.'[64] The regime was to be 'broadly consistent with the self-regulatory framework applying to

---

[60] Australian Broadcasting Authority, *Investigation into the Content of Online Services* (1996)
[61] Ibid 134.
[62] Ibid 117, 134.
[63] Senator Richard Alston, Speech delivered to Internet Industry Association of Australia (INTIAA) (5 July 1996).
[64] Department of Communications and the Arts, 'Principles for a Regulatory Framework for Online Services in the Broadcasting Services Act 1992' (Press release, 15 July 1997).

broadcasters and narrowcasters under the BSA ....'[65] Again the conflicts involved in online regulation were apparent, in that the principles provided that a regulatory regime should encourage online service providers to respect community values, establish means for addressing complaints, give high priority to the protection of minors,[66] encourage self-regulatory mechanisms and *'in particular avoid inhibiting the growth and development of the online services industry by placing unreasonable regulatory constraints on the online service provider industry....* '[67]

C. *Internet industry activity.*

As discussed above, a regulatory scheme for the control of online content had been envisaged for some years before the Online Services Bill was finally introduced to Parliament. Regulation of the content available online had been investigated, discussed, threatened, and proposed since the early 1990s, and just about every proposal, from the BBS Task Force, to the ABA, to the Government's own principles, suggested that self-regulation was the preferred option. As a result, the Online Services Bill surprised many in threatening a considerably harsher regulatory scheme than that which had been foreshadowed previously, far closer to co-regulation than to self-regulation. The Bill was far more prescriptive than had been expected, with stricter government regulation threatened if the industry failed responsibly to regulate itself. This was at least partly due to the Government perceiving the internet industry as unable or unwilling to regulate itself.[68]

As one would expect, internet industry associations were working during this time to establish codes of practice which could form the basis of self-regulation and thus avoid the imposition of such codes drafted by others. While some organizations managed to establish codes to the satisfaction of their members,[69]

---

[65] Ibid, Structure of Regulatory Regime.
[66] Ibid, Objectives.
[67] Ibid, Objectives.[italics added by author]
[68] Cth, *Parliamentary Debates*, Senate, 24 May 1999, 5198 (Senator Alston).
[69] See for example code developed by Western Australian Internet Association, concluded 1995, referred to in 'Introduction to WAIA and Code of Conduct' 25 October 1995

no national code had been completed. Prior to the *Online Services Act* passing through Parliament, the Internet Industry Association[70] had already spent four years drafting and redrafting proposed codes, but none had yet been approved as final.[71] As Senator Alston commented while the Bill was before Parliament: 'The Internet Association has been conscientiously developing Codes of Practice, but I think it is fair to say it would concede that it has not made a great deal of progress... This is not a position which we think is responsible. We have, therefore put down a framework ...'[72]

The regulatory scheme for the control of online content had been long in the making, and in fact there was little in the *Online Services Act* which had not been at least alluded to as a possibility as far back as the BBS Task Force Report. While the introduction of the legislation took some by surprise, the regulatory scheme introduced was not really out of line with what preceded it in terms of industry regulation, or with what had been suggested previously in terms of computer content control.

CONCLUSIONS

It can be seen from the above that the creation of a regulatory scheme for internet content was both informed by, and limited by, existing factors. The uniqueness of the internet and the technology upon which it was built limited the choice of content control mechanisms available to the Government. Overseas attempts to control internet content informed the Government of possibilities, but Australia's own regulatory schemes, for censorship and classification, as well as for industry

---

http://www.waia.asn.au/cgi-bin/db.cgi?db=waia&uid=default&sb1=4&so1=descend&view_records=1&Category=---&keyword=code+of+practice&nh=9&mh=1 at 20 August 2004.

[70] Formerly the Internet Association.

[71] 'The present Draft Code Version 5.0 is the product of almost four years development including extensive consultation and subsequent refinement. It is anticipated that the Code will form a fundamental element of the self regulatory landscape for the Internet in Australia and has been designed to raise consumer confidence in the medium, particularly for the purposes of e-commerce. [The previous] Code version 4.0 was the product of amendments following the publication of Version 3 in December 1998. Internet Industry Association, August 1999 <http://www.iia.net.au/contentcode.html> at 23 June 2004.

[72] Senator Alston, above n 68.

control, which had developed locally over many years, defined to a great extent the context within which any new regulatory scheme would need to be formulated. However, while self-regulation was increasingly becoming the norm in other industries, the lack of any voluntary movement in this direction by the Australian internet industry led to calls for more Government-mandated regulation, to which the Government responded.

PART TWO

PASSAGE, PROVISIONS, OPERATION, AND EFFECTS OF THE INTERNET CONTENT CONTROL REGIME.

In this part of the thesis the passage and provisions of the *Online Services Act* are examined, along with the operation and effects of the *Act*. This part initially discusses the introduction of the Online Services Bill and its passage through Parliament, and then looks at the provisions of the *Act* itself. The operation of the *Act*, including the drafting and registration of the Internet Industry Codes of Practice, the establishment and operation of a complaints regime, the establishment of NetAlert, and the proposed complementary state and territory legislative provisions, are all examined, before moving on to look at data from studies on internet content control, submissions made to the Review of the *Online Services Act,* and the report from the Review itself. Evaluation of the scheme's achievements and effects are then dealt with in Part 3 of the thesis.

CHAPTER SEVEN: PASSAGE AND PROVISIONS OF THE ONLINE SERVICES ACT.

A. *Passage of the Act*

As discussed in the previous chapter, the Government had first shown an interest in regulating the content available via computer networks in 1992, although at that stage less than 3% of homes were thought to have access to computer networks.[1] By 1999 over 650 ISPs provided internet access to over 3.6 million Australians.[2] Content accessed through the internet was thus thought to be increasingly influential in the community, concerns were being expressed about the nature of the material accessible through this medium, and the Australian States and Territories were increasingly introducing local legislation in attempts to control such material.[3] Against this backdrop, and after years of investigation, national legislation to regulate internet content was formally proposed in the Commonwealth Parliament.

A barrage of criticism accompanied the introduction to Parliament of the Broadcasting Services Amendment (Online Services) Bill, which was intended to be 'part of a multifaceted approach to ensure a uniform national approach to online content regulation.'[4] [5] The specific aims of the Bill were a) to provide a means for addressing complaints about internet content, b) to restrict access to internet content likely to cause offence to a reasonable adult, and c) to protect children from exposure to internet content unsuitable for them.[6] But these aims were subject to a regulatory intent that 'public interest considerations [should] be

---

[1] Computer Bulletin Board Systems Task Force, *Regulation of Computer Bulletin Board Services* (1995) 14.
[2] Broadcasting Services Amendment (Online Service) Bill 1999, Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 21 April 1999, 3957, 3958 (Senator Ian Campbell, Parliamentary Secretary to Senator Alston, Minister for Communications, Information Technology and the Arts).
[3] Ibid.
[4] Senator Ian Campbell, above n 2.
[5] Regulatory fragmentation was a major concern to the federal government, as some states and territories had already begun independently to enact their own legislation for the control of internet content. Discussed in more detail in Chapter 10: State and Territory legislative provisions.
[6] Broadcasting Services Amendment (Online Services) Bill 1999 (Cth) (schedule 1) cl 2, now incorporated to become *Broadcasting Services Act 1992* (Cth) s 3 (k) (l) and (m).

addressed in a way that does not impose unnecessary financial and administrative burdens on Internet content hosts and Internet service providers.'[7] While the Bill was before Parliament attempts were made to 'clarify the balance between the public interest in addressing concerns about content issues and the Government's desire not to impose undue financial or administrative burdens on industry,'[8] but in fact the relative weights of each were never really clear.

Such was the interest in the Bill that between its introduction and its enactment, an enquiry relating to the Bill by the Senate Select Committee on Information Technologies[9] received over one hundred written submissions and many oral submissions in a period of only three weeks.[10] A great deal of political and industry consultation also occurred while the Bill was before the Committee, and consequently it was substantially amended prior to passing the Senate on May 26th 1999 and proceeding to the Lower House. While the amendments quietened some criticisms of the Bill, very many criticisms remained, and were still being heard when the major substantive provisions of the *Act* came into effect six months later.[11] At this stage Industry Codes, drafted in response to the legislation, also came into effect, so for the first time those both within the industry, and outside it, came to see how the 'co-regulatory' scheme for controlling internet content was to work.[12] The Codes further addressed some of the initial concerns about the anticipated effects of the *Act.*

Initial criticisms of the *Online Services Act* were many and varied, but could be broken into four main categories. First, concerns were raised about the Government's motivations in attempting to regulate internet content at all, and why the government chose this particular time to act. Secondly, concerns were

---

[7] Ibid (schedule 1) cl 4, now incorporated as *Broadcasting Services Act 1992* (Cth) s 4(3)(a).
[8] Supplementary Explanatory Memorandum (undated), Broadcasting Services Amendment (Online Services) Bill 1999 (Cth).
[9] Senate referred the Online Services Bill to the Committee on 23 April 1999 (2 days after its introduction to the Senate). Report tabled in Senate 11 May 1999.
[10] Senator Jeannie Ferris, Introduction to the *Report of the Senate Select Committee on Information Technologies.* (May 1999) The committee received 104 written submissions, and heard from 33 witnesses in four public hearings.
[11] On 1 January 2000.
[12] Internet Industry Codes of Practice, registered by the ABA 16 Dec 1999, for implementation from 1 January 2000. The Codes can be found at <http://www.iia.net.au/index2.html> at 23 June 2004.

raised relating to the Government's technical ineptitude and its lack of understanding of internet technology. Thirdly, concerns were raised regarding the effect the legislation would have on the operation and development of the internet industry. Fourthly, concerns were raised about censorship and restrictions on freedom of speech. Within each of these main areas, concerns were complex and far-reaching, and often conflicting.

The many criticisms relating to the Government's motivation in proposing the new legislation were interwoven. The Government claimed that the legislation was a response to generalised 'community concerns'[13] about the availability of 'problematic' internet content, specifically that which is 'illegal, pornographic or unsuitable for children.'[14] Those skeptical of the Government's claims noted that surveys showed 'limited support for government censorship among internet users,'[15] with fewer than 3% of respondents to one survey citing indecent material as a concern, compared with 18% citing privacy.[16] For non-users, content ranked as less of a barrier to internet use than cost and lack of access. [17]

Further, while the government had for a considerable time foreshadowed legislation to control internet content,[18] the timing of the introduction of the legislation also led to criticism of the Bill as a primarily political manoeuvre.[19] While the government had sufficient seats to control voting in the House of Representatives, Independent Senator Brian Harradine, long noted for his moral

---

[13] Senator Ian Campbell, above n 2, 3957.
[14] Ibid.
[15] Peter Chen, 'Pornography, Protection, Prevarication: The Politics of Internet Censorship,' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 18, 18.
[16] Electronic Frontiers Australia, *Submission to Senate Select Committee on Information Technologies*, (30 April 1999). 'In the June 1997 www.consult survey of Australian Internet users, fewer than 3% of the 8,591 respondents cited indecent material as a concern (compared with 18% citing privacy and 28% access times). And in a telephone survey of over 1,000 non-users of the Internet, only 15% mentioned indecent material on the Internet as a concern, even with prompting.' <http://www.efa.org.au/Publish/senate99.html#7> at 23 June 2004.
[17] Australian Broadcasting Authority, *Interim Online Services Report of the ABA to the Minister* (July 1998).
[18] Ibid 5 and discussed in Chapter Four: Overseas internet content control prior to the *Online Services Act.*
[19] See for example David Marr, *The High Price of Heaven* (2000) 76, Kimberley Heitman, 'Vapours and Mirrors' March 2000 6(1) *UNSWLJ Forum, (Internet Content Control)* 30, Chen, above n 15, 19.

conservatism,[20] held the balance of power in the Senate until June 1999. For the Government to pass other - unrelated - legislation, Senator Harradine's support in the Senate was essential, and the passage of the *Online Services Act* was seen by many as the *quid pro quo*. Senator Harradine would vote with the Government on other legislation in exchange for the introduction by the Government of the *Online Services Act*.[21] Even the corporation set up under the *Act* to take responsibility for community education was to be based in Tasmania, Senator Harradine's home state.

Regarding technological limitations, the Government was accused of enacting legislation which it knew, or should have known, could not work. In this respect it was criticised for attempting to regulate internet content without understanding the technical impossibility of its plan,[22] and it was criticised on the other hand for engaging in a cynical exercise of symbolic politics.[23] It was suggested that the Government *did* understand that the legislation it was enacting could not work to achieve its stated aims, but wanted nevertheless to be seen to be doing something, even if that 'something' proved ineffective.[24] This of course was tied to concerns regarding the motivation of the Government; was the Government enacting legislation it knew would not work, simply to ensure Senator Harradine's support?

The third major concern related to the possible effects of the legislation upon the internet industry. The introduction of the Online Services Bill was commonly said to make Australia 'the village idiot of the internet world,'[25] a tag which may

---

[20] For discussion specifically of Senator Harradine's moral crusades see Ch 4, 'Soldiers of the Cross,' in Marr, above n 19.

[21] See for example Marr, above n 19, 76, Heitman, above n 19, 30.

[22] For example see Jon Casimir, 'Act of Stupidity' *Sydney Morning Herald* (Icon) 17 July 1999, referred to in Chen, above n 15, 18. See also Anna Johnson, *Key Legal and Technical Problems with the Broadcasting Services Amendment (Online Services Bill)* 1999, (unpublished) and see Heitman, above n 19, 33, who noted that of the two main tenets of the legislation as presented to the Australian public, a) removing problematic Australian hosted material and blocking problematic overseas hosted material and b) empowering users to decide for themselves through the use of filtering technology software, neither survives technical scrutiny.

[23] Chen, above n 15, 18.

[24] Marr, above n 19, 114.

[25] See for example Nadine Strossen, President of American Council for Civil Liberties, quoted in 'Australia Urged to Repeal Law' *Sydney Morning Herald* (Business Section) 24 August 1999, referring to a comment by Danny Yee of Electronic Frontiers Australia: 'The government has turned Australia into the global village idiot.' EFA Media Release 26th May 1999.

discourage investment in the Australian internet industry.[26] A more concrete concern was that Australian content would be moved offshore in response to the legislation, and in consequence create further content import from overseas hosts, lessening our proportion of input to output. This would take money out of the industry not only by forcing content providers to abandon local hosts, and use and pay for hosts overseas, but also by increasing the proportion of material downloaded by Australians from sites outside the country, and decreasing the proportion of content downloaded from Australian sites by users overseas.[27]

Major concerns also arose that hosts and carriers might need to monitor content, and could be liable for content over which they had no control, and which should be the responsibility of the content owner or provider.[28] The need for internet service providers (ISPs) and internet content hosts (ICHs) to monitor content they carried or hosted was likened to requiring a phone company to monitor the content of phone calls, or the Post Office to monitor the content of mail.[29] ISPs and ICHs were concerned that any such monitoring would be costly and time consuming, and could itself lead to liability if decisions about content were wrongly made. ISPs were also concerned that blocking[30] content would significantly slow internet traffic in Australia, making internet use far less attractive to both commercial and private users, and so have major economic repercussions. [31]

Fourthly, concerns about censorship and freedom of speech were also loudly voiced during and after the passage of the *Online Services Act*. While the Explanatory Memorandum to the Bill itself identified three possible categories of

---

[26] See for example Brendan Scott, *The Dawn of a New Dark Age – Censorship and Amendments to the Broadcasting Services Act* (April 1999) (unpublished).
[27] Ibid.
[28] Brendan Scott, 'Silver Bullets and Golden Egged Cheese: A Cold Look at Internet Censorship' (March 2000) 6(1) *UNSWLJ Forum,(Internet Content Control)* 14, 14-17.
[29] Peter Coroneos, 'Internet Content Control in Australia: Attempting the Impossible?' (March 2000) 6(1) *UNSWLJ Forum,(Internet Content Control)* 26, 27.
[30] As provided for in Broadcasting Services Amendment (Online Services) Bill (Cth) cl 37(1)(c), and after amendment of the Bill cl 40(1)(c).
[31] Scott, above n 28.

restriction of online material, the Government had chosen the most restrictive.[32] General concerns, relating to any media, about free speech protections, and the rights of adults to read, speak and hear what they choose, were commonly referred to, and statistics were quoted to show that the overwhelming majority of Australians supported such rights.[33]

Furthermore, this legislation came in the wake of the decision in the United States case of *Reno v ACLU*,[34] which had considered at length the issue of free speech as it related to the internet.[35] That decision was particularly salient to those arguing against internet content regulation in Australia, as it held that internet communications required and deserved free speech protections as much as any other medium. Consequently the United States Supreme Court had struck down the *Communications Decency Act*, the first US legislation enacted to restrict internet content unsuitable for minors.[36] The reasoning in that decision was used to support arguments against content regulation in Australia. Issues such as the danger of collateral censorship, whereby ISPs or ICHs, unable themselves to correctly classify material, might refuse to carry or host material about which they were uncertain, or agree voluntarily to take-down material without the material actually being classified, were raised. The court in *Reno* had anticipated that collateral censorship was likely to work particularly against non-commercial or smaller content providers,[37] who may have little power *vis a vis* ICHs, and may be unable to find hosts for their content even though it had not been classified. These

---

[32] D Lindsay, University of Melbourne, Centre for Media, Communications and Information Technology Law, *Censoring the Internet: The Australian Approach to Regulating Internet Content*. Research Paper No 9 (Nov 1999) 68. The EM presented 3 options: a) prohibiting RC material; b) prohibiting RC material, and X and R material not subject to an adult verification scheme; and c) prohibiting RC and X material, and R material not subject to an adult verification scheme. The last was included in the Bill.

[33] Electronic Frontiers Australia, above n 16. 'Despite the claims of moral crusaders that there is "wide community concern" to support the heavy-handed censorship they favour, surveys of Australian adults since at least 1992 have consistently shown vast support for the availability of X-rated (67%-83%) and R-rated material (72%-82%) to adults. These studies have been carried out by respected organisations including the OFLC and the ABA.' http://www.efa.org.au/Publish/senate99.html#7

[34] *Reno v ACLU* 117 S Ct 2329 (1997).

[35] Discussed further in Chapter Five: Censorship and freedom of speech.

[36] *Reno v ACLU* 117 S Ct 2329, 2347 (1997).

[37] *Reno v ACLU* 117 S Ct 2329, 2347 (1997).

and other concerns discussed in *Reno* were repeated in response to the proposed Australian legislation.[38]

Aligned to these free speech concerns were concerns over the classification system chosen for internet content. Internet content was to be classified as film under the National Classification Scheme, although the content often had little in common with film content. For example, even pure text on the internet would be classified under the more restrictive film classifications, rather than the less restrictive publications category.[39] Additionally, concerns were raised that restrictions on internet content would have repercussions for the medium itself, in a way that was not apparent in other media. For example, restricting a print version of Playboy would not change the nature of print communications, whereas restricting content on the internet, the last unregulated frontier, may change the very essence of the internet.[40]

Some of the above criticisms were dealt with in the final form of the legislation, and others were met in the drafting of the Industry Codes of Practice, which were required by the *Act* and were intended to work in conjunction with it. To address concerns that the Bill 'creates the impression that ISPs and ICHs are to bear the prime burden in relation to offensive material,' the Bill was amended to include the second and third components of the scheme, that is, the intended enactment of complementary State and Territory legislation, and the establishment of a community advisory body. Under the *Online Services Act* as passed, ICHs and ISPs were not required to make any classification judgments; the Australian Broadcasting Authority (ABA) and the Office of Film and Literature Classification (OFLC) were left with this responsibility, and ISPs and ICHs were required only to act upon ABA and OFLC decisions. Likewise, the *Online*

---

[38] See for example Electronic Frontiers Australia, above n 16 'Effects on Content Providers'.

[39] See for example Heath Gibson, 'Shooting the Messenger, A Critique of Australia's Internet Content Regulation Regime' (February 2000) No 10 *Issue Analysis - Centre for Independent Studies* [7] <http://www.cis.org.au/IssueAnalysis/ia10/ia10.pdf> at 25 June 2004.

[40] See for example Lawrence Lessig, 'Reading the Constitution in Cyberspace.' 45(3) Emory Law Journal (1996) footnote 63: 'Just at the point that we are understanding the power of this alternative world, the world is acting to turn the Web into an electronic version of this [real] world. Working, again, to replicate, only now more efficiently, all the structures of discrimination that real world zoning achieves. To some, the beauty of the net was just its escape from these zonings' 23. See also Chapter Two: The internet.

Services Act did not require vetting or monitoring of content by ISPs or ICHs, and required them to take action only once they were notified of such material by the ABA.[41] ISPs and ICHs were also excluded from civil liability if acting in accordance with an ABA notice.[42] Furthermore, while the legislation required ISPs to block access to content notified to them by the ABA, this was required only where no industry code was in place.[43] Where there was an industry code in place, compliance with that code would be sufficient.[44] The intended State and Territory legislation would ensure also that responsibility for provision or use of 'problematic' material would rest with those directly responsible, that is content providers and users, over whom the federal government had only limited power.

Although many concerns remained, some at least of the initial concerns had been allayed by the time the substantive provisions of the *Online Services Act* came into operation. This chapter now outlines these provisions, while the following chapters in this part look in more depth at the major elements of the online content control regime.

B. *The Provisions of the Act*

The *Online Services Act* was and is intended to operate through a system of co-regulation, whereby the Australian Broadcasting Authority (ABA) investigates and make decisions about internet content, and industry bodies develop codes or standards specifying the technical aspects of how those decisions are to be applied.[45]

---

[41] Supplementary Explanatory Memorandum (undated), Broadcasting Services Amendment (Online Services) Bill 1999 (Cth) Amendment 10. Amended (original) cl 20 to address concerns that the original wording 'might be read as implying that an Internet service provider is in some was responsible for the nature of that content available on the Internet.'
[42] *Broadcasting Services Act* 1992 (Cth) schedule 5 cl 88.
[43] Ibid cl 40
[44] Ibid.
[45] Discussed in more detail below, this chapter.

The ABA is given the power to investigate complaints made about online material,[46] and this complaints mechanism has been referred to as 'the cornerstone of the regulatory framework.'[47] The ABA also has power to investigate content of its volition,[48] although it was 'not intended that this discretion will be used to monitor content actively.'[49] Internet content is defined as information[50] kept on a data storage device, and accessed or available for access using an internet carriage service.[51] The initial Bill did not exclude email from the definition of internet content, due to the difficulty of distinguishing one-to-one email from e-mail with wider distribution.[52] Although the Government noted that it was unlikely in practice that private email would come to the ABA's attention,[53] this aspect of the Bill was amended during its passage so that 'ordinary electronic mail'[54] was specifically excluded. Ordinary electronic mail is not fully defined, except to exclude from its definition a posting to a news-group.[55] Information transmitted in the form of a broadcasting service is also excluded.[56]

Complaints may be made about prohibited or potential prohibited content accessible via the internet.[57] 'Prohibited content' is defined as Australian hosted R-rated material which is not subject to a restricted access system,[58] and all material rated X or RC.[59] 'Potential prohibited content' is unclassified content which, if classified, would be substantially likely to be prohibited content.[60]

---

[46] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 26.
[47] Senator Ian Campbell, above n 2, 3959.
[48] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 27.
[49] Senator Ian Campbell, above n 2, 3960.
[50] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 3. Definitions: Information; means information in the form of text, data, speech, music or other sounds, visual images (animated or otherwise) or in any other form or in any combination of forms.
[51] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 3. Definitions: Internet content.
[52] Senator Ian Campbell, above n 2, 3959.
[53] Ibid.
[54] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 3. Definitions: Internet Content.
[55] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 3. Definitions: Ordinary electronic mail.
[56] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 3. Definitions: Internet Content.
[57] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 22.
[58] A restricted access system is one which enables content to be accessed by adults, but not by children. Various means can be used for identifying adults (see also discussion of 'Zoning' in Chapter Three: Methods of content control). *Broadcasting Services Act 1992* (Cth) schedule 5 cl 4(1) gives the ABA power to declare a specified access control system is a 'Restricted Access System' for the purposes of the Act. In doing so, the ABA must take into account 'the objective of protecting children from exposure to Internet content that is unsuitable to children.' cl 4(2).
[59] Ibid cl 10.
[60] Ibid cl 11.

Where the ABA identifies internet material which is, or is likely to be classified R, X, or RC, the action to be taken by the ABA depends on whether the material is hosted in Australia or is hosted overseas.

1. Material hosted in Australia.

The ABA may issue interim take-down notices to Australian sites hosting what is believed to be X or RC material, and refer such material to the Office of Film and Literature Classification (OFLC) for classification[61] under the guidelines used for rating films.[62] Material hosted within Australia and believed to be R-rated is not subject to interim take-down orders, as it is generally of a less serious nature than X or RC material, and issuing interim orders for such material may substantially increase both the ABA's administrative costs and the industry's compliance costs.[63] However, the ABA will still refer such material to the OFLC for classification.[64]

The ABA may revoke its notices, or issue final take-down notices, depending on the classification which the material receives, whether there has been a voluntary take down of the material,[65] and in the case of R-rated material, whether or not an approved restricted access system is in place.[66] The ABA may also issue notices for removal of material 'substantially similar' to that which is the subject of such a notice.[67]

2. Material hosted outside Australia.

Where the ABA is satisfied that material hosted outside Australia is prohibited content (that is X or RC material), two possibilities arise. In the absence of an

---

[61] Ibid cl 30.
[62] Ibid cl 13, except computer games which are to be classified as computer games, cl 12.
[63] Senator Ian Campbell, above n 2, 3957
[64] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 30(2)(b).
[65] Ibid cl 33. Where a content host voluntarily removes content in response to an interim take-down notice, and gives an undertaking not to host that material, the ABA may dispense with classification of that material. This means however that hosts may simply agree to remove any such content, even though it may not in fact breach any regulations.
[66] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 30(2)(b).
Ibid cl 32-35, 42-45.
[67] Ibid cl 36, 46–47. These anti-avoidance provisions were inserted to stop ICHs or content providers from minimally altering content and then re-hosting it.

industry code dealing with the topic, the ABA may issue a standard access prevention notice requiring ISPs to 'take all reasonable steps to prevent end users from accessing the content,'[68] but where a relevant industry code of practice has been registered ISPs must comply instead with that code. This provision led to desperate drafting and re-drafting of industry codes in an attempt to have them registered before January 2000, when the substantive provisions of the Act came into effect. As the codes were in fact registered in time it is still unclear what 'all reasonable steps' may have entailed, but it was precisely this type of requirement which the internet industry was concerned about in the lead up to the operation of the *Online Services Act*.

Under the Internet Industry Codes of Practice currently registered[69] ISPs will be notified of overseas-hosted prohibited content via a Designated Notification Scheme,[70] and must then provide an approved filter to subscribers.[71] In the case of commercial subscribers ISP's must provide appropriate software (which may be an approved filter) or facilitate access to a consultancy service with respect to appropriate technology.[72] Provision of filters and access to consultancy services is not required where subscribers already have in place alternative access prevention arrangements such as firewalls.[73] R-rated material housed overseas will not be subject to blocking under the *Act,* although the inclusion of such material was specified in the *Act* as something to be examined during the required three-year review of the legislation.[74]

---

[68] Ibid cl 40(1)(c).
[69] Internet Industry Codes of Practice, registered by the ABA 16 Dec 1999, for implementation from 1 Jan 2000.
[70] Ibid, Code 2. 6.1.
[71] Ibid Code 2. 6.2.
[72] Ibid.
[73] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 60(3) and Internet Industry Codes of Practice: Code 2. 6.3 & 2. 6.4.
[74] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 95(2)(b). Under cl 95(1) the Minister must cause a review of the *Act* to be conducted before 1st January 2003. The Review was completed in May 2004, and is discussed further in Chapter Twelve: Statistics and Perceptions.

3. Penalties.

Those sections of the *Online Services Act* requiring content to be taken down or access to content prevented are defined as 'online provider rules.'[75] A contravention of the 'online provider rules' carries a penalty of 50 penalty units (currently $5500) for an individual, or up to 5 times that for a corporation.[76] The *Act* also provides that the ABA may direct a provider to take action to avoid contravening the online provider rules (a breach of such a direction also carries a penalty of 50 penalty units),[77] or may issue a formal warning to those in breach.[78] The Federal Court may also order a person found to be supplying or hosting internet content in contravention of the online provider rules to cease supplying the contravening internet carriage service or to cease hosting that content in Australia.[79]

4. General provisions

The ABA is also empowered to register appropriate industry codes,[80] and to draft codes or industry standards where there is no relevant industry body, where the industry body has not done so, or where the ABA believes that the code or standard is deficient.[81] The ABA must also monitor compliance with such codes or standards.[82] Further, the ABA is given power to approve restricted access systems (RAS)[83] behind which Australian R-rated material must be housed.

Not all of the powers given to the ABA under the Act are however so technical. Further functions include advising and assisting parents and adults in relation to supervision and control of children's internet access, conducting and co-ordinating community education programs, conducting and commissioning research into related issues, liaising with regulatory and other bodies involved in

---

[75] *Broadcasting Services Act 1992* (Cth) schedule 5 cl 79 states that rules set out in cl 37(1),(2),(3),&(4), 48(1) & (2), 66(2), 72, and 80 are 'online provider rules.'
[76] Ibid cl 82.
[77] Ibid cl 83.
[78] Ibid cl 84.
[79] Ibid cl 85.
[80] Ibid cl 62.
[81] Ibid cl 68-71.
[82] Ibid cl 94(a).
[83] Ibid cl 4.

the internet industry, and gathering information on technological developments and service trends in the industry.[84]

Industry codes likewise are required to cover more than just the technical aspects of content regulation. They should deal also with topics such as advising and assisting parents and responsible adults in relation to supervision and control of children's internet access, giving content providers information about their legal responsibilities, and informing users of complaints procedures regarding online content.[85]

5. Further provisions.

Following amendments while the Bill was before Parliament,[86] the Government's scheme for regulation of online services included two further aspects; firstly, complementary State and Territory legislation, and secondly, the establishment of a community advisory body. These were referred to in the *Online Services Act* as the second and third components of the proposed regulatory scheme for internet content.[87]

(a) Complementary state and territory legislation:

As discussed above the federal parliament has only limited powers to enact legislation, and any enactment must fit within the power specifically granted under the Commonwealth Constitution.[88] Therefore, while the Commonwealth had some power to legislate to restrict the carriage and hosting of specified content, it has no general censorship power, nor power to restrict individuals from creating, uploading, downloading, or possessing the content about which it was concerned. Thus it was necessary, if the scheme were to be more roundly effective, for States and Territories to enact complementary legislation. The second component of the proposed scheme was thus State and Territory laws to

---

[84] Ibid cl 94.
[85] Ibid cl 60.
[86] See Supplementary Explanatory Memorandum (undated), Broadcasting Services Amendment (Online Services) Bill 1999 (Cth), Amendment 5.
[87] *Broadcasting Services Act* 1992 (Cth) schedule 5 cl 1(3) and 1(4).
[88] Chapter Five: Censorship and Freedom of speech, and Chapter Six: Regulatory background.

cover producers of content,[89] and persons who upload or access content.[90] This component of the scheme was intended to ensure a uniform national approach to online content regulation, and to stop the fragmentary regulation of the internet in Australia which had been occurring prior to the enactment of the *Online Services Act*, and which could have had an 'adverse effect on the development of the online industry.'[91] Such legislation was intended to 'supersede online services specific legislation currently in place...'[92] This component of the scheme also included amendment to the Commonwealth's own *Crimes Act.*[93]

(b) Community Advisory Body

The third component of the scheme was a range of non-legislative initiatives directed towards monitoring content on the internet,[94] and educating and advising the public about content on the Internet.[95] It was envisaged that a body set up for this purpose would also operate a hotline to receive complaints about illegal material, and advise the public about options, such as filtering software, available to control online content.[96] The community body in fact established was NetAlert, which carries out a number of these functions, although the *Online Services Act* itself specifies that the receipt and investigation of complaints is the responsibility of the ABA.[97] Many of the other functions carried out by NetAlert overlap with those carried out by the ABA.

After the enactment of the *Online Services Act*, industry Codes of Practice were registered, the complaints process begun, attempts were made to introduce State and Territory legislation, and NetAlert was formed to provide community education regarding the internet. Each of these will be examined in turn in the following chapters.

---

[89] *Broadcasting Services Act* 1992 (Cth) schedule 5 cl 1(3)(a)(i).
[90] Ibid cl 1(3)(a)(ii).
[91] Senator Ian Campbell, above n 2, 3958.
[92] Ibid 3958.
[93] *Broadcasting Services Act* 1992 (Cth) schedule 5 cl 1(3)(b).
[94] Ibid cl 1(4)(a).
[95] Ibid cl 1(4)(b).
[96] See Supplementary Explanatory Memorandum (undated), Broadcasting Services Amendment (Online Services) Bill 1999 (Cth), amendment 5.
[97] *Broadcasting Services Act* 1992 (Cth) Schedule 5 cl 22-26..

CHAPTER EIGHT: INDUSTRY CODES OF PRACTICE

A. *Requirements and drafting of the Codes of Practice*

The clearest and most immediate effect of the *Online Services Act* was the registration of the Internet Industry Codes of Practice, drafted by the Internet Industry Association.[1] Part 5 of the *Online Services Act* provides for the drafting of Codes of Practice by bodies or associations which the ABA is satisfied represent the content host and internet service provider industries,[2] and outlines the topics which the Codes should and should not cover.[3] The Government intentionally did 'not mandate any particular technological solutions' in the *Online Services Act*; rather, it detailed its various aims but left it to the internet industry itself to determine how those aims may best be met.[4] The Government considered that industry drafting would 'best utilise industry expertise in the development of workable and practical codes of practice, with which compliance is more likely...'[5] As discussed above in Chapter Six, regulation of this type is in no way confined to the internet industry, and has in fact been a preferred approach in Australia for a number of years.

The ABA accepted the Internet Industry Association (IIA) as a sufficiently representative body to negotiate and draft Codes of Practice for the industry. The IIA is a '"national" industry association,'[6] and its ISP and ICH members, which include the industry's largest players such as Telstra and Optus, account for the majority of Australian internet users.[7] However, the IIA's membership is so

---

[1] The Internet Industry Association calls itself the '**architect** and **implementer**' of the Internet Codes of Practice registered by the ABA. Internet Industry Association, *Submission to Review of the Operation of Schedule 5 Broadcasting Services Act 1992* (November 2002) 2, emphasis in original.

[2] *Broadcasting Services Act* 1999 (Cth) schedule 5 cl 59(1), 59(2).

[3] Ibid cl 60, 61

[4] Broadcasting Services Amendment (Online Service) Bill 1999, Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 21 April 1999, 3957, 3961 (Senator Ian Campbell, Parliamentary Secretary to Senator Alston, Minister for Communications, Information Technology and the Arts).

[5] Ibid.

[6] Internet Industry Association, above n 1, 2.

[7] Australian Broadcasting Authority, *Submission to Review of the Operation of Schedule 5 Broadcasting Services Act 1992* (November 2002) 5.

diverse that it would be difficult really to name the 'industry' it represents. It includes for example city councils, accountants, banks, universities, and many law firms, as well as members who may be thought of more specifically as the 'internet industry.'[8] Further, many of those who *are* in the 'internet industry' are *not* members of the IIA.[9] There have also been concerns that more grass-roots industry associations have found it difficult to be heard in negotiations since the IIA's establishment in 1996, as the ear of government seems tuned to the IIA.[10] Nevertheless, by 1999 the IIA was certainly seen by the ABA and the Government as the appropriate body to represent the internet industry.

While the IIA had been drafting and re-drafting industry codes for over 4 years without reaching agreement on a final version, the *Online Services Act* forced the urgent finalisation of these Codes. To ensure the making of such codes, the *Act* made provision for the ABA itself to determine industry standards if the industry had no sufficiently representative body, or if the industry body did not draft codes of its own volition or on the ABA's request. To avoid the external imposition of such standards, which the legislation - combined with Government rhetoric - suggested may be extremely burdensome for the industry, the IIA undertook frenzied consultation and drafting and re-drafting,[11] leading to the registration of the Industry Codes of Practice just a fortnight before the substantive provisions of the *Online Services Act* came into force.[12]

The acceptance by the ABA of the industry Codes of Practice proffered by the IIA was a huge relief to many in the internet industry, and claimed as a great success

---

[8] A list of IIA members can be found at <http://www.iia.net.au/members.html> at 23 June 2004

[9] It is unclear why the IIA was seen by the ABA as a sufficiently representative body to draft and register Industry Codes under s 62 of the OSA, and to monitor performance with those codes. According to research undertaken by the Communications Law Centre on behalf of NetAlert, of industry members participating in industry awareness seminars, only 35% reported membership of any industry association, and only a quarter of those listed the IIA as the industry group to which they were affiliated. That is, less than one tenth of respondents were members of the IIA. Communications Law Centre, 'NetAlert Internet Industry Liaison Project Final Report' 20 August 2001, 18.

[10] For further discussion of this see Kimberley Heitman, 'Vapours and Mirrors' (March 2000) 6 (1) *UNSWLJ Forum, Internet Content Control* 6(1) 31-32.

[11] Telephone conversation between author and Peter Coroneous, chairman of IIA, Dec 1999.

[12] Internet Industry Codes of Practice, registered by ABA 16th Dec 1999.

for the IIA.[13] Government rhetoric, and the wording of the legislation itself, had suggested that the *Act* was intended to have the effect of prohibiting access to RC and X-rated material, and of regulating access to R rated material, on the internet. What was not clear however was whether effective prohibition and regulation was to take precedence, or whether it was required only if it could be achieved by an efficient, economically viable and happy internet industry. The ABA's registration of Codes which allowed industry compliance without any need to monitor local content, or to prohibit or regulate access to overseas-hosted content, suggested the latter. In one fell swoop it removed the extremely onerous responsibilities potentially falling on the industry under the *Online Services Act*, and replaced these with easily complied with Codes of Practice.

B. *Provisions of the Codes of Practice.*

Three Codes for internet content are registered by the ABA. These are Content Code 1: ISP obligations in relation to internet access generally; Content Code 2: ISP obligations in relation to access to content hosted outside Australia; and Content Code 3: Internet content host obligations in relation to hosting of content within Australia.[14]

Under the Codes, internet content hosts within Australia have no responsibility for monitoring content. Code 3 requires ICHs only to remove content notified by the ABA as prohibited or potentially prohibited, and to remove or make R-rated content subject to a restricted access scheme.[15] In the first four years of the scheme's operation, 312 'take-down' notices were issued for Australian hosted

---

[13] 'Amendments to the legislation negotiated largely by the IIA now provide for the creation of an alternate regime ... These sections provide for measures which the IIA believes are reasonable, having regard to issues such as technical and commercial feasibility and effect on network performance. When implemented they will avoid most, if not all, of the negative consequences which some commentators were predicting would result from the legislation.' <http://www.iia.net.au/index2.html> (document no longer available 29 July 2004)

[14] Codes are available at <http://www.aba.gov.au/internet/industry/codes/content/index.htm> at 21 February 2005.

[15] Internet Industry Codes of Practice: Content Code 3. 7.9.

content.[16] As there is no jurisdiction for enforcing such 'take-down' notices beyond Australia, overseas hosted content was treated differently.

Code 2 deals with ISPs and overseas hosted content. As discussed above in Chapter Seven, the Act itself provides that the ABA may issue a standard access prevention notice requiring ISPs to 'take all reasonable steps to prevent end users from accessing the content,'[17] but where a relevant Code of Practice has been registered ISPs must instead comply with that code. The relevant registered code[18] provides that ISPs will be notified of overseas-hosted prohibited content via a Designated Notification Scheme,[19] and must then 'provide for use' an approved filter to subscribers.[20] In practice neither 'provision' nor 'use' has been required. ISPs 'offer' a filter, but there is no requirement that subscribers either accept a filter, or use one. Further, filters are generally offered to subscribers upon subscription, not in response to the notification of prohibited content.[21] Thus there is no apparent connection between the notification of prohibited content and the prevention of access or offering of filters. While the *Act* envisaged ISPs taking steps to prevent end-user access to specific content, the Code waters this down so far that ISPs may in fact delegate any desired access prevention to subscribers who choose to use it.

The industry Codes of Practice did introduce some other minor responsibilities. ISPs, for example, need to ensure accounts are not provided to those under 18 without the consent of a parent or guardian.[22] They must encourage the use of

---

[16] ABA complaints statistics. Take-down notices issued Jan 2000 to Dec 2002: 297, Jan to Dec 2003: 15 < http://www.aba.gov.au/internet/complaints/statistics/pre2003.htm > at 29 July 2004.
[17] *Broadcasting Services Act* 1999 (Cth) schedule 5 cl 40(1)(c).
[18] Internet Industry Codes of Practice, registered by the ABA 16 Dec 1999, for implementation from 1 Jan 2000. Now updated to Code version 7.2 Registered May 2002 <http://www.iia.net.au/contentcode.html> at 29 July 2004.
[19] Internet Industry Codes of Practice: Content Code 2. 6.1.
[20] Ibid 2. 6.2(a).
[21] This is acceptable according to Internet Industry Codes of Practice 2. 6.3: 'Provision for use includes the provision of a Scheduled Filter as part of an online registration process, and in the case of user installable filters, links to effect download activation and instructions for use; a disk based registration process; or a notification containing, in the case of user installable filters, links to effect download activation and instructions for use.'
[22] Internet Industry Codes of Practice Code 1: 5.1

content labeling systems[23] consistent with the National Classification Code,[24] inform subscribers who are content providers of their legal responsibilities in relation to internet content,[25] and provide users with information about and procedures for supervising and controlling children's access to internet content.[26] ISPs are required also to inform their users about their right to make complaints to the ABA regarding Prohibited Content or Potential Prohibited Content, and about the procedures by which such complaints to the ABA can be made.[27] ISPs need also to have procedures in place to deal with complaints relating to spam.[28] Requirements for ICHs are very similar.[29]

C. *Compliance with Codes of Practice.*

Given how minimal the requirements of the Codes are, it is not surprising to see the ABA reporting high rates of compliance. By December 2000 all major ISPs were said to be complying fully with the industry Codes, and 78% of the smaller ISPs who responded to an IIA survey also reported full compliance.[30] By September 2001 the IIA reported continuing full compliance for major ISPs, and a compliance rate of 85% for smaller ISPs.[31] The only later report on the scheme, for the period to Dec 2002, does not include compliance statistics.[32] An small independent survey of 25 ISPs servicing the Melbourne area in October and

---

[23] Labeling schemes are discussed in more depth above, Chapter Three: Methods of internet content control.
[24] Internet Industry Codes of Practice Code 1: 5.2(a).
[25] Ibid Code 1: 5.2(b)
[26] Ibid Code 1. 5.3.
[27] Ibid Code 1. 5.5.
[28] Ibid Code 1. 5.7. Note that this is still a code requirement, but new SPAM specific legislation has also been introduced; see *SPAM Act 2003* (Cth).
[29] Internet Industry Codes of Practice Code 3.
[30] *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2000* (Second period) (April 2001) 8. Tabled by the Minister for Communications, Information Technology and the Arts.
[31] *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2001*(Third period) (February 2002) 1. Tabled by the Minister for Communications, Information Technology and the Arts.
[32] *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2001*(Fourth period) (August 2002) 7. Tabled by the Minister for Communications, Information Technology and the Arts.

November of 2002 likewise found claims of high compliance, with all but four respondents claiming to be code compliant.[33]

The figures look excellent. They raise two questions however. Firstly, on what basis are such claims made about compliance? Secondly, even if there is high compliance with industry Codes, what effect does that have? Does it help to fulfill the government's stated aims in enacting this legislation?

While the ABA carried out some investigation of its own with the larger ISPs, its reports suggest it relied generally on the IIA for information regarding Code compliance. The ABA report states 'the IIA advised the ABA that all major Internet service providers who are IIA members continue to be fully compliant with the codes. ...compliance for smaller providers increased... with 85% of those surveyed reporting full compliance.'[34] The IIA has indeed surveyed ISPs regarding compliance with the Codes, but at least one of its surveys was prefaced thus: 'There are political reasons why a positive response will be helpful at this stage.' The survey was footnoted: 'Until we can get a repeal or substantial amendment to this ill-conceived law, compliance with these comparatively minimal obligations ... will avert any temptation for a tightening of the regime.'[35] Such comments alone may lead to some concern about the objectivity of the figures reported. Do such comments discourage responses from those who cannot report compliance, and encourage responses only from those who can report compliance? Unfortunately, the extent of any skewing of results cannot be gauged, as the IIA refuses to release the data on which its reporting is based. It is quite unclear how many responses were gathered in the survey, and whether the 85% compliance is 85% of 5, 50 or 500 respondents. The figures may be accurate, but give little insight into actual industry Code compliance. Further, despite

---

[33] Peter Chen, *Survey of Small ISPs in the Melbourne Area* (October 2002) within Peter Chen, Centre for Public Policy, University of Melbourne, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (October 2002) 12. Discussed further below, Chapter 12: Statistics and Perceptions.

[34] *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2001*, above n 31.

[35] Email from Peter Coroneos (Executive Director of IIA) to IIA members, 8 July 2000.

requests to both organizations, the IIA and the ABA refuse to release the report made by the IIA to the ABA regarding compliance.[36]

As may be expected, the ABA accepts the verity of the IIA report, unless there is some reason not to.[37] The ABA has had no complaints regarding non-compliance with the Codes, and does not further investigate the IIA's report, particularly given that the IIA is (or appears to be) in a better position than the ABA to gather relevant information.[38]

That the ABA has had no reports of non-compliance leads into the second question; does compliance make any difference to the industry, to consumers, or to online content? While the ABA has received no complaints regarding Code of Practice compliance, lack of compliance by several ISPs 'came to the ABA's attention,' which led to meetings between the ABA and ISPs, and a prompt resolution of the issues at hand.[39] Why did no-one complain to the ABA regarding non-compliance? Does no-one care whether or not the Code is complied with? Would there be any reason to complain about non-compliance? It is unclear whether the lack of reported non-compliance is due to high compliance rates, or to the irrelevance of non-compliance.

Given how easy it is for ISPs and ICHs to comply with the internet industry Codes of Practice, it would not be surprising if compliance rates were, as stated, very high. But even if this is so, have the Codes made any difference? In reporting on the Codes of Practice, the ABA reports focus solely on compliance, and do not attempt to address what the effects of the Codes might be, nor whether

---

[36] An ABA officer suggested to the author that an FOI application for the report would be the appropriate way to gain access. Richard Fraser, Acting Manager, Online Services. Telephone conversation with the author, 21 November 2001.

[37] Fraser, above n 36. More recently the ABA has said that it focuses on compliance by the largest ISPs as they cover the majority of Australian users. No complaints have been received, and non compliance issues which have arisen have been dealt with satisfactorily. Email to the author from Mike Barnard, Hotline Manager, Content Assessment, ABA.. 28 June 2004.

[38] Fraser, above n 36

[39] Australian Broadcasting Authority, *Annual Report 2001 – 2002* (2002) 47. There is no indication in the report of how the lack of compliance may have come to the attention of the ABA. The only later annual report, 2002-2003, does not discuss code compliance in any detail, merely stating that the ABA 'monitors compliance with the codes and may direct an ISP or ICH to comply with a code...' ABA, *Annual Report 2002 – 2003* (2003) 45.

compliance actually goes any way toward achieving the desired effects of the *Online Services Act.* The IIA itself has not reported publicly either on statistics for Code compliance, or on the effect the Codes might have.

The Code requirement that internet account holders are over 18 or have parental consent is unlikely to have greatly changed people's behaviour. Most large providers required adult signatures to open accounts even before the Codes came into effect.[40] The Code requirement for the provision of filters and filtered services would also have made little difference, as filters and filtered services were readily available to consumers prior to the advent of the Codes of Practice. The Codes may however make it easier for subscribers to access information about filters.[41] There is no evidence that filters are widely, or more widely, used now than prior to the *Act* and Codes.[42]

The Codes also require the provision of information to consumers, about, for example, how to supervise and control children's access to internet content,[43] how to make complaints about content, how to make complaints about unsolicited material promoting prohibited content etc. To meet this requirement many service providers are linking from their home pages to IIA, ABA and Net Alert information pages, and / or providing their own information for subscribers. It has been suggested however that this has not been highly effective, with few users identifying ISPs as a source of internet information. [44]

---

[40] Emails from Optus@home to author, (23 Novemeber 01), AOL 23 November 01, telephone conversation with Telstra BigPond (Darren, 6 December 01).

[41] Discussed further below, Chapter Twelve: Statistics and perceptions.

[42] In fact there is an absolute dearth of knowledge in this area. Neither the ABA, IIA, NetAlert, nor even the Report of the Review of the Operation of Schedule 5 to the *Broadcasting Services Act* 1992 gives any information or even estimate as to the proliferation of filtering. In August 2000 17% of parents reported using filtering Internet@home, December 2001 p48; in June 2000 15% of public libraries were using or trialling filters or had blocked specific sites; in May 2002 Telstra Bigpond claimed there was little interest in filtering, even when free trials were offered. Steven Wardill, Consumer Affairs Reporter, 'Code to push Internet porn out of reach' *Courier Mail* 13 May 2002, quoted in Electronic Frontiers Australia Inc, Submission to *Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 21 of 27. Filters are also often sold as part of larger IT packages, bundled for example with virus filters / security software, and thus even data re *sales* of filter products would give little information as to filter *use*.

[43] Discussed below, Chapter 11: Community Education.

[44] Australian Broadcasting Authority, *Internet@home.* (December 2001) 73 <http://www.aba.gov.au/internet/research/home> at 24 June 2004. After set-up, subscribers rarely access ISP home pages however. This has been noted in the Report of the Review of the Operation

The registration of Codes of Practice which required neither monitoring nor blocking of content by industry could suggest that the Government's aim was largely symbolic; that is, that it intended to give the impression that internet content control would be brought into line with content control in other media, while the reality was much different. Much more could have been required under the Codes to control access to content. ICHs could have been required to monitor content, and ISPs could have been forced to block content. However, each of these would have placed a heavy burden on industry. The *Act* required that the industry should not bear unnecessary financial or administrative burdens,[45] and in this case the balance appears to have fallen in favour of industry.

The introduction of industry Codes of Practice has been a major effect of the *Online Services Act*, but the value of these Codes of Practice is questionable. As part of the examination of the provisions and operation of the online services regime, this chapter has aimed to explain the internet industry Codes of Practice, responsibilities they place on the internet industry, and compliance issues. More detailed discussion of the possible effect of these Codes takes place in Chapter Twelve, but before that the thesis looks to other direct effects of the scheme; the complaints regime, State and Territory legislation, and community education.

---

of Schedule 5 to the *Broadcasting Services Act* 1992 (May 2004) and is discussed in more detail below in Chapter Fifteen: Recommendations and Chapter Sixteen: Conclusion.

[45] *Broadcasting Services Act 1992 (Cth)* s 4(3)(a).

CHAPTER NINE: COMPLAINTS – PROHIBITIED AND POTENTIAL PROHIBITED CONTENT.

Within the system for controlling internet content, the complaints scheme was seen as 'the cornerstone of the regulatory framework.'[1] Indeed, the first listed objective of the *Act* is to 'provide a means for addressing complaints about certain internet content,' and it is these complaints about specifically identified content which are intended to trigger investigation, classification, and restriction of content. The government did not intend that pro-active investigation or classification should occur.[2] This allayed to some extent concerns that ISPs and ICHs would be required to monitor content, or that content would be subject to pre-classification.[3]

Part four of the *Online Services Act* allows complaints to be made to, and investigated by, the ABA. Complainants must be Australian residents, bodies corporate with activities in Australia, or the Commonwealth, a State or Territory.[4] No reasons are given for this restriction on potential complainants. It may be simply a desire to place some limit on complaints which can be received, but if content control is the aim, it would be appropriate at least to accept complaints from anywhere in the world if it is Australian hosted content which is complained about. Allowing complaints from the persons specified in the legislation, *or* from any person or body if relating to Australian based content, would appear a far more appropriate limitation.

---

[1] Broadcasting Services Amendment (Online Service) Bill 1999, Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 21 April 1999, 3959 (Senator Ian Campbell, Parliamentary Secretary to Senator Alston, Minister for Communications, Information Technology and the Arts).
[2] Ibid 3960.
[3] The ABA does have power to investigate of its own volition, and has done so for example in response to reports from overseas hotlines, and a media report regarding accessibility of RC internet material. Australian Broadcasting Authority, *Annual Report 2001-2002* (2002) 48.
[4] *Broadcasting Services Act 1992* (Cth) schedule 5, s 25. But note fourth *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2001* Tabled in Senate by the Minister for Communications, Technology and the Arts (August 2002) 8 'The ABA's hotline enables any person to complain to the ABA if they believe Australians can access prohibited or potentially prohibited content...'

As discussed above, the legislation initially envisaged the removal of prohibited and potentially prohibited material from Australian sites, and the blocking of such material hosted overseas. However, under the registered internet industry Codes of Practice, while take-down notices are issued to Australian hosts, no blocking of overseas hosted material occurs. Instead material should be notified to the makers of scheduled content filters, who have undertaken to include notified sites in their filter block lists,[5] and notified to ISPs, who must then offer a filter or filtered service to providers.[6] The latter has no effect. As discussed in the previous Chapter, filters are not offered in response to notification, but are offered more generally, and usually upon subscription rather than upon notification to an ISP of specific content. In addition to issuing take-down notices to ICHs and notifications to ISPs and filter makers, when ABA investigations find prohibited material of a 'sufficiently serious' nature – such as child pornography, paedophilia, and possibly other criminal matter – the content is referred to law enforcement agencies. This may occur whether the material is hosted within Australia or overseas.

A. *Complaints statistics*

Given that the complaints regime is the 'cornerstone' of the content control scheme, and is in fact the trigger for all enforcement aimed at limiting accessibility or availability of problematic internet content, a detailed examination of it is worthwhile. Statistics inform us of the quantity of complaints, the types of content being complained about, what investigations have revealed, and what has been done in response to those complaints and investigations. Reporting on the complaints scheme also reveals something about ABA and Government attitudes to the scheme.

---

[5] See for example first *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000* Tabled in Senate by the Minister for Communications, Technology and the Arts (September 2000) 9, 16.

[6] Although this action is envisaged under the *Act* it does not appear to occur. Reports refer only to notification to filter makers in relation to overseas hosted prohibited or potentially prohibited content.

Some of the following figures may appear outdated. However, some early data is specifically included as it is important in explaining the issues which have arisen in relation to complaint and investigation 'reporting.' Other figures may be out of date due to a lack of reporting on the scheme by the ABA. At the time of writing[7] detailed figures were available only for the period to December 2002, while less detailed figures were available for the more recent period.

In the first 3 years of operation[8] 1619 complaints about internet content were lodged with the ABA, leading to completed investigations of 1354 complaints within the same period.[9] Some complaints were dismissed as vexatious or frivolous, some failed sufficiently to identify the material complained about, and some were still under investigation at the end of the reporting period. As a result of the 1354 investigations completed over that period, 'action' was taken in relation to 1377 items of content.[10]

Outcomes of investigations into Australian-hosted and overseas-hosted content are reported separately by the ABA, due to the differentiation in the scheme depending on host location. The action taken in relation to Australian hosted prohibited or potentially prohibited items was to order the material to be removed from the host, and this occurred for a total of 297 Australian-hosted items.[11] Almost one third of those items ordered to be removed were or would have been rated R or X,[12] and thus the content was legal to possess in Australia. Two thirds of items ordered removed were or would have been refused classification within Australia,[13] and over one half of those items were classed as child pornography or paedophile activity.[14] While the ABA reported that all content was removed in

---

[7] This thesis is current to 1 June 2004.
[8] 1 Jan 2000 to 31 Dec 2002
[9] These figures are taken from the ABA website <http://www.aba.gov.au/internet/complaints/statistics/pre2003.htm> at 25 December. Internet Content Complaints - 1 January 2000 to 31 December 2002. It is assumed these figures are corrected figures and thus differ from figures given in initial reports, discussed further below.
[10] Internet Content Complaints - 1 January 2000 to 31 December 2002. Found on ABA website, ibid.
[11] Ibid.
[12] Ibid 95 of 297.
[13] Ibid 202 of 297.
[14] Ibid 127 of 202, and 42% of total prohibited and potentially prohibited Australian hosted content i.e. 127 of 297.

accordance with the notices issued, even the ABA conceded that some content moved to overseas hosts, and so remained accessible in Australia.[15] Further, where take-down notices are issued in relation to newsgroup postings hosted in Australia, the notice is issued only to the complainants' ISP, and hence the same material remains available on any other Australian servers carrying that newsgroup.[16]

The ABA of course has no jurisdiction over hosts located overseas, and thus cannot order problematic content hosted outside Australia to be removed. As discussed above, Australian ISPs are not required, under the currently registered Industry Codes of Practice, to take any action in relation to overseas material, and thus the ABA merely reports the outcome of its investigations to the makers of filter products 'scheduled' under the Codes. Such filter-makers include only those who have undertaken to add content so notified to their block lists.[17]

The ABA has notified 1080 items of overseas hosted internet content to filter makers as a result of complaints and investigations.[18] Two hundred and thirty (twenty two percent) of those items were or would have been classified X in Australia,[19] while 850 were or would have been refused classification.[20] Of the latter, seventy two percent were classed as child pornography or paedophile activity.[21]

During the same period the ABA also passed information to police relating to prohibited internet content of a 'sufficiently serious' nature. In the first two years

---

[15] See for example first *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000*, above n 5, 16 at note 2.
[16] Electronic Frontiers Australia *Hoodwinking the Public: Australia's Internet Censorship Regime* (November 2002) <http://www.efa.org.au/Publish/bsa_analysis2002.html> At 25 June 2004. And note Australian Broadcasting Authority, *Submission to Review of the Operation of Schedule 5 Broadcasting Services Act 1992* (November 2002) 25 'The requirement that the ABA be satisfied that an ISP is hosting such content prior to issuing a take down notice limits the ABA's capacity to take action in relation to content that may be simultaneously hosted by many ISPs.'
[17] See for example first *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000* above n 5, 16 note 2.
[18] Internet Content Complaints - 1 January 2000 to 31 December 2002. Found on ABA website, above n 8.
[19] Ibid 230 of 1080.
[20] Ibid.
[21] Ibid 614 of 850.

of the scheme's operation 132 items hosted within Australia were referred to State and Territory police forces, and 352 items hosted overseas were referred to the Australian Federal Police.[22]

B. *Problems with complaints statistics*

The statistics given by the ABA look both straightforward and pleasing. Complaints are being made as envisaged by the scheme, and the ABA is taking action and dealing with the problematic internet content. But a number of concerns arise.

Firstly, the ABA failed in its reporting to differentiate complaints it received under the *Act* which led to findings of prohibited content, from complaints it received from overseas hotlines and other sources. As a result it was unclear how much of its finding of prohibited content in fact resulted from complaints made under the scheme.[23] This makes it difficult to assess the success, or value, of the complaints scheme set up by legislation.

Secondly, ABA reports did not differentiate content ordered removed from the World Wide Web from content ordered removed from news groups. Where take-down orders were issued for the latter, these were issued only to the ISP of the complainant, while the same content carried by numerous other Australian ISPs was unaffected. The suggestion that a take-down notice relating to news group content led to the content being removed from Australian hosts in the same way as removal of WWW material, could thus distort understanding of the real effect of the take-down notices.[24]

---

[22] Figure aggregated from first four *Six Month Report(s) on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000* (September 2000), *July to December 2000* (April 2001), *January to June 2001* (February 2002), *July to December 2001* (August 2002).
[23] See discussion of this in Electronic Frontiers Australia, above n 15.
[24] Ibid.

Thirdly, the ABA has been accused of substantial manipulation of the figures it had reported. For example, although during the whole of the year 2000 only 22 items hosted in Australia were found to be prohibited or potential prohibited content,[25] 129 take-down notices were issued to Australian hosts during the year.[26] In the second half of the year only 6 of the complaints received by the ABA related to Australian hosted prohibited or potentially prohibited content, yet the ABA report states that 67 take-down notices were issued during that time,[27] and 45 items were referred to State and Territory police.[28] The expanding nature of the figures, that is, the very few complaints leading to far more take-down notices and referrals to police, raised concerns that reported figures were being manipulated to make the scheme appear more effective than it perhaps was. Electronic Frontiers Australia for example referred to 'the exploding statistics phenomenon,' and to the use of 'creative statistics' by the ABA.[29] Figures given for referrals to police may in fact include multiple referrals, for example the same one item may be referred to a number of different police forces, and thus increase the figure given for referrals beyond the items of content in fact referred.[30] Further, in response to questioning, the Minister responsible stated that one complaint may lead to investigation of a site which included many pages, each one of which would be reported as an 'item' ordered removed or referred to filter makers.[31] For this reason alone, the six complaints received in the second half of 2000 might have generated 67 take-down notices!

In addition to these expanding figures, there were also mistakes in the figures. The most basic examples show seemingly minor discrepancies. For example, the total number of Australian-hosted prohibited items reported in the second reporting

---

[25] 16 in Jan to June, 6 in July to Dec; second *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2000* Tabled in Senate by the Minister for Communications, Technology and the Arts (April 2001) 9.
[26] Ibid 10-11.
[27] Second *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2000*, above n 24, 10.
[28] Ibid 12.
[29] See for example Electronic Frontiers, above n 15.
[30] First *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000* above n 5, 17,
[31] Senator Alston, referred to in Electronic Frontiers Australia, above n 15, 5 of 17.

period as 67 was in fact 64,[32] the number referred to police totalled 44 and not the reported 45,[33] in the third reporting period the given total of 37 was in fact 34.[34] More worrying are mistakes in reporting the nature of the content. While the ABA claimed in the second reporting period to have found 50 items of Refused Classification material, 12 of X and only 5 R rated, in fact the correct figures were only 44 RC, 9 X, and 11 R Rated.[35] In the previous reporting period also RC items were claimed to total 28 when in fact they totalled just 17.[36]

The significance of the errors lies not in the difference in the small numbers alone. The significance is rather firstly, that every mistake made in fact *overstates* the effect of the scheme, increasing the figures for prohibited content found, and increasing the figures for content referred to police. The misreporting may have been innocent, but it is interesting to note that no mistakes *understated* the effect of the scheme. Secondly, it is significant that the quantity of material stated to be found at the more extreme end of the scale was overstated, and conversely figures for content prohibited although at the less extreme end of the scale, were understated. The incorrect figures suggested that the content being dealt with and taken down under this scheme was more often more extreme than in fact it was. Again, no mistakes were made *understating* the amount of RC material found.

While reports on the scheme were to be made every six months,[37] it is clearly difficult to rely on that reporting for the true figures relating to the complaints regime. The above errors were corrected only as a result of the questioning in Parliament of the Minister for Communications, Senator Alston, and in response to direct questions regarding the accuracy of the figures reported.[38] This is not an efficient way for the public to gain information about the scheme.

---

[32] Ibid 7 of 17.
[33] Ibid 5 of 17.
[34] Ibid 6 of 17.
[35] Ibid 7 of 17.
[36] Ibid 6 of 17.
[37] This reporting is required as a result of a Senate motion, 30 September 1999. However, the latest 6 monthly report as at June 2004 relates to the period July to December 2001!
[38] Question on notice, asked by Senator Greig, Cth, *Parliamentary Debates*, Senate, 8 April 2002 responded to by Senator Alston, Cth, *Parliamentary Debates*, Senate, 17 July 02 1914-16 .

C. *Complaints statistics and freedom of information.*

A possible alternative method of getting information about governmental activity is an action under the *Freedom of Information Act*. Unfortunately, in response to an early freedom of information application requesting detail about complaints to the ABA and their outcomes, an ABA officer determined that as 'the Minister will report to parliament every six months on the operation of the scheme... aggregated data on the outcomes of its investigations of complaints is made available to the public' and that 'these mechanisms provide a comprehensive and effective accountability regime.'[39] The ABA officer concluded therefore that the public interest favouring disclosure of the material was outweighed in this case, as accountability was assured through regular reporting on the outcomes of the scheme to Parliament.[40] This decision of the ABA not to disclose some of the requested information was later upheld by the Administrative Appeals Tribunal (AAT) in June 2002.[41]

For the AAT the major consideration weighing against release of the information was the possibility that fewer complaints would be made and less information would be passed to the ABA if addresses of the content complained about were to be disclosed.[42] This was based on the ABA's argument that

> should the IPs and URLs of internet content be revealed to the public, the number of complaints [would] be substantially reduced. That would follow from the perception that the list of IPs and URLs would encourage certain people to seek access to the internet content complained about... [It is also] reasonable to expect that INHOPE members will not refer to the ABA complaints about internet content that they have received if URLs and IPs are publicly revealed.[43]

---

[39] Letter to Dale Clapperton of EFA from Richard Fraser, ABA Acting Manager, Online Services Content Regulation, 21 July 2000 at para 27-28. Document available at: <http://www.efa.org.au/FOI/foi_aba_2000.htm> at 25 June 2004.
[40] Ibid, para 27.
[41] *Re Electronic Frontiers Australia Inc and Australian Broadcasting Authority* [2002] AATA 449 (unreported, Fogie DP, 12 June 2002).
[42] Ibid [46]-[47].
[43] Ibid.

The AAT acknowledged that complaints - even those followed by X or RC ratings - would not ensure that access to the content was limited.[44] It found however that complaints and reporting to the ABA at least allowed information to be passed to filter makers, and that fewer complaints may lessen these reports to filter makers, and thus lessen the usefulness of filter products.[45] The effectiveness of the scheme, and in particular the effectiveness of voluntary content control (via the use of internet content filters), would thereby be reduced.[46] The AAT thus held that 'disclosure under the *FOI Act* would not, on balance, be in the public interest... On this occasion considerations favouring its disclosure are outweighed by the substantial adverse effect that we consider would result from disclosure.'[47]

It was clear that the AAT was able in the circumstances to balance for itself the competing interests involved in that particular case. The Government however was not satisfied with that, and moved to exempt certain content from the application of the *Freedom of Information Act*, on the basis that its release 'would undermine the policy and objectives of the framework...'[48] The Government suggested that without such an exemption paedophiles and miscreants may use FOI applications to gain access to pornography, and that disclosed information may be used to 'feed the bizarre sexual appetites of deviants.'[49] Senator Alston accused those critical of the exemption of favouring unrestricted access to pornographic content, and to 'offensive material in all its manifestations.'[50] [51]

---

[44] Ibid [46].
[45] Ibid [49].
[46] Ibid.
[47] Ibid para [97].
[48] Communications Legislation Amendment Bill (No 1) 2002, Second Reading Speech, Cth, *Parliamentary Debates*, House of Representatives, 27 June 2002, 4550 (Mr McGauran, Minister for Science).
[49] Comment attributed to Senator Alston in 'FOI Loophole opens way to banned websites.' *Courier Mail* (Queensland) 4 September 2003, quoted in Lexis Nexis Legal Express 5 September 2003.
[50] Cth, *Parliamentary Debates* Senate, 9 September 2003,14061 (Senator Alston).
[51] While Senator Alston claimed that if the information relating to restricted content is released under FOI it would be released without restriction (and could thus be given to paedophiles), he made no effort to explain why, if that were the concern, an amendment was not instead made to the *Freedom of Information Act* to allow for restricted release only. For example, there could be restrictions on who could access the information, on purposes for which people could access the information, and restrictions on further release etc. In that way the information could be protected without removing accountability.

In passing the new legislation the government failed entirely to engage with the arguments regarding accountability and scrutiny, and the very reasons for the original introduction of the *Freedom of Information Act*. As was pointed out by Democrat Senator Cherry:

> It is about government accountability. It is about whether we should be putting an exemption into the *Freedom of Information Act* 1982 to ensure that a particular government agency will no longer be accountable under FOI for its decisions.... The AAT has shown that it can make these decisions. The AAT has shown that it balances these criteria effectively. The AAT has shown that the current Act is working well in balancing the issue of disclosure and accountability on the one side and the integrity of government processes on the other. We should leave it to do that.[52]

However, the amendment to the *Freedom of Information Act* was passed and came into effect on 27th March 2003.[53]

D. *Current reporting.*

Some of the issues relating to the ABA's reporting of complaints statistics have now been addressed. After substantial criticism and parliamentary questioning, reports on the scheme include notes explaining discrepancies between complaints numbers, numbers of items found, and notices and referrals made.[54] The ABA's Annual Report stated that some notices and referrals may not be the result of complaints made under the scheme itself.[55] If fails to specify however which actions arise from valid complaints and which from other formal or informal notifications. Unfortunately, since 2001 no report at all on the scheme has been issued by the ABA or the Minister. The latest report covers only the period up to December 2001. This is hardly the operation of a reporting regime one would call a 'mechanism providing a comprehensive and effective accountability regime.'[56]

---

[52] Ibid 14059 (Senator Cherry).
[53] *Communications Legislation Amendment Act (No 1) 2003* (Cth). (Schedule 2 is the relevant part of that amendment).
[54] Fourth *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2001* Tabled in Senate by the Minister for Communications, Technology and the Arts (August 2002) above n 4, 9.
[55] Australian Broadcasting Authority, above n 3, 48.
[56] As it was called by Richard Fraser in a letter to Dale Clapperton of EFA, above n 38 [27]-[28].

However, during the period since 2001 some data regarding the ABA's activities has been made available through the ABA's Annual Reports, and on its website.[57] The latter includes an aggregated set of figures for the first 3 years, and monthly figures for more recent months. Unfortunately, the website information is scant, and does not for example distinguish the number of complaints made about Australian content from those made about overseas hosted content. No numbers are given for referrals to police, nor is it clear whether world wide web or newsgroup content is being referred to.

E. *Usefulness of the Complaints Scheme.*

It can be seen from the above that many issues arise in relation to reporting on the complaints regime. In addition, issues arise as to whether the complaints process leads to useful outcomes. Although complaints may be made, take-down notices issued, extra URLs included in filter software, and referrals made to police forces, the question remains as to whether the complaints regime really has any impact on the content available on the internet, or on access to that content. This is unlikely. While it is true that some content has been taken down from Australian servers, it is also true that some at least is known to have been removed from Australian servers and immediately relocated overseas,[58] and, in the case of newsgroup content, removal from one server is likely to occur even while the content remains on other servers within Australia.[59] As for notifying content to filter-makers, few internet users in Australia appear to be using filters.[60] Also, there is evidence that

---

[57] Internet Content Complaints - 1 January 2000 to 31 December 2002. ABA website above n 8.
[58] See for example first *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000* above n 5, 16.
[59] Australian Broadcasting Authority submission, above n 15, 25 'The requirement that the ABA be satisfied that an ISP is hosting such content prior to issuing a take down notice limits the ABA's capacity to take action in relation to content that may be simultaneously hosted by many ISPs.'
[60] There is no published material relating to the rate of filter use, but there have been comments from ISPs such as Bigpond to the effect that users are not really interested in filter software, even when free trials have been offered. Steven Wardill, Consumer Affairs Reporter, 'Code to push Internet porn out of reach' *Courier Mail* 13 May 2002, quoted in Electronic Frontiers Australia Inc, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 21. Further, many filters are sold as part of IT packages, such as anti-virus software, and thus the rate of sales of filter products are not indicative of the rate of usage. The Australian Broadcasting Authority submission, above n 15, notes that while research shows that internet users

filter makers do not always act upon the ABA's notifications of content, and/or that filter products are inadequate to the task, as testing for accessibility of URLs specifically notified to filter makers yielded large failure rates.[61] Thus it does not appear that providing filter makers with the URLs of overseas hosted X and RC rated material would make much if any difference to content accessibility. Further, even if filters were used to block access to notified content, and were effective in doing this, the quantity of content blocked is nothing compared to the number of sites still freely available.

Although there is evidence of removal of some content from Australian servers, there is little evidence that the complaints regime is at all effective in controlling access to content. It may be effective in other ways however, such as by providing the public with an avenue of complaint, and by helping to bring to light criminal behaviour which can then be dealt with by police or international bodies, but again there is little evidence of this. In addition to the reported statistics discussed above, the perceptions of many individuals and groups as to the effects of the complaints regime will also be discussed, in Chapter Twelve: Statistics and Perceptions. Prior to that however, the thesis continues to examine the direct effects of the *Online Services Act*, moving now to State and Territory legislative provisions.

---

would accept a 95% accuracy rate and a 5 second delay, none of the products currently available meet these requirements.

[61] Of fifteen scheduled filters only 4 had less than 10% failure rates. CSIRO *Effectiveness of Internet Software Filtering Products* (Sept 2001) results summarised in 'Table 1. Scheduled filters – rates of failure to block content notified by the ABA' in Australian Broadcasting Authority submission, above n 15, 7.

CHAPTER TEN: STATE AND TERRITORY LEGISLATIVE PROVISIONS.

A. *The overall picture.*

The *Online Services Act* was intended to engender and be part of an integrated legislative response to internet content regulation. State and Territory governments were to enact legislation complementary to that enacted by the Commonwealth, such that internet content control all over Australia would be subject to the same regulatory scheme. As discussed previously, the Federal Government's various heads of power allow it to legislate over telecommunications, external affairs, customs etc, but not to regulate many purely intrastate activities of individuals, such as creating content.[1] Like the Australian classification scheme, where complementary legislation allowed the Commonwealth OFLC to classify material, and those classifications to be applied under State and Territory legislation, it was hoped that a similar framework would succeed for internet content. Commonwealth legislation would cover those parts of internet content regulation which fell within federal power, but those outside power would be covered uniformly by the States and Territories. The Commonwealth Government frequently referred to its intended legislation as part of a broader scheme, to be enacted throughout the country.[2]

However, while the uniform national scheme was referred to in the Second Reading Speech[3] it was not initially specified in the Online Services Bill. It was added by amendment, in response to concerns that the Bill 'creates the impression that ISPs and ICHs are to bear the prime burden in relation to offensive material,

---

[1] Discussed above in Chapter Five: Censorship and freedom of speech.

[2] See for example Broadcasting Services Amendment (Online Service) Bill 1999, Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 21 April 1999, 3957, 3959 (Senator Ian Campbell, Parliamentary Secretary to Senator Alston, Minister for Communications, Information Technology and the Arts). 'The bill is intended as part of a multifaceted approach to ensure a uniform national approach...'

[3] Ibid 3958. 'The Commonwealth will be responsible for regulating the activities of Internet service providers (ISPs) and Internet content hosts (ICHs) and the Attorney-General will encourage the development of uniform State and Territory offence provisions complementing the Commonwealth legislation (including section 85ZE of the Crimes Act) that create offences for the publication and transmission of prohibited material by users and content creators.'

rather than those who create and upload such material.'[4] While the Second Reading Speech had stated that the Attorney General would 'encourage the development of uniform State and Territory offence provisions complementing the Commonwealth legislation,'[5] the amended Bill made this more specific and more definite, stating that the second component of the scheme 'will be: (a) State / Territory laws that impose obligations on (i) producers of content and (ii) persons who upload or access content.'[6]

This second component also included amendment of the *Crimes Act* 1914 (Cth). This was amended to exclude 'internet content' from provisions which dealt with use of carriage services, and to make clear that the *Crimes Act*'s treatment of carriage services was in no way to interfere with the concurrent operation of any laws of the States or Territories.[7]

Prior to the enactment of the *Online Services Act*, some States and Territories had enacted legislation aimed at control of internet content. The Commonwealth Government was troubled by this 'possible regulatory fragmentation of differing State/Territory legislation and the possible adverse effect on the development of the online industry.'[8] It was concerned that State legislation would vary greatly, and would lead to multiple barriers to internet content distribution, and to industry growth and development. As much of the relevant internet content originated overseas, it was seen to be very much a Commonwealth matter, but limited federal powers meant that Commonwealth legislation alone would necessarily achieve less than might be achieved through a concerted effort. Thus the Commonwealth Government consulted all State and Territory censorship ministers, and garnered their support for the enactment of uniform legislation.[9]

---

[4] Supplementary Explanatory Memorandum (undated), Broadcasting Services Amendment (Online Services) Bill 1999 (Cth): Amendment 5.
[5] Senator Ian Campbell, above n 2, 3958.
[6] Broadcasting Services Amendment (Online Services) Bill 1999 (Cth) schedule 5 cl 1(3).
[7] Supplementary Explanatory Memorandum, above n 4; and Broadcasting Services Amendment (Online Services) Bill 1999 (Cth), schedule 2.
[8] Senator Ian Campbell, above n 2, 3959.
[9] Supplementary Explanatory Memorandum above n 4. This amendment 'puts the Bill in the context of a national scheme already agreed to by the Commonwealth, State, and Territory Attorneys'General.'

However, 4 years after the enactment of the federal legislation, only South Australia has the complementary legislation in place, and internet content regulation in the States and Territories continues to vary drastically. It differs in whether or not internet material is specifically restricted, what categories of material are restricted, and what penalties apply for breaches of the laws.

B. *State and Territory laws.*

State and Territory laws regarding internet content control can be divided broadly into three types. Firstly, Queensland, Tasmania and the ACT do not have legislation specifically covering this area.[10] Secondly, Victoria and the Northern Territory in 1995, and Western Australia in 1996, enacted legislation specifically regulating online content,[11] the provisions of which are discussed below. And thirdly, New South Wales and South Australia have enacted the draft model legislation, which is now operative in SA but not in NSW.[12] Thus online content is not subject specifically to State or Territory laws in Queensland, Tasmania, New South Wales or the Australian Capital Territory; it is subject to legislation in Victoria, Western Australia and the Northern Territory, and it is subject in South Australia to the draft model legislation envisaged in the enactment of the *Online Services Act*. The discrepancy in the various schemes is vast, and consequently the treatment of online content in the States and Territories is confused, complex, and

---

[10] Queensland had enacted the *Classification of Computer Games and Images Act* in 1995, which a court has found does not apply to content on online services (although it would apply to images on one's computer disk). *R v Quincey* (Unreported, District Court of Queensland (Ipswich), Robertson DCJ, (29 October 1996) Discussed at length in Electronic Frontiers Australia, *The first "net porn" trial in Queensland. Verdict: Not Guilty* (15 December 1996) <http://libertus.net/liberty/qcaseone.html#bkgrnd> at 28 June 2004). Tasmania and the Australian Capital Territory introduced *Classification Acts* in 1995, *Classification (Publications, Films and Computer Games) Act 1995* (Tas), *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (ACT) but neither cover online content. The Australian Capital Territory proposed amendments to its *Act* in 1999 to include regulation of internet content, but these have not been enacted.(Electronic Frontiers Australia, *Internet Censorship in Australia: Australian Capital* Territory (2002) <http://www.efa.org.au/Issues/Censor/cens1.html#draftmodel> at 28 June 2002).

[11] *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic), *Classification of Publications, Films and Computer Games Act* 1995 (NT), *Censorship Act 1996* (WA).

[12] *Classification (Publications, Films and Computer Games) (Online Services) Amendment Act 2002* (SA), *Classification (Publications, Films and Computer Games) Enforcement Amendment Act 2001* (NSW).

sometimes conflicting. A number of these regimes are illustrated below to highlight the variety of approaches taken, and the continuing fragmented nature of regulation in this area.

In Victoria, Western Australia, and the Northern Territory, current legislation relating to the transmission of objectionable or restricted content preceded the Commonwealth scheme. None of these jurisdictions have altered their legislation to bring it into line with the legislation drafted to complement the Commonwealth scheme.[13]

1. Western Australia and the Northern Territory

In the Northern Territory and Western Australia, a person shall not use a computer to

(a) transmit, (b) obtain possession of, or (c) demonstrate an article knowing it to be objectionable material; (d) advertise that objectionable material is available for transmission; or (e) request the transmission of objectionable material (in WA 'knowing it to be objectionable material').[14] For the purpose of these *Acts* 'objectionable material' means:

(a) a film classified RC, a computer game classified RC,[15] or a refused publication;

(b) child pornography;

(c) an article that promotes crime or violence, or incites or instructs in matters of crime or violence; or

(d) an article that depicts, in a manner that is likely to cause offence to a reasonable adult –

i) the use of violence or coercion to compel a person to participate in, or submit to, sexual conduct;

ii) sexual conduct with or on the body of a dead person;

---

[13] An exposure draft of the model legislation was released for public comment in September 1999. The draft can be found at <http://www.efa.org.au/Publish/actdraft1.html> at 28 June 2004.

[14] NT s 50Z(1), WA s 101(1).

[15] All adult computer games are refused classification (RC). Thus even if the content would be classified R in another format, as a computer game it will be Refused Classification if unsuitable for those under 18.

iii) the use of urine or excrement in association with degrading or dehumanising conduct or sexual conduct;

iv) bestiality; or

v) acts of torture or the infliction of extreme violence or extreme cruelty.[16]

Breach of these sections gives rise to penalties of $10,000 in the Northern Territory, and considerably harsher penalties in Western Australia of $15,000 or 18 months imprisonment for an individual, or in any other case $75,000.[17] A defence is available on proof that the article concerned is an article of recognised literary, artistic or scientific merit, or is a bona fide medical article, and that transmitting, obtaining, demonstrating, advertising, or requesting the article is justified as being for the public good.[18]

Additionally, a person shall not use a computer service to transmit restricted material to a minor, or to make restricted material available to a minor, also under penalty of $10,000 in the Northern Territory, or in Western Australia $5000 or 6 months imprisonment for individuals, or $25,000 in any other case.[19] 'Restricted material' means an article that a reasonable adult , by reason of the nature of the article, or the nature and 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 or hear.[20] Defences to this section include proof that the defendant complied with a Code of Practice,[21] took all reasonable steps in the circumstances to avoid a contravention, or believed on reasonable grounds that the person to whom the material was transmitted was not a minor, or that the material would not be made available to a minor.[22]

---

[16] NT s 50X, WA s 99.
[17] NT s 50Z, WA s 101.
[18] NT s 50Z(2), WA s 101(2).
[19] NT s 50ZA(1)&(2), WA s 102(1)&(2).
[20] NT s 50X, WA s 99.
[21] Codes of Practice relating to computer services may be approved by the Minister under WA s 100, NT s 50Y.
[22] NT s 50ZA(3), WA s 102(3).

2. Victoria

The Victorian *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* is somewhat different. It uses the 'objectionable' category (for RC material) in a way that corresponds broadly to that used in Western Australia and the Northern Territory. But rather than using a 'restricted' category the Victorian legislation uses another three distinct categories; child pornography, material unsuitable for minors of any age, and material unsuitable for minors under 15 years of age.

Four separate offences are created. Firstly, the legislation states that 'a person must not use an on-line information service to publish or transmit, or make available for transmission, objectionable material.'[23] Unlike the Northern Territory and Western Australian *Acts,* it is not necessary for the prosecution to prove that the defendant knew that the material was objectionable. Rather, the onus is on the defendant to prove that he or she believed on reasonable grounds that the material was not objectionable.[24] ISPs are exempt from this section unless they create or knowingly download or copy objectionable material.[25] Breach of the section carries a penalty of up to 240 penalty units (currently $24,000) or two years imprisonment.[26]

Secondly, an amendment made in 2001 distinguishes child pornography from other objectionable material. It provides that a person who knowingly uses an on-line information service to publish or transmit, or make available for transmission, objectionable material that describes or depicts a person who is, or looks like, a minor under 16 engaging in sexual activity or depicted in an indecent sexual manner or context is guilty of an indictable offence and liable to up to 10 years imprisonment.[27]

[23] Vic s 57(1).
[24] Vic s 57(2).
[25] Vic s 57(3).
[26] Vic s 57(1).
[27] Vic s 57A.

Thirdly, a person must not use an on-line information service to publish or transmit, or to make available for transmission to a minor material unsuitable for minors of any age.[28] It is a defence that the defendant did not know and could not reasonably have known that the person to whom the material was published or transmitted or made available was a minor, and had taken reasonable steps to avoid publishing or transmitting or making available for transmission, the material to a minor, or the defendant believed on reasonable grounds that the material was not material unsuitable for minors of any age.[29] Exemptions for ISPs are available as for section 57.[30] If such material is objectionable material a penalty of $24,000 or two years gaol applies, but if not the penalty is $6000 or 6 months imprisonment.[31]

Fourthly, the same section proscribes publishing, transmitting, or making available for transmission to a minor under 15 years of age material knowing it to be unsuitable for minors under 15.[32] It is a defence that the defendant did not know and could not reasonably have known that the person to whom the material was published or transmitted or made available was a minor under 15, and that the defendant had taken reasonable steps to avoid publishing or transmitting or making the material available for transmission to a minor under 15.[33] Interestingly, it is also a defence that the defendant believed on reasonable grounds that the parent or guardian of the minor had consented to the material being published, transmitted, or made available to the minor.[34] For breach of this section, a fine of 30 penalty units (currently $3000) applies.[35]

---

[28] Vic s 58(1).
[29] Vic s 58((2).
[30] Vic s 58(3).
[31] Vic s 58(1).
[32] Vic s 58(4).
[33] Vic s 58(4).
[34] Vic s 58(5).
[35] Vic s 58(4).

3. New South Wales and South Australia

New South Wales and South Australia are the only States to have enacted the draft model legislation[36] which was intended to complete a uniform national scheme for internet censorship, or internet content control.[37] But in common with the Online Services Bill, both in South Australia and New South Wales there was considerable criticism of the proposals and opposition to enactment.

In South Australia the Bill was originally submitted to Parliament in September 2000, but due to industry concern and public outcry it was referred in June 2001 to a committee convened specifically to enquire into it.[38] On 30 October 2001, the Select Committee tabled the report of its inquiry in which the majority recommended passage of the Bill with minor amendments.[39] However, the Bill did not pass both houses prior to the state election, and was re-introduced in June 2002. It then proceded smoothly through the South Australian Parliament, and was proclaimed to commence on 1st December 2002.

In NSW the *Classification (Publications, Films and Computer Games) Enforcement Amendment Bill* had a similarly long and difficult history. Having passed through the NSW Parliament and received the Governor's assent in December 2001, expressions of considerable concern from many groups, including media, the internet industry, and civil liberties organizations, led the NSW Attorney General to promise that the legislation would not be proclaimed until a public enquiry had been held to canvass the issues involved.[40] The enquiry was completed and reported to Parliament in June 2002, recommending against the commencement of the *Act*.[41] The enquiry found that the legislation may

---

[36] *Classification (Publications, Films and Computer Games) (Online Services) Amendment Act 2002* (SA), *Classification (Publications, Films and Computer Games) Enforcement Amendment Act 2001* (NSW).

[37] Classification (Publications, Films and Computer Games) (Online Services) Amendment Bill 2002 (SA), Second Reading Speech, SA, *Parliamentary Debates*, House of Assembly, 4 June 2002 (MJ Atkinson).

[38] Select Committee, Parliament of South Australia, *The Classification (Publications, Films and Computer Games) (Miscellaneous) Amendment Bill (No2)* (2001).

[39] Ibid.

[40] Referred to by the Standing Committee on Social Issues, NSW, in *Safety Net? Inquiry into the Classification (Publications, Films and Computer Games) Enforcement Amendment Bill 2001. Final Report: On-line Matters* (June 2002).

[41] Ibid.

adversely affect legitimate news and current affairs reporting, deter other legitimate uses, criminalize those publishing academic or other material legal to publish off-line, impact unfairly on providers of non-commercial content,[42] and would not meet its policy objectives.[43] It suggested that the policy aims could be better achieved through using *Crimes Act*[44] provisions to prosecute individuals supplying the most serious illegal content, using take-down notices under the *Broadcasting Services Act*[45] to remove less serious content, encouraging voluntary filtering, and increasing community education and advice.[46] The NSW Parliament has yet to respond to this report and thus the legislation remains inoperative.

Neither the NSW nor the SA legislation states its aims but Government speeches are enlightening. During its passage through the NSW Parliament the legislation was said to be 'designed to catch... suppliers and creators of objectionable content.'[47] The legislation aimed to 'deter the making of objectionable matter available on the internet, and protect children from matter unsuitable for minors.'[48] In heady rhetoric the legislation was described as 'another brick in the wall,' giving police 'another string to their bow,' and as 'one more weapon in the armoury of those who fight against child porn and child access to cyber porn.'[49] Like that of the Commonwealth legislation, the NSW Second Reading Speech claimed that the legislation rested on the principle that 'any matter that is illegal or controlled offline should also be illegal or controlled online.'[50] The Minister was 'confident that the amendment [would] improve the operation and enforcement of the national classification scheme. Furthermore, it represents an important step in safeguarding our children from exposure to offensive and disturbing material on

[42] Ibid 18.
[43] Ibid 32.
[44] *Crimes Act 1900* (NSW).
[45] *Broadcasting Services Act 1992* (Cth).
[46] Standing Committee on Social Issues, Parliament of Australia, *Safety Net? Inquiry into the Classification (Publications, Films and Computer Games) Enforcement Amendment Bill 2001. Final Report: On-line Matters* (2002) 44.
[47] NSW, *Parliamentary Debates*, Legislative Assembly, 25 October 2001, 18037 (General Bob Debus) in response to questioning.
[48] Ibid.
[49] Ibid.
[50] *Classification (Publications, Films and Computer Games) Enforcement Amendment Bill 2001* Second Reading Speech, *Parliamentary Debates*, Legislative Assembly, 7 November 2001 18251 (Mr Stewart, on behalf of AG Debus).

the internet.'[51] South Australian politicians were more realistic: 'While no South Australian law can... provide a complete solution to the problem of offensive or illegal internet content... it is nonetheless appropriate that South Australia does what it can to address the problem of offensive content that originates here.'[52]

The New South Wales and South Australian amendments are brief, and almost identical.[53] ISPs and ICHs are not caught by their provisions,[54] nor is ordinary email.[55] Further, the amendments allow regulations to exempt certain online services from their provisions.[56] Substantive provisions relate to objectionable matter and matter unsuitable for minors. A person must not, by means of an online service, make available, or supply, to another person objectionable matter (X or RC)[57] knowing it is objectionable matter, or being reckless as to whether it is objectionable matter.[58] A person is reckless as to whether matter is objectionable if the person is aware of a substantial risk that the matter is objectionable matter, and that having regard to the circumstances known to the person, it is unjustifiable to take the risk.[59] The question of whether taking the risk is unjustifiable is one of fact.[60] Breach of this section gives rise to a penalty of 100 penalty units ($11000) for an individual, 250 penalty units ($27500) for a corporation (NSW), or $10,000 (SA).[61] No specific defenses to this section are provided.

A similar provision applies to transmitting or making available matter unsuitable for minors (R),[62] with penalties of $5500 for individuals, $11000 for corporations (NSW), or $10,000 in SA. It is a defence under this section to show that the

---

[51] Ibid.
[52] MJ Atkinson, above n 37.
[53] *Classification (Publications, Films and Computer Games) Enforcement Amendment Act* 2001 (NSW), *Classification (Publications, Films and Computer Games) (On-line Services) Amendment Act* 2002 (SA).
[54] Ibid NSW s 45B(3), SA s 75B(3).
[55] Ibid NSW s 45E note, SA s 75A.
[56] Ibid NSW s 45B(1)&(2), SA s 75B(1)&(2).
[57] Broadly equivalent to 'objectionable material' in WA, NT and Vic legislation.
[58] *Classification (Publications, Films and Computer Games) Enforcement Amendment Act 2001* (NSW) s 45C, *Classification (Publications, Films and Computer Games) (On-line Services) Amendment Act 2002* SA s 75C.
[59] Ibid SA s 75E(1), NSW s 45E(2).
[60] Ibid SA s 75E(2), NSW s 45E(2).
[61] Ibid SA s 75C, NSW s 45C.
[62] Ibid NSW s 45D, SA s 75D.

matter was subject to an approved restricted access system,[63] or in South Australia that the defendant had taken steps to put a restricted access scheme into operation and that failure of such a system did not result from any act or omission of the defendant.[64]

C. *Continuing fragmentation.*

It can be seen from the above that no national scheme for the regulation of internet content has come into being. Queensland, Tasmania, and the Australian Capital Territory have no legislation operating in relation to online content, NSW has the draft model legislation enacted but not operating, SA has the draft model legislation in operation. WA and the NT have schemes similar to one another but which preceded the *Online Services Act,* as does Victoria but with quite different legislation. Categories of material to be regulated include objectionable material, restricted material, child pornography, material (or matter) unsuitable for minors, and material unsuitable for a minor under 15. Required knowledge, onus of proof, defences and penalties vary markedly across the various jurisdictions. This is despite the agreement of all State and Territory censorship ministers prior to the enactment of the *Online Services Act*, that they would enact legislation to ensure the creation of a uniform national scheme.[65]

It is not clear why States and Territories other that New South Wales and South Australia have not moved to enact the model legislation, but historical attempts to protect autonomy may have played some part. While the laws of England were initially 'received' into each of the Australian colonies, and initially formed the basis of state and territory laws, legislation in individual states and territories has since developed to suit the specific jurisdiction. Concerns over the ensuing lack of uniformity between Commonwealth, State, and Territory laws have been voiced

---

[63] *Classification (Publications, Films and Computer Games) Enforcement Amendment Act 2001* (NSW) s 45D(2).
[64] *Classification (Publications, Films and Computer Games) (On-line Services) Amendment Act 2002* (SA) s 75D(2).
[65] Supplementary Explanatory Memorandum (undated), Broadcasting Services Amendment (Online Services) Bill 1999 (Cth) amendment 5.

for many years, and not simply in relation to internet content.[66] Nevertheless, while attempts toward uniformity have been made, and model uniform provisions drafted for many areas of the criminal law for example, these have not led to uniform enactment in the States and Territories.[67] The States and Territories have traditionally shied away from encouragements to uniformity, jealously protecting their legislative autonomy, and they continue to do so in many areas. Although the States and Territories had apparently agreed to uniform legislation for the internet, the model legislation in this sphere may have been seen by the States and Territories merely as another attempt to bring them into line with the federal government.

Alternatively, the failure of States and Territories to enact the draft model legislation for internet content control may have been due to a belief that existing legislation dealt effectively with the issues raised. The creation, display, distribution and sale of illegal content was covered by legislation prior to the *Online Services Act*, and continues to be so covered. Criminal offences already existed to deal with creators, sellers and distributors of illegal content, and the *Online Services Act* deals with its removal from local sites.

The Federal Government claimed the uniform national scheme to be an important part of its internet content regime, but it is clear that the States and Territories have not seen it as so important. As a result, the Federal Government has recently introduced amendments to its own Criminal Code,[68] to ensure that users and producers of certain online content will be subject to criminal sanctions by the Commonwealth, if not by the States and Territories. These amendments are discussed further below in Chapter 15. For now however the thesis continues to examine the direct effects of the *Online Services Act*, moving next to Community Education.

---

[66] MR Goode, Constructing Criminal Law Reform and the Model Criminal Code. (Accessed at http://www.isrcl.org/Papers/Goode.pdf 3 January 2005).
[67] Ibid, 'Current Implementation Record.'
[68] Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004 (Cth).

CHAPTER ELEVEN: COMMUNITY EDUCATION AND AWARENESS.

As mentioned above, the *Online Services Act* includes provision for community education, and both the ABA and NetAlert are charged with carrying out this function. Like the second component of the scheme, that is complementary State and Territory legislation, this third component was further specified after amendment during the passage of the Bill through Parliament. Although initial statements had referred to the need for community education as part of the regulatory regime, this was more fully spelled out in the amended Online Services Bill. The third component of the scheme was stated to be 'monitoring content on the internet, and educating and advising the public about content on the internet.'[1]

NetAlert was set up in late 1999 to undertake these functions.[2] It was to provide community education regarding internet use and content, to monitor content,[3] to research access management technologies, and to provide advice to concerned community members,[4] as well as 'to encourage and promote the use of the internet by all Australians, particularly young people and their families...'[5] Like the objects of the *Online Services Act* itself, the aims of NetAlert may at times conflict, and it is unclear in such a situation which is or are to be given priority.

Both the ABA and NetAlert have prepared advice for families on internet use, safe surfing, managing family access to the internet, and both maintain web sites offering this information as well as providing links to further information. The ABA's 'Cybersmart Kids Online'[6] along with NetAlert's web pages,[7] provide some good information and advice for families, especially for those with little

---

[1] While the Broadcasting Services Amendment (Online Services) Bill was before parliament schedule 5 was amended to include a new clause 1: 'Explanation of the context of this schedule' which included reference to the 'third component of the scheme, aimed toward monitoring internet content, and educating and advising the public about content on the internet.' Online Services Bill, Supplementary Explanatory Memorandum: Amendment 5

[2] NetAlert Limited, *Annual Report 2002 – 2003* (2003) 12.

[3] *Broadcasting Services Amendment (Online Services) Act* 1999(Cth) schedule 5 cl 1.

[4] Senator Alston, *Internet content advisory board announced* (Press release on establishment of NetAlert, 26 November 1999) quoted in NetAlert Limited, above n 2.

[5] NetAlert Limited, above n 2, 12.

[6] <http://www.cybersmartkids.com.au/> at 28 June 2004.

[7] <http://www.netalert.net.au/index.php> at 28 June 2004.

understanding of the internet. While the site displays are quite different, the information provided by each is quite similar; and there have been concerns that in this respect the ABA and NetAlert are in fact repeating the same work.[8]

A particular aspect of community education was the provision of filter advice. Initially both the ABA and NetAlert websites included considerable promotion of filters 'approved' under the internet industry Codes of Practice, as a suitable method of protection from exposure to inappropriate internet content. Unfortunately, prior to the drafting of the Codes of Practice by the IIA and their registration by the ABA, there had been no examination of the quality of the 'approved filters.'

Rather, the 'approved filters' were chosen for approval by the IIA on the basis of a study conducted by the CSIRO,[9] [10] and seemingly without reference to numerous studies into filtering products which had been undertaken overseas.[11] The CSIRO study had evaluated these filters according to a number of criteria; ease of installation, ease of use, configurability, ability for updates in respect of newly notified offending content, and availability of support.[12] Unfortunately, the criteria were technical only, and no substantive evaluation of any of the approved filters had been carried out by the CSIRO or by the Internet Industry Association. The CSIRO report itself made this very clear, stating in no less than three places that 'the products were not tested for how well they actually carried out filtering.' [13] The report also noted that such testing 'is a sizable task and the authors understand that the task of examining filters will be a matter for the

---

[8] See NetAlert, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) and Australian Broadcasting Authority, *Submission to Review of the Operation of Schedule 5 Broadcasting Services Act 1992* (November 2002) 5.

[9] 'The sixteen approved filters are included as a result of an independent study of available options by the CSIRO.' Peter Coroneos 'Internet Content Control in Australia: Attempting the Impossible?' (March 2000) 6 (1) *UNSWLJ Forum, Internet Content Control* 28.

[10] P Greenfield, P McRea, S Ran, CSIRO, *Access Prevention Techniques for Internet Content Filtering* (Dec 1999) prepared for the National Office of the Information Economy.

[11] Discussed in more depth in Chapter Three: Methods of internet content control.

[12] P Greenfield, P McRea, S Ran, CSIRO above n 10.

[13] Ibid 4,5,31-32.

Commonwealth Government's recently established community advisory board, Net Alert.'[14] '...Hence, fitness for purpose is not warranted.'[15]

Considerable criticism was leveled at the promotion of filter software generally by NetAlert, the ABA and the IIA, and at the promotion of the 'approved filters' in particular. Concern was expressed that governmental authorities may be seen to endorse particular commercial filter products without any attempt at qualitative evaluation of the products, and that problems with filtering products were glossed over by those promoting their use.[16] Both the ABA and NetAlert's web sites did mention the need for responsible care and supervision of internet use, and referred briefly to possible problems associated with filters. However, while links were provided to many internet information resources, no links were provided to sites critical of filter software, nor to organizations such as PeaceFire[17] which actually test and report on filtering products, their problems and effectiveness. Potential problems such as over-blocking and under-blocking of content were referred to, while more serious problems such as lack of transparency and bias in filter products were not mentioned.

It is understandable that the ABA and NetAlert would not wish their information to be either alarming or overly detailed. But by under-stating and over-simplifying problems with filter products they perhaps underestimated the ability and intelligence of internet users, and of those who supervise the internet use of others. While both bodies promote community education and family responsibility, more information would better empower users to make safer and more appropriate choices. The limitations of filtering technology and of individual filter products are significant,[18] and may impact greatly on users' decisions with regard to both the use of filters generally, and the use of specific products. Fuller and more open discussion of these would not only better inform the community,

---

[14] Ibid 31-32.
[15] Ibid 5.
[16] See for example Carolyn Penfold 'The Online Services Amendment, Internet Content Filters, and User Empowerment.' (November 2000) NLR 7 http://www.lexisnexis.com.au/nlr/Articles-files/penfold2/default.htm at 30 July 2004.
[17] <http://www.peacefire.org/> at 28 June 2004.
[18] These limitations have been discussed in detail above in Chapter Three: Methods of internet content control.

but may also encourage the development of better tools, or more appropriate use of the tools available.

After considerable criticism on this score, two changes were made. Firstly, the IIA Codes of Practice were varied to replace the term 'approved filters' with 'scheduled filters.' This way, there would not be any suggestion that the listing of particular filters provided endorsement, although in fact the schedule still only includes a small fraction of the filtering products available. The wording change from 'approved filters' to 'scheduled filters' is unlikely to be significant to, nor even noticed by, users researching filter information via the IIA, ABA or NetAlert. A statement that the filters are not endorsed may be more informative.

The second, and more substantive action taken was NetAlert's funding of research into filter effectiveness. With a grant from NetAlert the CSIRO was able to carry out qualitative testing of the now 'scheduled' products,[19] testing each product for how well it blocked access to 'undesirable' content, and whether it also blocked access to 'desirable' content. The results of those evaluations are now included in links from the ABA and NetAlert websites. [20] These results are useful in enabling internet users to see how each filter performed in a particular test, but are perhaps also somewhat misguided. As mentioned above[21] very many content filters had already been extensively tested for effectiveness, but NetAlert and the ABA had failed to link to results of those tests. Further, the research looked only at filters currently available, and 'scheduled.' No research has been undertaken into the development or improvement of filter technologies, and the claim that NetAlert would be responsible for 'researching new access management technologies'[22] has not been followed up at all. It may have been a better use of research funds to have looked into research and development for the future, particularly the development of *Australian* content management schemes, which development

[19] CSIRO, *Effectiveness of Internet Software Filtering Products* (Sept 2001).
[20] <http://www.aba.gov.au/internet/research/filtering/index.htm>
<http://www.netalert.net.au/00379-CSIRO-Filter-Report.pdf> at 28 June 2004.
[21] See Chapter Three: Methods of internet content control.
[22] Senator Alston (Press release) above n 4, 12.

could take into account the Australian classification scheme and the Australian context.

NetAlert also funded an industry awareness program during 2001, which through seminars in all States and Territories aimed to raise awareness within the internet industry about the *Act* and Codes, and the industry's responsibilities thereunder.[23] NetAlert has also appointed an internet ambassador, has produced and distributed fridge magnets and brochures, circulates an e-newsletter, provides a help line, and has participated in international conferences.[24] However, there is no evidence that NetAlert has had any impact in terms of community education. In fact, its latest annual report of 54 pages covers community education in 4 lines![25] The report, like its submission to the Review of the *Online Services Act*, refers constantly to what it will do in the future, but gives no assessment of what it has done,[26] other than repeating statistics which make it look busy. While NetAlert claims to have distributed '419,057 brochures, 74,955 posters, 244,695 fridge magnets, 269,540 mouse mats, and 135,150 complete information kits,'[27] the Australian Library Information Association reported that less than one third of public libraries were even aware of NetAlert's existence![28]

Interestingly, during the course of the Review into the *Online Services Act,* and very possibly in response to criticisms made to the Review, NetAlert's charter was changed somewhat. Its objects and powers were consolidated to delete redundant provisions and to 'further focus the organisation on child safety online.'[29] The report of the Review itself recommended that NetAlert and the

---

[23] One may ask why NetAlert, and therefore taxpayers, should pay to inform the internet industry of its own codes! This seemed, on any reading of it, to fall beyond the charter of NetAlert.
[24] Net Alert Limited, above n 2, 18-26.
[25] Ibid 23.
[26] NetAlert, above n 8, states: 'In concert with [the] maturing of the ongoing implementation of the co-regulatory scheme, NetAlert's role has also matured – to the extent that it is now ready to meet, along with its existing role, clear demand within the scheme for a truly independent community education and advocacy body.' 5
[27] NetAlert, above n 2, 25.
[28] Australian Library and Information Association, *Survey of internet access in public libraries, 2002 preliminary report*, included in ALIA's *Supplementary Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (November 2002).
[29] Department of Communications, Information Technology and the Arts (DCITA), *Report of the Review of the Operation of schedule 5 to the Broadcasting Services Act 1992*. (2004) 25.

ABA work co-operatively to ensure their activities complement each other, and to identify appropriate constituencies for their roles.[30]

From the above discussion it can be seen that there has been some attempt by the ABA and NetAlert to provide community education as provided for under the *Online Services Act.* There is little evidence however that this community education has been effective, or that the research commissioned in this regard has been the most useful. Nevertheless *effective* community education is still regarded as the best way of assisting internet users to manage their internet experiences, and there is still hope that Australia will be able to improve in this sphere. Overseas attempts to use community education for this purpose are discussed in more detail below,[31] to give a clearer picture of the type of community education that may be possible. Before looking however at how improvements to the Australian scheme may be informed by overseas activities, this paper goes on to look at more of the possible effects of the *Online Services Act.*

[30] Ibid 28.
[31] See Chapter 14: Comparative content control.

CHAPTER TWELVE: STATISTICS AND PERCEPTIONS.

The previous chapters have dealt with clear effects of the online services regime; Codes of Practice, a complaints regime, State and Territory legislation, and the setting up of a community education scheme. The online services regime may also have had less clearly identifiable effects.

It is always going to be extremely difficult to say whether changes to internet content are related to the various legislative and other regulatory regimes in place around the world; and whether changes have occurred because of, or despite, or entirely without reference to, attempts at content control. Further, quite apart from the difficulty of ascribing a cause to changes in internet content, there is the difficulty of discovering what changes have occurred. The sheer quantity of material would make it difficult even to estimate how much of it might be children's content, pornography, sci-fi, news, racism, astrology, religion, education etc. If there *were* changes in the types of content available, given the quantity of internet content, would anyone be able even to spot such changes?

With this in mind, it would be wrong to claim that the *Online Services Act* has had no effect on internet content simply because there is no quantitative evidence of this. It is necessary rather to look to all possible sources of information on the topic, which include the very few small studies conducted on the topic, submissions to and the report of the Review of the *Act*, and reports of bodies such as the ABA. None of these answers the question as to what changes have occurred as a result of the online services regime, but each sheds some light upon its possible effects. Furthermore, while many of these sources deal with perceptions of the regime's effects rather than evidence of those effects, they are nonetheless valuable sources of information in the absence of more concrete evidence. This chapter reports on these studies, on submissions to the Review of the *Online Services Act*, and on the Review Report.

A. *Studies and surveys.*

The author conducted her own survey regarding effects and perceptions of the online services regime in July and August 2001, 18 months after the scheme for online content regulation came into operation. The survey was not intended to test any hypothesis, but to elicit information regarding the effects of the scheme, and perceptions of the effects of the scheme. The survey was conducted in two parts. The first, addressed to industry participants, was distributed electronically to members of the Internet Industry Association, and to members of two Australian ISP email lists.[1] The second was distributed in hard copy to those who had made submissions to the 1999 enquiry into the Online Services Bill undertaken by the Senate Select Committee on Information Technology. It was assumed that the former group would be familiar with changes online and within the industry, and that the latter group would have an interest in those changes. One hundred responses were received overall; 74 responses to the email survey, and 26 to the hard copy survey. Respondents included content providers, content hosts, filter makers, ISPs, internet users and community groups.

Not all questions were relevant to all respondents, and thus numbers of responses varied from question to question. Furthermore, it was sometimes difficult to categorise a response as a yes or no answer for quantitative purposes. Where responses could not be reliably grouped into yes / no categories, they were not included in figures given, or where appropriate were separately categorised as 'possibly,' 'maybe,' etc. In this regard the author took great care to ensure that the figures given were not skewed by forcing inappropriate categorisation. Results of the author's survey are reported below along with other relevant studies.[2]

[1] isp-australia@lists.isp-lists.com list and aussie-isp@aussie.net list.
[2] A fuller report of this survey was published in C Penfold, 'Internet Content Regulation in Australia: Perceptions Thus Far' (June 2002) 48. *Computers and Law* 24 (and is included with this thesis at appendix 1).

The other main studies have been conducted by Chen,[3] the Australia Institute,[4] Aisbett for the ABA,[5] and the Australian Library and Information Association (ALIA).[6] It must be noted that all of the studies have involved very small numbers and are thus limited in their findings. Furthermore, the studies have looked at diverse topics, each relevant to internet content regulation in Australia, but not comparable with one another, and hence their results cannot be aggregated. The studies have also been conducted at different times, and with different populations. However, while none of these studies can tell us how effective the legislative scheme has been, together they provide a glimpse into some of the effects, or perceived effects, of the online services regime.

1. Concerns about internet content.

Information regarding concerns about internet content was collected as part of the Internet@Home study commissioned by the ABA and conducted in August 2000,[7] and in a study conducted by the Australia Institute in February 2003.[8] The Internet@Home survey, which interviewed 1203 randomly selected people in Australia, found that 47% of 11-17 year olds had seen or experienced something offensive or disgusting on the internet.[9] It also found that although 77% of all those surveyed, and 84% of parents, perceived some risks associated with use of the internet, 90% of all those surveyed with internet access at home thought that the advantages of internet access outweighed the disadvantages.[10] According to this survey the issue of greatest concern to Australian internet users was financial

[3] Peter Chen, *Australian Adult Industry Survey* (2002), Report included as an attachment to Peter Chen, Centre for Public Policy, University of Melbourne, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (October 2002) 31-38; and Peter Chen, *Survey of Small ISPs in the Melbourne Area* (October 2002) ,within the submission at 12.

[4] Clive Hamilton & Michael Flood, Australia Institute, *Youth and Pornography in Australia; Evidence on the extent of exposure and likely effects* (February 2003) and Clive Hamilton & Michael Flood, Australia Institute, *Parents' Attitudes to Regulation of Internet Pornography* (March 2003).

[5] Aisbett K, The Internet at Home, A report on internet use in the home (2001) (Internet@Home) <http://www.aba.gov.au/internet/research/home> at 24 June 2004.

[6] Australian Library and Information Association, *Survey of internet access in public libraries, 2002: preliminary report,* included in ALIA's *Supplementary Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (November 2002).

[7] Aisbett, above n 5.

[8] Clive Hamilton & Michael Flood, *Youth and Pornography in Australia; Evidence on the extent of exposure and likely effects,* above n 4.

[9] Aisbett, above n 5, 41 (misreported as 53% in Clive Hamilton & Flood, *Youth and Pornography in Australia; Evidence on the extent of exposure and likely effects,* above n 2, 12.)

[10] Aisbett, above n 5, 35-37.

danger, such as fraud and credit card theft, which was reported by 54% of respondents.[11] Personal data misuse and privacy issues were the second greatest concern, nominated by 45% of respondents, while exposure of children to content followed as the third largest concern, nominated by 27% of respondents.[12] Concerns also included racist material and propaganda on the internet, unsolicited email, and the possibility of encountering undesirable people on the internet.[13]

Parents were more concerned about content, and about child related risks, than were those without children.[14] Parents were concerned also about their inability to limit or control content available on the internet, a lack of consumer information by which to judge suitability (ie no classification scheme to inform parents), the ease of access to the internet, and the lack of timing constraints or controls (such as nothing adult appearing on television before 9pm etc). Concerns were as broad as internet use wasting time, tying up phone lines, and interfering with homework.[15]

The Australia Institute also examined content concerns, by surveying 377 households in February 2003.[16] Respondents were asked: 'Are you concerned or not concerned about your child seeing unsuitable material such as pornography on the internet?' 61% were very concerned, and 85% overall were concerned.[17] Interestingly, respondents in households with internet access were less concerned about this than those in households without internet access.[18]

The Australian Library and Information Association (ALIA) conducted a survey of public libraries in 2002, receiving responses from 91 library services, which cover a total of 455 branches, and almost 2000 public access internet terminals.[19] Sixty percent of library services responding to this survey reported receiving

---

[11] Ibid 38.
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Ibid, ch 3.
[16] Hamilton & Flood, Australia Institute, *Parents' Attitudes to Regulation of Internet Pornography*, above n 4.
[17] Ibid.
[18] Ibid at footnote 3.
[19] Australian Library and Information Association, above n 6.

complaints about internet content.[20] Most complaints about content concerned sexually explicit material, while some concerned violence, racism, gambling, advertising, junk mail, and children in chat rooms.[21] The majority of negative comments which libraries received about the internet related however to technical and service issues, with complaints received for example about slow connections and restricted access to the internet.[22] Library services reported that they were able to deal directly with all complaints and none needed to complain to the ABA.

2. What is or should be done about these concerns?

The Internet@Home study found that most of the surveyed families who had home internet access used a variety of strategies to protect children from accessing unsuitable internet content.[23] Sixty seven percent of homes with children and with internet connections claimed to have rules for internet use.[24] Strategies included the use of filter tools and safe sites, spy-ware, rules about using the internet only with an adult present, only at specific times, only at specific sites etc.[25] Children reported taking immediate action such as exiting a site or deleting a file if they encountered undesirable content on the internet, and 44% of children reporting exposure to unwanted content told a parent of such experiences.[26] Although survey respondents reported significant levels of concern regarding internet content, it is clear that few of them saw available filters as an appropriate safe-guard. While installing a filter was the action most commonly taken to prevent or minimize exposure to pornographic content, only 17% of parents reported using such software to block content.[27] This figure is backed up

[20] Generally between 1 and 10 complaints per year. Ibid 5.
[21] Often this last is complaint about other library users rather than complaint about internet content per se. Ibid 5.
[22] Ibid 2.
[23] 186 responses were given by people with children under 18 at home, and with home internet access, Aisbett, above n 5, 48.
[24] Ibid 49.
[25] This survey was conducted in August 2000, and shows that even at that stage families were already using a broad range of methods of controlling, assisting, or protecting children from exposure to content unsuitable for them. Ibid 48-61.
[26] Ibid 47-48. The total number here is unclear from the report.
[27] Ibid 48. Of a total 186 parents with internet at home.

by at least one ISP which reported very little interest or uptake when filters were offered to subscribers.[28]

Most households seem then to have some strategies in place for protecting against unwanted or inappropriate internet content, but many remain concerned about exposure to that content, and would welcome outside assistance with controlling it. An Australia Institute study, which surveyed households including at least 1 person between 12 and 17 years of age, asked 'Would you support a system which automatically filtered out Internet pornography going into homes unless adult users asked otherwise?' to which 93% of parents responded that they would.[29] Although the question was seriously flawed (see below), the response suggests nonetheless that many would like the control over internet content to be administered elsewhere, lifting the burden from themselves.

Eighty five percent of respondents to the Australia Institute survey would also support high schools educating students about pornography.[30] This was evident also in findings of the Internet@Home study in which schools were nominated by over 40% of parents as appropriate sites from which to distribute information about internet use and related parenting issues.[31]

It should be noted that while the Australia Institute surveys may give some helpful information relating to content control, serious concerns arise in relation to the survey itself. For example, the question asking whether respondents would support a system which blocks pornography, suggests to respondents that such blocking is possible. It fails to ask respondents whether they would support such blocking if it meant that much innocuous material would also be blocked, and what error rates for both under-blocking and over-blocking would be acceptable

---

[28] 'A BigPond spokesman said customers were offered filtering software automatically when they completed registration forms online. The spokesman said despite offering a **free trial** of one of the most recognised filters, the majority of BigPond's 1.2 million customers had opted not to download. [emphasis added] "Most people aren't interested in it, that is our experience," he said.' Steven Wardill, Consumer Affairs Reporter, 'Code to push Internet porn out of reach' *Courier Mail*, 13 May 2002, quoted in Electronic Frontiers Australia Inc, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 21 of 27.

[29] Hamilton & Flood, *Parents' Attitudes to Regulation of Internet Pornography*, above n 4.

[30] Ibid.

[31] Aisbett, above n 5, 72-74.

to them. Secondly, the question does not define, nor ask respondents to define, what they mean by pornography. Thirdly the rider 'unless they ask for it' fails to explain what adults might need to do to ask for it. Other questions included in the Australia Institute surveys raise similar concerns. However, even taking account of the flawed nature of the questioning, it is apparent from these surveys that there is concern, and that parents and others would like assistance in dealing with the problems they encounter or anticipate regarding online content.

3. Extent of knowledge and understanding of the online services regime.

No statistics show the extent to which the regime for online content control is understood by either the internet industry or the community, but surveys show awareness or understanding of different aspects of the scheme. In Chen's survey of twenty five small ISPs in Melbourne, all respondents claimed to be aware of the requirements of the *Online Services Act*, but in fact many went beyond the legal requirements of the *Act*, and were monitoring and/or removing/refusing to host/carry content they saw as problematic.[32] The Australian Library and Information Association (ALIA) stated that less than one third of libraries surveyed were aware of NetAlert and that even fewer (8%) use or have used it.[33] The Internet@Home study asked about the main sources from which respondents got information about the internet. 60% of parents said they had read advice about children using the internet, most commonly in newspapers or magazines.[34] 27% had received information from the internet itself, while 15% had received information from their ISP.[35] Most of the latter group were those most recently connected to the internet.[36]

4. Responses to and effects of the online services regime.

Surveys conducted by Chen and by the author asked various groups of industry participants about their responses to the *Act* and Codes. The latter survey found that less than half of the industry respondents had made any changes to policy or

[32] Note problematic, not illegal to host. Peter Chen, *Survey of Small ISPs in the Melbourne Area*, above n 3.
[33] Australian Library and Information Association, above n 6, 5.
[34] Australian Broadcasting Authority, above n 5, 73.
[35] Ibid.
[36] Ibid.

practice as a result of the *Act* and Codes.[37] Changes which had been made included moving content overseas, using anonymous proxy servers, ensuring *Act* and Code compliance (such as checking subscribers are over 18 years of age or having parents sign application forms), putting information regarding the *Online Services Act* and Codes on ISP websites, providing links to such information on other sites, and selling or advising on filter software.[38] Other action included restricting web content in various ways, such as refusing to host anything controversial and removing public service web hosting.[39] It is not clear however what impact this has had on community groups, individuals, or businesses who provide content, nor on the availablility of content to users. Industry respondents were more likely to view the changes to policies or practices as a result of the *Act* or Codes as trivial than as significant.[40]

Chen's survey of the adult industry[41] also found some changes, including respondents having removed or modified content,[42] added warnings,[43] or placed material behind restricted access systems.[44] A do-nothing or avoidance approach to the *Online Services Act* was more common however. Chen's survey found that in response to the *Act* 26 of 60 respondents had taken no action at all, while 17 of the 60 respondents had removed content offshore to avoid the *Act's* requirements.[45]

The few changes which may have occurred are perceived however to have had little impact on the content available to Australian users of the internet. In the survey conducted by the author, the great majority of respondents thought that

---

[37] 17 of 33. Respondents to this survey totalled 100, but not all questions were relevant to all participants, and thus responses to individual questions are likely to be fewer. For more detail see Penfold, above n 2 (and attached as appendix 1).
[38] Ibid.
[39] Ibid.
[40] Ibid, Trivial only: 9, significant: 6, in between: 8.
[41] 'Adult Industry' is not defined in the survey report, but presumably it includes those providing adult (erotic and pornographic) content, as Chen notes that the survey focuses on the adult industry as 'the regulation of adult (erotic and pornographic) content was the core aim of the enacted legislation.' Peter Chen, *Australian Adult Industry Survey*, above n 3, 31.
[42] 9 of 60. Peter Chen, *Australian Adult Industry Survey*, above n 3, 33.
[43] Ibid 10 of 60.
[44] Ibid 6 of 60.
[45] Ibid.

there had been no change to the internet content available as a result of the *Act* and the Codes,[46] there had been no change in the ability to access content as a result of external controls such as remote filtering or password protection of sites,[47] and there had been no change in users' ability to control access for themselves or for their children.[48]

These findings are supported by an Australia Institute survey.[49] Regarding pornography, the Australia Institute notes the lack of content control continuing under the operation of the *Online Services Act*. In its survey of 200 youths, 84% of boys and 60% of girls reported accidental exposure to sex sites on the internet.[50] The Institute asserts that the 'existing regulatory scheme can have no impact on the volume of porn available, or even on the sub set of internet sex sites which portray extreme material. There is no evidence that children and young people are being impeded from accessing or protected from exposure to material on the internet...'[51]

B. *Review of the Act*

In addition to the studies discussed above, perceptions of the operation and effects of the online services regime may be found in submissions to a Review of the *Online Services Act*. Section 95 of the *Act* includes a requirement that the scheme be reviewed within 3 years. Consequently an Issues Paper was released by the Department of Communications, Information Technology and the Arts, with submissions invited to be lodged by November 2002.[52] While a report of the Review has now been issued, it is submissions to the Review which give the most information regarding the operation and effects of the scheme, and perceptions of

---

[46] 42:16. Penfold, above n 2, 25.
[47] Ibid 26, 51:6.
[48] Ibid 26, 37:17.
[49] Hamilton & Flood, Australia Institute, *Youth and Pornography in Australia; Evidence on the extent of exposure and likely effects,* above n 4.
[50] Ibid vi. 38% of boys and 2% of girls also reported actually having searched for such sites.
[51] Hamilton & Flood, Australia Institute, *Regulating Youth Access to Pornography* (March 2003) 7.
[52] Department of Communications, Information Technology and the Arts, *A review of the operation of Schedule 5 to the Broadcasting Services Act 1992, Issues Paper* (September 2002).

those. Thus those submissions are discussed at length. This is followed by reference to the findings of the Review, which give yet another perspective on the effects and operation of the online services regime.

Only 26 submissions were made to the Review,[53] compared with well over 100 submissions made to the Senate enquiry preceding the 1999 passage of the *Act.*[54] The significance of this is unclear. It may be that the Review was less publicized than the initial enquiry, that with the legislation already enacted the urgency of speaking out was lost, or that merely through the passage of time the issue had lost its gloss and interest. It may suggest that community concern has been allayed by the operation of the *Act* in its first 3 years, and that those with an interest in online content regulation issues are satisfied with the current scheme. Alternatively, those whose views were marginalised or ignored by the earlier enquiry may not have felt it worthwhile to make a submission to this review. From a Government point of view however, the small number of submissions may signal, at the very least, a willingness to accept quietly the current scheme.

Issues raised in submissions to the Review are summarized below, and no attempt is made at this stage to answer or deal with the points raised; this is left to the following chapters. The aim is rather to report on the main themes arising in submissions, and particularly on those ideas or issues which were raised repeatedly. Thus points made more specifically by particular authors may be generalised to enable a broader description of the issues, themes, criticisms, and suggestions arising, rather than reporting in detail on each submission made.

1. Submissions to the Review

A certain cosiness is apparent in a number of Review submissions which glowingly report on the success of the *Online Services Act.* Those who might be called 'key stake holders,' (or alternatively 'the in-crowd') appear keen to support

[53] Submissions are available at <http://www.dcita.gov.au/Article/0,,0_1-2_10-3_481-4_111736,00.html> at 29 June 2004.

[54] The committee received 104 written submissions, and heard from 33 witnesses in four public hearings. Senator Jeannie Ferris, Introduction to the Select Committee Report, *Report of Senate Select Committee on Information Technologies.* (May 1999).

the current scheme. Some of their submissions are entirely self-congratulatory and non-analytical, with comments highly repetitive of one another. The submission of NetAlert, the body established to undertake community education activities as part of the internet regulatory regime, is a good example of this.[55] Its submission includes nothing substantive at all, but claims that the scheme is 'widely regarded as having achieved successful outcomes, and has become a benchmark for many jurisdictions around the world...'[56] 'The scheme has proven to provide an excellent balance...' [and there is] '...very high regard for the scheme [in] overseas jurisdictions'[57] [It is] 'widely accepted both in Australia and internationally, that the Australian model has developed into one that works extremely well.'[58]

The Internet Industry Association, which sees itself as largely responsible for having headed-off the government's more serious internet censorship plans, and which itself has favoured status as representative of the Australian internet industry, makes similar claims. According to the IIA 'Australia can rightly be said to possess one of the most advanced systems of internet governance in the world ... largely as a result of dialogue between government, industry and community.[59] Telstra, represented on the IIA board, similarly claims that the internet content regime 'is working very well. It strikes a balance between providing consumers with information and tools to manage online content themselves while ensuring that the obligations on ISPs do not undermine the commercial viability of providing Internet access...'[60] Optus, represented on both the IIA board and the board of NetAlert, not surprisingly makes similar comments, claiming that the regime 'works extremely well'[61] and 'provides an effective and efficient structure to balance the needs of the Australian community... with the need not to impose

---

[55] NetAlert, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002).
[56] Ibid 4.
[57] Ibid 8.
[58] Ibid 12.
[59] Internet Industry Association (IIA), *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 13.
[60] Telstra, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002).
[61] Optus, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 2.

unnecessary financial and administrative burdens.'[62] Optus goes on to state that '... the regime has been extremely successful in meeting its objectives'[63] and that the 'Australian Internet content regime is widely recognised internationally as one of the most effective regimes for the management of Internet Content in the world.'[64] None of these admirers of the current regulatory regime makes any attempt to measure the effectiveness of the *Online Services Act* against its stated aims.

While a number of submissions to the Review are generally supportive of the *Act*, and others are quite critical, most are concerned to address specific issues, rather than attempting to evaluate the scheme as a whole. Some of these specific points involve issues existing when the *Act* first came into operation, while some have only become relevant during the operation of the *Act*. Looking at the hugely different perspectives from which submitters write, it is clear why the proposed legislation caused such controversy initially. Submissions range in perspective from social welfare orientations (it is imperative to legislate to protect our children, and thus our society, from unsuitable content) to purely industry driven orientations (only durable market failure should be a trigger for regulation). Most submissions lie somewhere between the two.

(a) Co-regulation, and balancing needs.

A submission from the UK claimed that the Australian scheme for regulating internet content goes considerably further than any other scheme in the world, and is unique in combining requirements for Industry Codes of Practice with hotlines, provision of filter information, etc.[65] Because it is a government initiated scheme it may be slower to respond to change than non-governmental schemes would be, but the statutory backing also gives the scheme more clout than it would otherwise have.[66] There was a great deal of support generally for the co-regulatory nature of the scheme, with a number of submissions noting the advantages of co-

[62] Ibid 3.
[63] Ibid 5.
[64] Ibid 23.
[65] Nigel Williams, Childnet International, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 2.
[66] Ibid.

regulation, the willingness of industry to self-regulate, and the disadvantages which would have been seen if the scheme had chosen a top-down regulatory model.[67]

The balance between end-user needs and the capacity of business was seen as highly important.[68] Authors of a number of submissions were clearly happy that the IIA had negotiated Codes of Practice requiring minimal, if any, compliance work. Some submissions made it clear that while they supported the current co-regulatory scheme and Codes of Practice, they would not support anything imposing greater responsibilities on industry.[69] Austar for example claimed that 'the current framework provides adequate safeguards and meets community concerns *in a way the industry is able to support'* and as such requires no amendment.[70] Telstra claimed that the scheme worked well in '*ensuring obligations on ISPs do not undermine commercial viability,*'[71] while Optus claimed the regime successfully balanced the needs of community and family with the '*need not to impose unnecessary financial and administrative burdens'* on the internet industry.[72] The IIA claimed that extra regulation would be a hardship to industry.[73]

(b) Complaints and reporting

A complaints-based regime for regulating internet content was generally seen to be better than intrusive censorship.[74] Over the past three years complaints made to the ABA regarding online content had averaged only about 1.3 per day, seen by some submitters as very few given the quantity of objectionable content on the

---

[67] For example Williams, Internet Industry Association (IIA), Optus, Vodafone, Australian Consumers Association, & ABA *Submissions to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (2002).
[68] Internet Industry Association (IIA), above n 59, 3, Optus, above n 61, 6&24, Australian Broadcasting Authority, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 5-10.
[69] Optus, above n 61, 18.
[70] Austar United, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) (italics added).
[71] Telstra, above n 60. (italics added).
[72] Optus, above n 61, 3 (italics added).
[73] Internet Industry Association (IIA), above n 59, 6.
[74] Internet Society of Australia (ISOC-AU), *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 1.

net.[75] It was suggested that this reflected poor public awareness of the complaints system, but another submission saw that numbers of complaints as neither overwhelming nor trivial.[76] It was pointed out also that however many complaints were made, the scheme has not changed the available material in any way.[77]

Complaints handling by the ABA was said to be world's best practice when measured against international criteria for this kind of scheme, and one submission praised the ABA's release of the statistics generated by their investigation of complaints under the *Online Services Act.*[78] Others however were concerned about the information which the ABA refused to release. The ABA submission claimed that other hotlines would not co-operate with the ABA if they could not be certain that the information they give would be kept confidential,[79] and claimed that publication of further information regarding complaints could invite distribution of child pornography and could jeopardise police enforcement.[80] However, a number of submissions were critical of the ABA unnecessarily taking an 'all or nothing' approach to release of information.[81] Submissions suggested that specific information regarding content which was the subject of a complaint could be given with conditions placed on its release,[82] or that only information identifying RC content should be withheld.[83] One submission noted that those wishing to access more detailed information regarding complaints and classification of online material were few, and were bodies with legitimate interests in the information, not those seeking 'roadmaps to

---

[75] Australian Children's Television Foundation, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 2. (This could of course be referable to community recognition of the futility of complaining).
[76] Australian Consumer's Association, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 2.
[77] For example Peter Chen, above n 3, 5, Convergent Communications Research Group, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 3.
[78] Williams, above n 65, 2.
[79] Australian Broadcasting Authority, above n 68, 21.
[80] Ibid.
[81] For example Communications Law Centre, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 2, Australian Council on Children and the Media (Young Media Australia) *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 7.
[82] Australian Council on Children and the Media (Young Media Australia) above n 81.
[83] Peter Chen, above n 3, 9.

pornography.'[84] It was also argued that the effect of refusing to identify content the subject of complaints is to stop critics from scrutinising the operation of the OSA.[85]

(c) Community education

There was a widespread belief amongst submitters that community education was a very important part of ensuring safe and rewarding internet use, and a number of submissions were critical of the level of community education which had been achieved so far. It was felt that more active education of children, parents and carers was necessary, and not just the provision of links to information for those who happened to look.[86]

Some submissions praised both the ABA and NetAlert community education activities,[87] while others noted apparent duplication between the community education work of the two.[88] The ABA's community education website was said to be relevant and family-friendly, while NetAlert's was more corporate, and less likely to appeal to families and children.[89] Few public libraries had heard of NetAlert, and even fewer had used it as a resource. [90]

Concerns were raised that community education undertaken by these bodies relied too much on web-based outreach,[91] and did not make sufficient use of existing organizations such as schools, libraries and other community bodies[92] who should have a greater role in community education. There was concern that ABA and NetAlert education activities could even displace or discourage education by

---

[84] Ibid 8-9.
[85] Ibid 8.
[86] For example, Australian Consumer's Association, above n 76, 2-3 (information required at point of sale of hardware and software), Australian Children's Television Foundation, above n 75, 3, (information on ISP home page not sufficient when most subscribers only went to ISP home page once, when setting up account).
[87] For example Optus, above n 61, Internet Industry Association (IIA), above n 59.
[88] Williams, above n 65, 3-4, Australian Children's Television Foundation, above n 75, 4.
[89] Williams, above n 65, 3. This submission also questioned the value of NetAlert's phone help line, at 4.
[90] Australian Library and Information Association, above n 6, 5.
[91] Australian Children's Television Foundation, above n 75, 4.
[92] Ibid 4, & Australian Council on Children and the Media (Young Media Australia) above n 81.

community groups.[93] The Singapore model, whereby community groups undertake community education tasks, co-ordinated by the SBA, was recommended.[94]

(d) Policy engagement

Some submitters felt that the current scheme did not encourage the broader community to engage with issues regarding the use of new technologies, and that more diverse and ongoing engagement with policy developments in this area would lead to better outcomes for users and consumers and for the community generally.[95] The current Codes of Practice were said to encourage a 'tick and flick' approach to compliance by industry, rather than an engagement with policy development.[96]

(e) Linking speech restrictions with child protection.

Concern was expressed that attempts to protect children were bundled together with restrictions on adult speech. It was argued that less restrictive access to content for adults could not be equated with a lack of care for children,[97] and that the aims of the *Act* could be achieved without restricting rights to information.[98] Comment was also made that police are in a better position to investigate and prosecute crimes involving children than are bodies such as the ABA. One submission noted that in the USA, although expression was highly protected, investigation and prosecution of crime involving children are rigorous.[99] The linking together of child protection and censorship raised concern that things such as child pornography may not be reported, because such reporting may lead to more content restrictions.[100]

---

[93] Williams, above n 65, 3-4, Peter Chen above n 3, 21-24.
[94] Williams, above n 65, 3.
[95] For example ibid 5, Peter Chen above n 3, 27-30, Convergent Communications Research Group, above n 77.
[96] Peter Chen above n 3, 14, (cf IIA, which claims that easy linking to information increases code compliance. Chen also suggests that getting industry to pay some money may increase engagement.)
[97] Ben Caradoc-Davies, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 4.
[98] Australian Library and Information Association, above n 6, 7.
[99] Ben Caradoc-Davies, above n 97, 4.
[100] Ibid.

(f) Appropriateness of the content restricted.

There was some concern about the actual content caught by the *Online Services Act*. For example, it was said that some content may have an R rating due to adult themes, but should not perhaps be required to be housed behind a restricted access system (RAS).[101] News for example may involve adult themes, but would never be accessed if housed behind an approved restricted access scheme. For such material supervision of access was more appropriate than an RAS.[102] Furthermore, the requirement for R-rated Australian material to be housed behind RAS meant that non-commercial operators are unlikely to be able to make their material available, thus taking away the internet's promise of providing a haven for non-mainstream material, and discriminating against those who could not afford to have their content hosted overseas.[103] There was definite feeling that the 'restrictions' on RC and X in overseas content should certainly not be broadened to include R-rated material.[104]

A concern about the inconsistency in content caught by the scheme was apparent in submissions. For example it was noted that a great deal of racist material, hosted both within and outside Australia, was freely available on the internet, and much of it fell outside the *Act's* restrictions.[105] Further it was suggested that restrictions on such material should go beyond the *Act's* current restrictions to include the distribution or supply of this material whether by email, chat, newsgroups or other means.

Banning X-rated material from Australian hosts was also seen as inconsistent with, and restrictive beyond, off-line restrictions. It was argued that X-rated material should be permitted to be hosted in Australia, so long as it is behind an

---

[101] Communications Law Centre, above n 81, 2, Convergent Communications Research Group, above n 77, 3.
[102] Communications Law Centre, above n 81, 2.
[103] Ben Caradoc-Davies, above n 97, 5.
[104] For example Kimberley Heitman, Adultshop.com, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002), Australian Broadcasting Authority, above n 68, 15, Communications Law Centre, above n 81, 2, Internet Society of Australia (ISOC-AU), above n 74, 4, Optus, above n 61, 3.
[105] Race Discrimination Commissioner, Human Rights and Equal Opportunity Commission, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002), Australian Broadcasting Authority, above n 68, 15.

RAS, as required for R-rated Australian-hosted material. The total ban on hosting X-rated material in Australia was said to disadvantage the Australian adult industry *vis a vis* the industry overseas, and drive adult material offshore without any effect on Australian's access to the material. Furthermore, it missed an opportunity for Australia to better regulate the adult industry.[106]

(g) Technological solutions / filters

Technological solutions to internet content regulation were not proposed in any submissions to the Review. Some in fact specifically cautioned against technological approaches, both because no existing technological solutions were sufficiently effective, and because technological solutions continually become outmoded with the constant and ever increasing development of new and diverse technologies.[107]

Some submissions suggested that requiring ISPs to provide filters gave the necessary balance between consumer control and regulatory intervention,[108] and that filters, although imperfect, do provide a useful additional layer of protection.[109] There was however considerable concern about the heavy reliance which the *Act* and Codes of Practice place on the use of filtering products,[110] which may be ineffective to protect or restrict children from accessing inappropriate content (and adults from content they do not wish to find), and which lack transparency in some instances.[111] It was noted that the 'scheduling'[112] of overseas filter products paid no attention to their appropriateness in an Australian cultural context, nor to their consistency (or otherwise) with the Australian classification scheme.[113] It was suggested that the Government should rather fund research and development of Australian filter products.[114]

---

[106] Heitman, above n 104.
[107] Convergent Communications Research Group, above n 77, 6, Ben Caradoc-Davies, above n 97, 2-6.
[108] Australian Consumer's Association, above n 76, 2.
[109] Australian Children's Television Foundation, above n 75, 2.
[110] Australian Council on Children and the Media (Young Media Australia) above n 81, 6.
[111] Australian Consumer's Association, above n 76, 2, Peter Chen, above n 3, 7, Internet Society of Australia (ISOC-AU), above n 74, 2-4.
[112] Filters included in the schedule to the Internet Industry Codes of Practice.
[113] Peter Chen, above n 3, 6-8, Internet Society of Australia (ISOC-AU), above n 74, 4.
[114] Australian Council on Children and the Media (Young Media Australia) above n 81, 6.

Some submitters thought that more specific and analytical information about filters should be given in community education, such as actual recommendations of filters appropriate for different ages, contexts, and values; rather than simply listing 'scheduled' filters.[115] The Australian Consumers Association had found that filters could be effective if configured by a knowledgable person to suit that person's needs.[116] Thus, ISP level filtering would not be useful, and more information for consumers about filter use was necessary.[117] A number of other submissions also concluded that better education, and better transfer of control to parents and users was the only way content regulation could be effective.[118]

Submissions from industry resisted the idea that filters should be provided freely, claiming that the cheapest filters would then be used, rather than the best quality or most appropriate.[119] Others suggested that the internet industry should actually fund filter research.[120] The ABA submission claimed that it is monitoring the continued development of filter effectiveness. It stated that a 5% failure rate and a 5 second delay would be acceptable in filter products, but no filter is yet at this stage.[121] The ABA notes that in Europe action is being taken to develop better filtering products, rather than just testing existing ones.[122]

(h) Content rating and labelling.

Some submissions encouraged the use of voluntary labelling using schemes such as the ICRA[123] scheme,[124] backed up by penalties for false labelling. Such tools

---

[115] Ibid 7.
[116] Australian Consumer's Association, above n 76, 2-3.
[117] Ibid. IIA submission also strongly argued that mandatory filtering at ISP level would be neither technically nor commercially feasible, Internet Industry Association (IIA), above n 59, 10.
[118] Convergent Communications Research Group, above n 77, 3, Australian Library and Information Association, above n 6, Internet Industry Association (IIA), above n 59, 9.
[119] Internet Industry Association (IIA), above n 59, 11, Optus, above n 61, 14.
[120] Australian Council on Children and the Media (Young Media Australia) above n 81, 7.
[121] Australian Broadcasting Authority, above n 68, 37.
[122] Ibid.
[123] The Internet Content and Rating Association is known as ICRA. ICRA has developed a labeling system for internet content, and the term 'ICRA' is now also used to denote the labeling and rating scheme devised by the Internet Content and Rating Association.
[124] Williams, above n 65, 5-6, Internet Content Rating Association (ICRA) *Submission to 'Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002), Australian Children's Television Foundation, above n 75.

were seen as consistent with the aims of the *Online Services Act*, as they promote choice rather than censorship, could be integrated with the Australian classification scheme, could better inform users about content, and were not financially onerous.[125] Use of a system such as ICRA would not create restrictions on speech, as content providers could choose whether or not to label content, but those wishing better to control content could then choose only to allow labeled content to be accessed.[126] Other submissions however noted that schemes using PICS type software and ICRA labeling were still not highly refined and are difficult to use, and have had, and are likely to have, very little uptake.[127] The ABA says it encourages the use of ICRA labels, and claims that about 50,000 sites are now labeled.[128] ICRA states that about 100,000 sites have applied to ICRA for labels since 2001, but it is not clear (even to ICRA) how many sites actually use them.[129]

(i) More Specific Criticisms.

A few very specific criticisms were also made in submissions, relating to the use of film classifications, the effect on universities, and mechanisms for appeal.

One concern continuing from prior to the *Act's* introduction related to the use of film classifications for internet content. One submission suggested as an alternative that internet content should be classified according to the most analogous offline content, [130] and thus text would be classified as a publication for example, moving images as film. This would reduce the danger of online material being rated inconsistently with off-line content due to format, rather than due to any substantive difference in the material itself.

Another specific concern related to universities with students under 18 years of age. As ISPs to students, universities need parental permission before allowing

[125] Internet Content Rating Association (ICRA) above n 124.
[126] Martin Aungle, Dimension Data , *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002).
[127] Internet Society of Australia (ISOC-AU), above n 74.
[128] Australian Broadcasting Authority, above n 68.
[129] Email to author from Lynn Edwards, ICRA, 11 November 2003.
[130] Internet Society of Australia (ISOC-AU), above n 74, 2.

students under 18 years old to access university internet facilities, creating huge administrative difficulties. It was suggested that universities be exempt from the provisions of the *Online Services Act* and the industry Codes of Practice. [131]

It was also suggested that classification decisions should be reported to the content provider rather than just to the relevant ICH or ISP, and content providers should have rights to appeal rulings about the classification of their content to the AAT.[132] Classification of online material was thought to be too expensive, the classification not commensurate with off line, and too few rights existed to challenge classification decisions.[133]

2. The findings of the Review of the Online Services Act.

While the Review of the *Online Services Act* was required to be conducted within 3 years of the commencement of the legislation - that is by 1st January 2003, and submissions closed in December 2002 - the Review Report was not issued until May 2004. During the life of the Review a Ministerial reshuffle saw Senator Alston's Communications portfolio taken over by former Attorney General Daryl Williams, who himself has now signaled his imminent retirement.[134] At the time of writing the Review Report has not yet been discussed in Parliament, and so it is unclear what response the Government, or Opposition, might make. However, the findings and recommendations are unlikely to encourage substantial changes to the scheme.

(a) Filtering

The Review was required[135] to investigate whether or not filtering technology had developed sufficiently 'to feasibly filter R-rated content hosted overseas that is

---

[131] Australian Vice Chancellor's Committee, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 199'* (October 2002), Geoffrey Dengate, Griffith University, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (October 2002).

[132] Communications Law Centre, above n 81, 2.

[133] Ibid, Electronic Frontiers Australia Inc, above n 28, 3.

[134] Senator Helen Coonan took over the portfolio on 18th July 2004.

[135] DCITA *Review of the operation of Schedule 5 to the Broadcasting Services Act 1992; Issues paper (September 2002)* 1. The review was conducted by individuals within the Department of Communications, Information Technology and the Arts, and will be referred to here as 'the Review.'

not subject to a restricted access system.'[136] While the *Online Services Bill* was before Parliament it had been noted that

> as things currently stand it may be very difficult to apply the same adults only approach to R-rated material onshore as to offshore....We propose to move an amendment which will provide a statement of intent ... that [R-rated] material should be accessed by adults only and that, if and when the technology becomes available to do that, we would expect the legislation to reflect it. That will be part and parcel of the review...[137]

The Review found that filtering technologies have not developed to that point.[138]

Regarding prohibited overseas content more generally (ie X or RC content), the Review examined the feasibility of upstream (ISP or proxy) filtering. It found that such filtering would not be appropriate if complex analysis techniques, such as keyword, word string, image or profile analysis were to be used. It found that such filtering at ISP or proxy level was 'no more practical than it was at the introduction of the scheme.'[139] The Review did find however that improvements had been made to index filtering (of URL or IP addresses) which would reduce delays such that this filtering at ISP or proxy level would not even be noticeable to end-users.[140] The Report noted however that while technology had improved in this respect, such filters still had the problems of block lists becoming quickly outdated, incorrect categorization of content occurring when lists were automatically generated, huge resources being required for human checking and updating of lists, and IP blocking being too broad-brushed. For example, the Report stated that thousands of domains may now be published from one IP address, all of which would be blocked if anything issuing from that IP was blocked.[141] Further, according to the IIA, such filtering at ISP level would impact on speed, which for users would cut into broadband's main advantage over other internet connections. The Report noted that Ovum's report on content filtering

---

[136] DCITA *Review of the operation of Schedule 5 to the Broadcasting Services Act 1992; Report* (May 2004) 16.
[137] Cth, *Parliamentary Debates,* Senate, 24 May 1999, 5220 (Senator Alston, Minister for Communications, Information Technology and the Arts).
[138] DCITA above n 136, 23.
[139] Ibid 17.
[140] Ibid.
[141] Ibid18.

disputed this, stating that index filtering at ISP level would not make broadband unfeasible.

The Review Report notes the high costs which might be involved in introducing such a filtering scheme. Based on figures given by Ovum, the Review Report states that ISP level blocking would cost the internet industry over $45 million in initial set-up costs, and over $33 million annually.[142] Further, it found it likely that the costs would have much greater impacts on the smallest ISPs. Set-up costs for very small ISPs are likely to be eight times those of small ISPs, and for small ISPs almost four times the cost for medium ISPs. It found that ongoing costs would similarly disadvantage the smaller players in the industry.[143] Overall the Review found that '[g]iven the limited benefits of an ISP-level filtering system, the costs of a mandated requirement to filter do not appear justified.'[144]

The Review also found that there was little encouragement given by ISPs to use filtering. It found for example that some ISPs merely link to pages including filter information from the bottom of their home pages, or from subsidiary pages. It looked then to two possible approaches for 'strengthening community safe guards,' that is, increasing the use of filtering and blocking. It suggested firstly that more active promotion of filter services by ISPs upon subscription, and regular advertising of filter services to subscribers, may encourage take-up of these tools.[145] Secondly, it found that ISPs could be required to include end-user filter products with subscriptions, but subscribers would have the option to 'opt-out' of the purchase of a filter.

Neither of these techniques would mandate changes to access to content, while both would make end-users more aware of the filtering tools available. While the Review is worded to suggest in the second option that subscribers may opt out of filter use, it really means subscribers could opt out of filter purchase. Whether the filter *purchase* is 'opt in,' 'opt out,' or compulsory, there is no suggestion that

[142] Ibid 19, 20, and see Ovum, *Internet Content Filtering: A Report to DCITA.* (April 2003) 26, 27
[143] DCITA above n 136, 19.
[144] Ibid 23.
[145] Ibid 21.

filter *use* be made compulsory. The cost to industry of both of these options 'would be significantly lower than requiring mandatory implementation of server-side filtering'[146] and they are to be looked at in the Review of the Internet Industry Codes of Practice currently underway.[147]

(b) Family friendly ISPs

The Review noted that the 'family friendly ISP' program, which would entitle code-compliant ISPs to display a logo identifying them as code-compliant and family friendly, has been distinctly unsuccessful. Of 563 ISPs in Australia, only 11 have registered under the program in the two years it has been in operation.[148] It is not clear just why the take-up has been so poor. Perhaps ISPs are not convinced of the value of displaying their 'code-compliant' credentials, other may not wish to be identified with the IIA, and possibly others are not compliant.

(c) Community education

The Review found that the internet industry could do a lot more by way of community education, as could the ABA and NetAlert. It found that the ABA and NetAlert need to work co-operatively to ensure their activities complemented one another, and need to make an effort to identify their relevant constituencies, which may include for example councils, libraries, state education departments, and academic institutions.[149] NetAlert should also make regular assessments of filter products and widely promote its findings in a user-friendly form. The Review noted that (during the course of the Review) NetAlert's objects and powers had been consolidated 'to delete redundant provisions and further focus the organisation on child safety online,'[150] and suggested that NetAlert should now go further and commission an independent evaluation of its community education activities.[151]

[146] Ibid 22.
[147] Ibid 24.
[148] Ibid 21.
[149] Ibid 28.
[150] Ibid 15.
[151] Ibid 28.

(d) ABA monitoring of the scheme.

According to the Review, the ABA also could do more. A previous study had found that even when content was notified to the makers of scheduled filters, users of those filters could frequently still access the content. This suggested that either the filter technology was ineffective, or that notified content was not being added to block lists as agreed. The Review stated that the ABA should 'ensure that the enforcement regime is credible and effective, with sanctions for failing to comply with ABA notifications, including de-listing' (removing filters from the Code Schedule).[152] The Review agreed with the ABA's submission that industry Codes of Practice should be monitored and regularly reviewed (every three years) to ensure they met their objectives, and to ensure that the scheme deals appropriately with technological and market developments.[153]

C. *Conclusions.*

From the studies and submissions discussed above it is clear that many concerns still arise in relation to the *Online Services Act* and the Australian scheme for online content control. The studies first referred to raise serious questions about the effect of the *Act* and its operations. The review submissions also demonstrate concerns about the *Act* and its effects, as well as showing a clear tension between on the one hand the industry association, large industry players, and major participants in the scheme, such as the ABA and NetAlert; and on the other hand individuals and community groups.[154] Generally the former group seemed happy with the overall workings of the scheme, its minimal obligations, and its minimal effect; whereas the latter submitters appear more concerned about the effect or lack of effect which the scheme has had. The Review Report, while acknowledging some of the concerns raised, did not recommend any major changes to the current scheme.

---

[152] Ibid 44.
[153] Ibid 45.
[154] This is not to suggest that all individuals and community groups agree with one another, but that they appear to be more critical of the scheme, and more disparate in their comments, than the former group.

Part two has attempted to explain the passage and provisions of the *Online Services Act*, the effects and operations of the regime overall, and the perceptions of these effects as found in the studies, submissions, and Review Report discussed above. Part three will now attempt to evaluate the scheme and to make recommendations for its improvement.

PART THREE

EVALUATING AND IMPROVING THE INTERNET CONTENT CONTROL REGIME.

Having looked at the context into which the *Online Services Act* was introduced, and at the operation and effects of the *Act* and of the scheme overall, this thesis now moves on to critique the online services regime and to offer suggestions for the future. Firstly in Chapter Thirteen the *Online Services Act* is evaluated upon the terms of its legislative objectives; has the *Act* met its own stated aims? The thesis then moves to a broader perspective on the topic, with Chapter Fourteen examining some of the methods currently used overseas in internet content control. In the light of the operation and effects of both Australian and overseas systems, Chapter Fifteen then makes recommendations for improvements to the Australian scheme.

CHAPTER THIRTEEN: THE STATED AIMS – HAVE THEY BEEN ACHEIVED?

A. *The Stated Aims*

The stated aims of the *Online Services Act* were a) to provide a means for addressing complaints about internet content, b) to restrict access to internet content likely to cause offence to a reasonable adult, and c) to protect children from exposure to internet content unsuitable for them.[1] In the light of the effects, statistics and perceptions reported in previous chapters, can it be said that the *Online Services Act* has achieved its stated aims?

1. Providing a means for addressing complaints about internet content.

The *Act* has certainly provided a means for addressing complaints about internet content. As discussed in chapter Nine above, under the *Online Services Act* complaints can be made to the ABA, and are then investigated according to ABA procedure. In some cases the content complained about is referred to the OFLC for classification, and take-down notices may be issued to force the removal of the content from Australian servers. Some such take down notices have been issued, and the content subsequently removed from Australian sites. However, as also discussed above, there is no evidence as to whether or not this makes any difference to the availability of this material on the internet. In fact, the ABA itself has reported that at least some content ordered removed was simply re-hosted overseas, remaining equally accessible in Australia.[2]

Whether or not this aim has been met really depends on what the aim really was. Was it simply to provide a means for addressing complaints, or was this aspect of

---

[1] *Broadcasting Services Amendment (Online Services) Act 1999* (Cth) schedule 1 cl 2, now incorporated to become *Broadcasting Services Act 1992* (Cth) s 3 (k) (l) and (m).
[2] For example first *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000* Tabled in Senate by the Minister for Communications, Technology and the Arts (September 2000) 16 note 3.

the legislation intended to have some more substantive effect? A more substantive intent seemed likely when regarded with the Online Services Bill initially proposed, whereby complaints may have led both to removal of the content from Australian servers, *and* to blocking of the content from overseas. However, when viewed in operation, and thus in conjunction with the Internet Industry Codes of Practice, it would be silly to think that complaints could possibly have all the substantive effects initially envisaged, as the blocking of content from overseas is now no part of the scheme.

It is possible however that the restriction of content was not the only aim, and that the complaints mechanism was intended also (or rather) as a means of deflecting complaints with which politicians would otherwise need to deal. The establishment of the complaints regime may have been seen more as a way to channel the complaints of those lobbying for tighter internet content regulation into a more finite and manageable arena. This is suggested particularly by the stipulation that complaints under the legislation be made only by Australian residents, and corporations and businesses resident in Australia. If the complaints regime were concerned with bringing to light prohibited material, and restricting accessibility to it, there is no reason why it would distinguish between where the complaints originate or who is the complainant.

The first aim of the *Online Services Act* may then be said to have been achieved, as there is now a method for addressing complaints about internet content; one which allows the independent ABA to bear the brunt of 'community concern,' by redirecting to it complaints which would otherwise have been made to politicians. The mere establishment of this alternative avenue to make complaints removes from government both the burden of engaging with these complaints at all, and the more substantial burden of acting in response to them.

The introduction of the complaints mechanism thus firstly allows complaints to go through an administrative rather than political procedure, thereby reducing pressure on Government to act. Secondly, it changed allowable complaints from the expression of general concerns about illegal, objectionable, and / or unsuitable

material available on a particular medium, by requiring the complainants to identify specifically material of concern which could then be examined independently of the more general concerns. Thirdly, it provided an outlet for those most worried about internet content, and by doing so bought time for the medium to reach higher levels of general accessibility and acceptability, and to become better entrenched and more widely used. This way, further development of the medium was able to occur without constant public criticism and lobbying regarding the dangers of the internet.

Thus the first stated aim of the *Online Services Act,* to provide a means for addressing complaints about internet content, may be said to have been fulfilled, ineffectively in terms of changing or limiting the material available, but effectively in terms of providing a channel through which concerned constituents could voice their concerns, without requiring political responses.

2. *Restricting access to internet content likely to cause offence to a reasonable adult.*

The second stated aim, that is, to restrict access to internet content likely to cause offence to a reasonable adult, has not been met in any way. While some material may have been removed from Australian servers, there is no evidence that any material is more restricted or less available than it was prior to the enactment of the *Act.*[3] In fact, the ABA's submission to the Review of the *Online Services Act*, which claimed the scheme was effective in addressing complaints about internet content and restricting children's access to unsuitable content, did not even mention this aim.[4]

As discussed above in regard to the complaints scheme, this aim also was in line with the initially proposed Online Services Bill, and although it was a major part of regulating online content consistently with off-line content, it could not be

[3] Discussed in more detail in Chapter Twelve, Statistics and Perceptions.
[4] Australian Broadcasting Authority, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002).

achieved once the blocking of content from overseas was removed as a requirement of the legislation. Prior to the passage of the *Act,* much criticism focused on the costs the industry would bear to even partly meet this aim. Restricting such content would have required classification of material hosted within Australia, not only in response to complaints but more generally, along with classifying or filtering and blocking material from outside Australia. Classification to the extent required to fulfill this aim would have been physically impossible. Filtering and blocking would have been expensive, time consuming, and still only very partially effective.

It could be claimed that there is less X and RC material hosted in Australia as a result of the *Online Services Act*,[5] but there is no suggestion that this material is not equally available from overseas servers, or that it makes any difference to the ability to access content 'likely to cause offence to a reasonable adult.' The quantity of such material available on the internet, and without any access restrictions for Australian users, suggests that even a complete removal of Australian-hosted RC and X material from the internet (ie if the material was disposed of rather than moved overseas) would not have any impact on the ability to access virtually the same material from overseas.

3. Protecting children from exposure to internet content unsuitable for them.

There is no evidence that content unsuitable for children is any less available on the internet than it was prior to the enactment of the *Online Services Act.* However, heightened awareness of the internet, and of methods of dealing with childrens' access, may well have gone some way toward fulfilling this aim. If for example, community education has been successful, it may be that more schools, libraries, parents and carers now supervise better, and / or use products and

[5] If for example content has been removed due to take-down notices, and not simply re-hosted elsewhere. There is no evidence however to this effect, while there is evidence that at least some content has been moved overseas to avoid the provisions of the Act. See *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000 above n 2.*

techniques enabling closer control over, or restriction of, what children access on the internet.

The community education activities resulting from the *Online Services Act* are discussed above.[6] NetAlert and the ABA, for example, both provide information on their sites, and NetAlert produces other material also (such as fridge magnets and mouse pads!) to educate children and adults about internet dangers and tips for safer internet use. However, neither the ABA nor NetAlert is able to show any evidence that there has been any change at all in the protection of children from unsuitable or harmful material, although the Review of the *Online Services Act* provided a perfect opportunity for both bodies to do so.

NetAlert's submission to the Review unfortunately appeared to include only self-serving statements made in an attempt to secure further funding.[7] It included no evaluation of its first three years, except to claim that those three years have been very successful, and have placed it well to continue and expand its role into the future. It claims that during the past three years it has 'unearthed a clearly demonstrable and unmet need within the Australian community at large to be fully engaged and brought to the co-regulation table.' Given that NetAlert's specific brief was community education, it might have been expected that its Review submission would include some evidence as to how it has operated and what it has achieved in terms of community education, and the protection of the community from internet dangers. Rather, NetAlert lists highlights of its activities to include 'establishment of a corporate identity, establishment of management systems, information systems and corporate governance systems, appointment of Noni Hazlehurst as NetAlert ambassador, creation of a toll free helpline and email response service, national advertising campaigns, creation of information resources to provide practical advice and information to the community, introduction of NetAlert to state and territory stakeholders, conduct of comprehensive research into access management technologies, presentation of

[6] See Chapter 11: Community education.
[7] There had been concern that NetAlert would not be further funded and would be forced to close down. See for example Senator Kate Lundy, *Coalition ignores net education – NetAlert to be wound up*. Media Release, (6 March 2003).

information seminars for industry, and seeking out and building relationships with international counterparts.'[8] Unfortunately, this is the full extent of NetAlert's analysis and evaluation of its role over the first three year's of the *Act's* operation.

NetAlert may in fact have conducted some community education which may have helped in the *Online Services Act's* third objective of protecting children, although there is nothing to demonstrate that that is the case, and there are suggestions that NetAlert's community education may not have been particularly engaging. By November 2002 for example, only one third of public libraries had even heard of NetAlert, and far fewer had actually dealt with the body. Also, there is evidence to suggest that regardless of any community education initiatives undertaken, children are still able easily and readily to access unsuitable content. The Australia Institute survey conducted in 2003 found that Australian teenagers continued to have easy access to extremely explicit content on the internet.[9]

B. *Evaluation*

It can be seen from the above that although there is a complaints mechanism in place, it could not be said that the *Online Services Act* has really achieved all its stated aims. It must be remembered though that these aims were all subject to the regulatory intent that 'public interest considerations be addressed in a way that does not impose unnecessary financial and administrative burdens on Internet content hosts and Internet service providers.'[10] It may be said that any further achievement of the stated aims would in fact have placed 'unnecessary' financial and administrative burdens upon the internet industry, and perhaps upon others also.

---

[8] NetAlert, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 'highlights.' In fact, of a 43 page submission, NetAlert's activities over the past 3 years take up just over one half page, comprising 10 bullet points of highlights!

[9] Clive Hamilton & Michael Flood, Australia Institute, *Youth and Pornography in Australia; Evidence on the extent of exposure and likely effects* (Feb 2003).

[10] *Broadcasting Services Act 1992* (Cth) s 4 (3)(a).

In fact, there is nothing to suggest that these aims could have been achieved without huge expense to one or more of users, government, and the internet industry. To actually achieve the aims the costs may have been of such magnitude as to outweigh the economic, social, educational and other benefits of the internet to Australia and Australians. To restrict specified content from adults and children would require either a closed internet, with only approved material being allowed in, or an open internet combined with a massive amount of monitoring and blocking of content. The former would allow only a tiny proportion of the mass of available internet material into Australia, and would restrict access to legal and illegal content alike. The latter would require an incredible amount of time and expense to be even partially effective. Both would change the nature of the internet as it is known in Australia, and still the restrictions would not be complete. Many methods could be used to circumvent the former, even methods as simple as making a long distance call to log on to the internet via an overseas ISP. The latter would still allow access to illegal material as a result of the sheer impossibility of monitoring even a small proportion of content on the internet.

It would be easy simply to say then that the aims of the *Online Services Act* have not been met, but perhaps it is a good thing that they have not been. While real content restrictions are in place in some countries, at great expense, and with considerable infringements to freedom of speech, no other western democratic country has attempted regulation as broad as the *Online Services Act.* Many such countries have in place however regimes for managing concerns about internet content as effective as Australia's, and in some aspects more effective, without having attempted the breadth of control which the Australian government seemed set upon.

Paradoxically, had the Australian Government attempted less, it may have achieved more. If, instead of insisting on regulating online content as offline content is regulated, the Government had looked more at the differences between the media, it may have introduced a more effective scheme for dealing with internet content. Currently however the scheme in place is ineffective to a great

degree, and as can be seen from studies and submissions to the Review, the *Act* itself is still cause for considerable concern.

However, rather than simply writing off the Australian scheme as ineffective, it is worth looking also to what is currently being done in this area overseas. From that we might get a better picture of alternative methods of allaying concerns about internet content in a country like Australia, as well as some specific ideas regarding change for the future improvement of the Australian scheme. The next chapter thus looks to what has been achieved in this area in other comparable jurisdictions, and drawing on that the following chapter makes suggestions for improvement of internet content control in Australia.

CHAPTER FOURTEEN: COMPARATIVE CONTENT CONTROL.

The previous chapter evaluated the *Online Services Act* against its own stated aims. However, to appreciate more fully both its flaws and its achievements, it is necessary to place the scheme within an international context. Other countries are also grappling with concerns about internet content, and examination of their activities gives a broader basis from which to view both the possibilities and the limitations in this sphere. This chapter thus concentrates on some current overseas approaches to internet content control.

It has been claimed that the Australian scheme for internet content regulation has become a 'benchmark for many jurisdictions around the world...'[1] Net Alert states that there is '...very high regard for the scheme [in] overseas jurisdictions'[2] [It is] 'widely accepted both in Australia and internationally, that the Australian model has developed into one that works extremely well.'[3] According to the IIA 'Australia can rightly be said to possess one of the most advanced systems of internet governance in the world.[4] Optus asserts that the 'Australian Internet content regime is widely recognised internationally as one of the most effective regimes for the management of Internet Content in the world.'[5]

Unlike the above-mentioned Australian claims, the submission of Childnet International noted only that 'the Australian model has become one of the approaches for countries to consider and compare themselves against.'[6] Although content regulation in many countries does share some aspects with the Australian

---

[1] NetAlert, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 4.
[2] Ibid 8.
[3] Ibid 12.
[4] Internet Industry Association (IIA), *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 13.
[5] Optus, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 23.
[6] Nigel Williams, Childnet International, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 4.

scheme, there is no evidence that any country has moved toward, or is moving toward, the Australian scheme for internet content regulation.[7]

The discussion below focuses on relevant overseas attempts to deal with internet content. Although no country can be said to be 'the same as Australia' for the purpose of content regulation, the global nature of the internet means that many other countries have faced the same dilemnas as Australia in this sphere. It is thus useful to look at what they have done in response to this problem.[8]

A. *Use of local general law.*

While many countries have attempted to use general national laws to control internet content, such attempts have commonly been unsuccessful. In Norway, Germany, and France for example the use of local law has not succeeded, and these attempts have evidenced the unsatisfactory nature of this approach to controlling internet content.

In Norway for example, a Norwegian ISP succeeded on appeal against charges it had negligently spread illegal pornography on the internet.[9] While the charges were brought and the company convicted under local Norwegian law, it was overturned on appeal as conflicting with the *European E-Commerce Directive*, which stated that only willful acts, and not negligent ones, could lead to such a conviction.[10] Had the conviction been upheld in this case, and had other ISPs also been prosecuted, it may have made this content less accessible within Norway *to*

---

[7] For a discussion of online content regulation prior to the *Online Services Act* see above Chapter Four: Overseas content control prior to the *Online Services Act*. For a more recent survey of online regulation see Electronic Frontiers Australia, *Internet Censorship – law and policy around the world* (March 2002). Paper submitted to NSW Standing Committee on Social Issues, enquiring into Classification (Publications, Films and Computer Games) Enforcement Amendment Bill 2001. <http://www.efa.org.au/Issues/Censor/cens3.html> at 30 June 2004.

[8] For a summary of overseas schemes see Electronic Frontiers Australia, above n 7.

[9] Declan McCullagh's Politech, 'Norwegian ISP yanks Usenet newsgroups after child porn ruling.' <http://www.politechbot.com/p-03645.html> at 30 June 2004.

[10] Tele2 Norge Case, Bogarting Court of Appeal, 27 June 2003. Author has access to summary only, from Baker and McKenzie e-Law Alert 8/11/2003.

those using Norwegian ISPs, but it is likely the content would still have been readily accessible through other means.

In Germany an attempt to block content 'stirring up hatred against national, ethnic, racial or religious groups...' in breach of the local *Criminal Code* also failed, when ISPs outside the jurisdiction simply refused to co-operate with blocking requests.[11] Furthermore, even those within the jurisdiction were not effective in their compliance, as the orders failed properly to specify the content to be blocked, and the method of blocking.[12] As a result few of the ISPs served with the order were able to comply, while a number erroneously blocked additional content not subject to the order.[13] Regardless though of the action of the German ISPs, the content was still readily accessible from ISPs outside Germany.[14]

In France, a similar attempt to use local law to control internet content stirred international interest and concern, and is thus worth examining in detail. It was however likewise unsuccessful in controlling access to content.

In May 2000 the Superior Court of Paris handed down its decision in the case of *LICRA et UEJF vs Yahoo! Inc and Yahoo France.*[15] The plaintiffs in the case, LICRA, a group whose objects include combating racism and anti-Semitism, and defending the honour and memory of the departed, and UEJF, a Jewish student group, asked the court to find that Yahoo's advertising and sale of Nazi objects and memorabilia on and through its portals breached Article R.645-1 of the French Penal Code, and Articles 808 and 809 of the New Code of Civil Procedure, banalized Nazism, encouraged the propagation of anti-Semitism, and constituted an offence against the collective memory of a country profoundly

---

[11] CNN.com 'German official asks US ISPs to block neo-Nazi sites.' August 29th 2000 http://www.cnn.com/2000/TECH/computing/08/29/hate.sites.idg/index.html at 20 July 2004.
[12] Maximillian Dorseif, Government Mandated Blocking of Foreign Web Content, in Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Editors) *Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze*, Düsseldorf 2003, Lecture Notes in Informatics 617-648.
[13] Ibid.
[14] At this stage only the use of general laws to regulate internet content is discussed. German law relating specifically to the internet is discussed further below.
[15] *LICRA et UEJF vs Yahoo! Inc and Yahoo France,* Tribunal de Grande Instance de Paris (Superior Court of Paris), *22/5/2000 , English translation at* <http://www.gyoza.com/lapres/html/yahen.htm>

wounded by the atrocities committed by and in the name of a Nazi criminal enterprise.[16] The plaintiffs requested that Yahoo France and Yahoo Inc (US), which lists and displays Nazi items and memorabilia on its auction site, be ordered to make that material inaccessible in France, and that the court impose heavy fines for breach of such orders.[17]

There was no dispute that the site was accessible from France, that such objects were available for sale through the Yahoo Inc auction site in the USA, nor that the advertising and selling of these objects would breach the French Codes. Although Yahoo's French site had no involvement in this selling or advertising, it did provide French web users with links to the US site.

Yahoo France defended itself on the grounds that the French site was not in breach of the Codes as it did not participate in the selling or advertising or display of the items. The court accepted that Yahoo France was not itself hosting advertisements or auctions for Nazi items. However, as a result of the links available from Yahoo France to Yahoo Inc's (US) auction site, the court ordered Yahoo France to warn internet users that they must terminate their connection if the result of their searches (on Yahoo Inc (US) through links on Yahoo France) led to sites, pages, or forums the title or contents of which constituted a breach of French law.[18]

This finding against Yahoo France itself raises broader questions. As Yahoo France and Yahoo Inc (US) are separate entities, on what basis is the former required to warn about material on the latter? Would the decision be the same for any internet search engine and any internet portal which provides links to the Yahoo Inc (US) site, or does the name Yahoo France give it an apparent connection which gives rise to greater responsibility? While this aspect of the decision is beyond the scope of this thesis, it is likely to be an important issue in the future, and certainly deserves closer analysis.

[16] Ibid p7.
[17] Ibid.
[18] Ibid p10.

For Yahoo Inc (US), the defence disputed the jurisdiction of the French court, claiming that the action complained of was committed on the territory of the United States, and could not therefore be in breach of the French Penal Codes. The defence also claimed that it would be impossible for Yahoo Inc (US) to comply with the orders requested by the plaintiffs as it would be technically impossible to identify which of those internet visits to the US Yahoo's auction site were initiated in France.

The Superior Court of Paris was not persuaded by this defence, and upheld the plaintiffs' claims. On the issue of jurisdiction, the court held that although the action of Yahoo Inc (US) in placing this material on a server occurred in the US, by 'permitting the visualization *in France* of these objects, and [permitting] the participation of a surfer *in France*[19] in such an exposition / sale, Yahoo! Inc thus has committed a wrong on the territory of France,'[20] and the matter is therefore within the competence of the court.[21] As a result the Court ordered that Yahoo Inc (US) 'take such measures as will dissuade and render impossible any and all consultation on Yahoo.Com of the auction service for Nazi objects...'[22]

As for technical difficulties in screening out French users, the court found the obstacles to identifying the geographical location of users and blocking their access to certain content were real but not insurmountable.[23] It gave Yahoo US two months grace to make arrangements to carry out the court order, and to report back to the court on the measures it intended to implement.[24]

After studying its options, Yahoo Inc (US) returned to Court in July claiming that it was not technically feasible to block French web users from accessing its site. The court, dissatisfied with this response, asked a panel of international experts to identify ways in which Yahoo could screen out visits initiated in France.

---

[19] Italics added.
[20] Ibid p7.
[21] Ibid p7.
[22] Ibid p10.
[23] Ibid p8.
[24] Ibid p11.

Unfortunately for Yahoo, the experts advised the court that multi-level filtering systems could be used to block the great majority of French visits to the Yahoo Inc (US) auction site, and on November 20th 2000 the court confirmed the rulings made in May.[25] That is, it ordered that Yahoo Inc (US) 'take all measures likely to dissuade and make impossible[26] any consultation on Yahoo.com of the service of auction sale of Nazi objects and any other site or service which constitute an apology for Nazism or a dispute of the crimes of Nazism.'[27]

It was also argued on behalf of Yahoo Inc (US) that such a ruling would be contrary to the 1st Amendment of the US Constitution, and that Yahoo could not therefore comply with it. The French court treated this as nonsense. Firstly, the French court was interested only in what people did in France, and not in the US. Secondly, the court pointed out that in other areas Yahoo made selective choices about what material to carry or refuse to carry; it does not see itself bound for instance to carry on its auction sites live animals, human organs or drugs.[28] There was no constitutional 'guarantee of freedom of thought and expression' restricting Yahoo Inc (US) from blocking Nazi material.[29]

However, although the decision in this case appeared to herald a breakthrough in nations taking control of the internet in their own jurisdictions, enforcement of the order against Yahoo Inc! in the USA was subsequently refused by a court in the USA.[30] Thus the French Court's concern that the content was inimical to France's anti-nazi stance was irrelevant, and the content complained of, hosted as it was in the USA, remained accessible to users in France.

---

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

[26] Compare the wording of the Australian legislation, which requires ISPs only to; 'take all **reasonable steps** to prevent end users from accessing the content.' *Broadcasting Services Amendment (Online Services) Act 1999* (Cth) s40(1)(c).

[27] *LICRA et UEJF vs Yahoo! Inc and Yahoo France,* Tribunal de Grande Instance de Paris (Superior Court of Paris), 20/11/2000 http://www.gigalaw.com/library/france-yahoo-2000-11-20.html p1.

[28] Ibid p15.

[29] Ibid.

[30] *Yahoo! v. La Ligue Contre Le Racisme et L'Antisemitisme*, No. C-00-21275-JF (N.D. Cal. Nov. 8, 2001).

B. *International Approaches.*

It is apparent that the attempts of individual states to use general laws to regulate access to internet content are rarely effective in actually preventing access to the content. There have thus been some endeavours at an international level to attempt to control or regulate internet content. Given the global nature of the internet, and the desire of so many states to control its content, it may be thought surprising that there have not been more such endeavours. A major stumbling block has been the extreme variations in what individual countries wish to have regulated, and why, and how.

It would be tremendously difficult to find even one type of content that all, or even most nations believed should be censored, and would be willing to actively censor. For example France and Germany do not want their citizens to access hate speech/ vilification/ nazism, but free speech principles in the USA protect it; probably no-one wants their citizens to access child pornography, but other pornography is not so clear; pro-democratic material would be a positive for some and a negative for others, likewise anti-democratic material, pro-communist material and so on. As Lessig and Resnick note: 'What constitutes "political speech" in the United States (Nazi speech) is banned in Germany; what constitutes "obscene speech" in Tennessee is permitted in Holland; ...what is harmful to minors in Bavaria is Disney in New York.'[31]

The most 'international' move regarding internet content regulation is the *Convention on Cybercrime* drafted by the Council of Europe.[32] This convention covers a vast array of computer related topics. In relation to content control it requires signatories to criminalise certain behaviour, and to set up frameworks for the prosecution of relevant offences. While this has been both hailed (at last a step toward controlling what happens on the internet) and decried (losing sovereignty and individuality to other states or the international community), it appears that

[31] Lawrence Lessig and Paul Resnick, (1999) *Zoning Speech on the Internet: A Legal and Technical Model* Michigan Law Review 98 (2) 395-431, 395.
[32] Convention on Cybercrime (No. 185)
<http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm> at 1 August 2004.

this treaty also will do little really to regulate online content even within signatory states. The only section of the convention which deals with content related offences deals only with child pornography. Article 9 Paragraph 1 of Title 3, 'Content-related offences,' requires signatories to establish as criminal offences:
a) producing child pornography for the purpose of its distribution through a computer system;
b) offering or making available child pornography through a computer system;
c) distributing or transmitting child pornography through a computer system;
d) procuring child pornography through a computer system for oneself or for another;
e) possessing child pornography in a computer system or on a computer-data storage medium.

Paragraph 2 states that for this purpose 'child pornography' includes pornographic material that depicts:
a) a minor engaged in sexually explicit conduct:
b) a person appearing to be a minor engaged in sexually explicit conduct;
c) realistic images representing a minor engaged in sexually explicit conduct.
Paragraph 3 states that the term 'minor' shall include all persons under 18 years of age.

However, while Article 9 appears minimal at most, signatories have the right to agree to even less; they may require a lower age limit, terming a minor as under 16 rather than 18 years, and also need not apply, in whole or in part, paragraphs 1(d) and 1(e), and 2(b) and 2(c). The minimum required under the Treaty is therefore: signatories must establish as criminal offences:
a) producing child pornography for the purpose of its distribution through a computer system;
b) offering or making available child pornography through a computer system;
c) distributing or transmitting child pornography through a computer system;
'child pornography' includes pornographic material that depicts:
a) a minor under 16 years engaged in sexually explicit conduct.

Not only was the outcome minimal in terms of what it prohibited regarding internet content, but to get even to that stage the Convention took over 40 drafts with input from over 30 countries. It was opened for signature and first signed on 23rd November 2001. It came into force on 1 July 2004, having received only six ratifications.[33]

Unfortunately, the effectiveness of the *Convention on Cybercrime*, like most other attempts to regulate internet content, will falter on the issue of jurisdiction. While individual signatory states agree to act to criminalize and to prosecute certain actions, content prohibited under the Convention will remain available and accessible from servers outside the jurisdiction, unless most of the world takes up the Convention. While member countries may be able to limit some acts in accordance with the convention, and prosecute those hosting, making, selling or distributing certain content within the jurisdiction, the content itself is likely still to be accessible within member countries.

In addition to the *Convention on Cybercrime*, a *European Union Directive on Ecommerce* was issued in 2000.[34] While this directive generally relates more to commercial computer related activities than to content regulation, it includes requirements that European member states should not impose general obligations on ISPs either to monitor the information which they transmit or store, or to actively seek illegal activities on the network.[35] States may however compel ISPs to inform public authorities about illegal data or infringements reported to them, and ISPs may also be required to divulge to public authorities the identities of subscribers.[36] Under the *Directive,* ISPs can be asked to terminate or prevent an infringement under the law of their own state,[37] but they will not be held liable for

---

[33] Chart of signatures and ratifications to Convention on Cybercrime <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm> 1 August 2004

[34] The Directive can be found in English at <http://www.spamlaws.com/docs/2000-31-ec.pdf> at 30 June 2004.

[35] Article 15.1.

[36] Article 15.2. Meaning and effects of the Directive are also discussed in Frydman and Rorive, above n 32, 52ff.

[37] Articles 12.3, 13.2, 14.3.

material where they take only a passive role, so long as they are not aware of the material or activity and they remove it upon receiving such knowledge.[38]

These international initiatives will do little to restrict the availability of internet content. Other initiatives such as hotlines, codes of practice, content labeling, and community education, while not restricting content, may help users to control or deal with internet content for themselves, and for those in their care. Active policing can also help to deal with content at its source. Some of these are currently in place in Australia and overseas. Those in Australia have been discussed above, and it is worth examining relevant overseas activities also.

C. *Codes of Practice*

Although legislation aimed at controlling internet content was proposed in the New Zealand Parliament in the early days of the internet, it was not passed and a voluntary Code of Practice was instead recommended.[39] Industry groups and others, concerned that there may be more attempts to legislate to control the internet,[40] got together to launch what is now the Internet Code of Practice, and which has the endorsement of the New Zealand Government.[41] While good commercial practice appears to be a priority, the aims of the Code also include protecting rights of access and free speech, ensuring information and procedures are in place to protect minors from accessing objectionable material over the internet, and ensuring information and procedures are in place so internet users know how to limit access to protect a user from accessing inappropriate or objectionable material.[42] It is worth noting that NZ ISPs are voluntary subscribers

---

[38] Articles 13.1(e), 14.1(b).
[39] Electronic Frontiers Australia, above n 7, 11: 'New Zealand.'
[40] *Netsafe, The Internet Safety Group website,* 'Internet Infrastructure' <http://www.netsafe.org.nz/infrastructure/infrastructure_default.asp> at 1 August 2004.
[41] Ibid.
[42] InternetNZ, *Internet Code of Practice,* Article 1 (1999) http://www.internetnz.net.nz/icop/icop99the-code.html at 30 June 2004.

to the Code of Practice, and it is up to individual ISPs to decide how they will go about ensuring such things. InternetNZ does not police compliance.[43]

The NZ Code of Practice proposes that internet content be subject to the NZ *Films, Videos and Publications Act* 1993, and in fact annexes relevant parts of that Act to the Code.[44] The Code of Practice requires members operating commercial or public sites to inform clients of whether they take responsibility for the sites' content, or whether they are only carriers of information. They are also required to work toward systems of content recognition and tagging of content suitable for children.[45] Commercial and public sites hosting adult services must ensure that they are classified in accordance with a commonly used classification system such that users may reasonably be able to exclude unwanted material, and that warnings as to content are given on the home or title page, and/or that subscription to such sites excludes under-aged subscribers. Members are also to work toward and support the adoption of a system of content identification for adult services.[46] ISPs are responsible for informing 'parents and other responsible persons of options and precautionary steps they can take to ensure that vulnerable groups are protected and to monitor usage.'[47] They must offer links to material helping to educate users and guardians, including links to software which can be purchased to help protect minors from accessing objectionable material over the internet.[48] All of the above provisions are guidelines to govern and guide the practice of ISPs in New Zealand. InternetNZ is not a regulatory body and has no ability to enforce the Code of Practice. It tries rather to modify the behaviour of the internet industry through encouragement and leadership.[49]

Again without government intervention, the Internet Service Providers Association in the United Kingdom (ISPA, UK) has adopted a Code of Conduct

[43] Email from Keith Davidson, President, Internet NZ, to author. 24 August 2003.
[44] InternetNZ, *Internet Code of Practice*, above n 42, Article 3.4.
[45] Ibid Article 3.5.1. For example the use of ICRA labels.
[46] Ibid Article 3.5.2.
[47] Ibid Article 4.1a.
[48] Ibid Article 4.1b.
[49] Keith Davidson, above n 43.

covering a wide range of matters.[50] Application of the Code is uniform and obligatory to all members, without modification or exception, although even strict compliance with the Code will not guarantee that members are acting within the law.[51] An early version of the UK Code of Practice was discussed above,[52] but the Code has developed considerably since that time.

The ISPA UK Code begins with three core principles. Firstly, it encourages the emergence of technologies which will give parents and consumers choice regarding the content to which they wish to (or not to) have access. Secondly the Code states that providers of content are responsible for ensuring that the content is not illegal, and that it is suitable for its intended audience. Thirdly, the Code provides that any censorship or filtering should be carried out by government, and that ISPs should not be responsible for determining legality or suitability of content, or for filtering or restricting access. The Code states support however for any member who 'proactively limit(s) the accessibility of illegal material via its service.'[53] The Code also requires members to provide information to customers about tools which may assist in filtering unwanted content.[54] While the UK ISPA takes no responsibility for content, it does co-operate with the Internet Watch Foundation (see below) to remove illegal material (see below) from web sites and news groups.[55] Members agree that where notified by IWF of illegal child pornography, members will remove such material whereever it is technically possible to do so.[56]

The co-regulatory system in place in Singapore involves a great deal more government control of the internet industry and content providers than do the UK and NZ approaches. Many commentators note that while the law regulating internet use in Singapore appears to be based on self-regulation, in reality,

---

[50] UK, Internet Service Providers Association (ISPA) Code of Practice, can be found at <http://www.ispa.org.uk/html/index3.html?frame=http%3A//www.ispa.org.uk/html/about_ispa/ispa_code.html> at 30 June 2004.
[51] Ibid preamble (a) & (f).
[52] See above Chapter Four: Overseas content control prior to the *Online Services Act*.
[53] UK, Internet Service Providers Association (ISPA) above n 45, Statement of Policy.
[54] Ibid 7.2, 7.3.
[55] Ibid 5.1.
[56] Ibid 5.3.

political factors make the internet content control regime extremely harsh, 'demanding total compliance and subjugation of its citizen-subjects.'[57] Thus while the following discusses outward manifestations of the Singaporean scheme, it must be remembered that the politics of the society within which it operates may make its effects more significant that its specific requirements would suggest.[58] Nonetheless, it is included here as many aspects of the scheme coincide with those found in Australia and in a number of other countries.

The Singapore Industry Code of Practice is produced by the Media Development Authority, and enforced by that Authority also.[59] Non-compliance can lead to fines, imposition of license conditions or even loss of license.[60] A class license scheme requires registration of many participants in the internet industry, including ISPs and ICHs, political parties providing content on the internet, and anyone else within Singapore propagating, promoting or discussing political or religious issues relating to Singapore.[61] Under the Internet Code of Practice 'licensees' must use their best efforts to ensure that 'prohibited material' is not broadcast via the internet to users in Singapore.[62] ISPs are not required actively to monitor material they carry,[63] nor are hosts required to monitor material they host over which they do not have editorial control,[64] but must block or remove

---

[57] Terence Lee, Internet Use in Singapore: Politics and Policy Implications, *Media International Australia*, No 107 May 2003 75, 77.
[58] See James Gomez, *Internet Politics; Surveillance and Intimidation in Singapore* (2002), Terence Lee, above n 43, Terence Lee, 'Internet Regulation in Singapore: A Policy/ing Discourse' *Media International Australia*, No 95 May 2000 147, Terence Lee, 'The Politics of Internet Policy and (Auto) Regulation in Singapore' *Media International Australia*, No 101 November 2001 33.
[59] Singapore Internet Code of Practice 1(1)-(2). http://www.mda.gov.sg/medium/internet/i_codenpractice.html at 18 August 2004.
[60] Ibid.
[61] Singapore Media Development Authority: Registration of Internet Class Licencees, http://www.mda.gov.sg/medium/internet/i_register.html at 18 August 2004.
[62] Singapore Internet Code of Practice, 2 http://www.mda.gov.sg/medium/internet/i_codenpractice.html at 18 August 2004.
[63] Media Development Authority : Internet Industry Guidelines, 16, http://www.mda.gov.sg/medium/internet/i_guidelines.html at 18 August 2004, and see Anil, S. 'Re-Visiting the Singapore Internet Code of Practice,' 2001 (2) Journal of Information, Law and Technology, 3.1.
[64] Media Development Authority : Internet Industry Guidelines, 16. http://www.mda.gov.sg/medium/internet/i_guidelines.html at 18 August 2004

prohibited material of which they become aware, or of which they are notified by the MDA.[65]

Codes of Practice in Australia are similar to and different from the above. In Singapore the MDA drafted the Code of Practice for industry, in NZ and the UK industry itself drafted the regulatory codes. The Australian Codes of Practice lie somewhere in between; the codes were drafted by the industry, but legislation directed what should and should not be included.[66] The legislation also allowed for the ABA to set industry standards if the industry itself did not do so or if the codes drafted by the industry were inappropriate.[67] Regarding enforcement, in NZ code compliance is entirely voluntary. In the UK code compliance is mandatory for members of the ISP association, but membership itself is not mandatory. In Singapore code compliance is mandatory and licenses may be revoked for non-compliance. In Australia code compliance itself is not mandatory, but if the ABA becomes aware of non-compliance it may issue a notice directing an industry participant to comply with the code.[68] Failure to comply with that direction will be a breach of the *Online Services Act* and may lead to fines, or prohibition from hosting or providing internet services.[69] In respect of Codes of Practice, and a self or co-regulatory approach, Australia appears to be fairly well in line with a number of other similar countries.

D. *Hotlines, community education, and policing.*

Unlike most western countries, Singapore has considerable government involvement in all aspects of internet content control. As the Government of Singapore has been outspoken in its encouragement and provision of internet services in Singapore, it has also been proactive in ensuring the availability of community education and appropriate internet services. In response to parental

---

[65] Ibid.
[66] *Broadcasting Services Act* 1992 (Cth) schedule 5 cl 60-61.
[67] Ibid cl 68-71.
[68] Ibid cl 66.
[69] Ibid cl 79-80, 82-85.

concerns about children's access to inappropriate content, the SDA worked with a number of major Singaporean ISPs to develop optional 'family friendly' subscription services, which filter services at ISP level, and avoid the need, for those who want filtered services, to use end-user filtering technology.[70] Further, the MDA oversees the voluntary Parental Advisory Group for the internet (PAGi), which has been very active in the provision of information and education for internet users, parents and supervisors.[71] While the SBA has overseen this work, PAGi has drawn upon and grown out of considerable community interest and concern relating to internet content. The MDA has recently won awards for its promotion of child safety online, and for excellence in internet awareness.[72]

In many other countries, hotlines, community education and policing go almost hand-in-hand. Bodies which operate hotlines to receive complaints also give advice and provide community education, and they tend not to be government bodies. These bodies then pass relevant information to the police.

For example, rather than a government-based approach, New Zealand has broad and diverse representation in cyber matters. The Internet Safety Group was founded in 1998 by a group comprising a rape and sexual abuse prevention agency, a secondary school, a police sexual abuse team, an ISP and a sexual offender treatment program.[73] From this clearly grassroots beginning, the Internet Safety Group has expanded to include representatives of the Department of Internal Affairs (censorship), the Department of Child, Youth, and Family Services, the Department of Courts, the Customs Service, the Ministry of Education, businesses, community groups, educators, students and parents.[74]

---

[70] Singapore Media Development Authority, *Family Access Networks* <http://www.mda.gov.sg/medium/internet/i_family.html> at 30 June 2004.
[71] Singapore Media Development Authority, *Parents Advisory Group for the Internet* <http://www.mda.gov.sg/committees/i_pagi.html> at 30 June 2004.
[72] Singapore Media Development Authority, *Singapore receives world wide awards for promoting internet safety.* Media Release (10 March 2004) http://app.mda.gov.sg/scripts/MDA/news_room/press.asp?id={D16AE2F3-EFFD-4A52-876C-004F297145DE}&type=date&content= at 9 August 2004.
[73] Liz Butterfield, 'NetSafe: The New Zealand Model for Internet (ICT) Safety Education' (Paper presented at NetSafe: Growing Australia Online Conference, Canberra, Dec 2002) 2.
[74] Ibid.

The Internet Safety Group has developed an internet safety kit for schools, distributed information regarding internet safety and education to every New Zealand school, and developed a website including all that information and more. It has been working to develop lesson plans for use in schools, and a study in June 2001 found 82% of New Zealand schools addressing inappropriate use of the internet.[75] The Internet Safety Group has also formed a permanent alliance with over 140 police youth educators across NZ. To ensure continuing engagement from all sectors of the New Zealand community on the issue of internet safety, in 2002 the Group ran a national symposium with over 100 people invited from a wide selection of government departments, community groups and workers, the education sector, researchers, and law enforcement. In 2002 the Group won the International Law Enforcement Cybercrime Award,[76] for innovation and best practice pertaining to prevention, detection, and / or response to cybercrimes.[77] There is interest now in introducing the NZ schools education scheme in both the UK and USA.[78]

In the USA the National Center for Missing and Exploited Children (NCMEC) provides community education regarding internet dangers. The Centre offers considerable training programs for legal, law enforcement, healthcare, and education professionals, as well as for children and parents. The training focuses on protection of children rather than the dangers of the internet per se, and topics of courses run by the Centre range from school and online safety to technical issues regarding responses to missing child cases. NCMEC also run a website offering interactive internet safety tips and activities for children, and links to further information for parents and other adults.[79]

---

[75] Ibid 5.
[76] From the Society of Policing of Cyberspace. For more information about this body see its web site: http://www.policyb.org/ at 1 August 2004.
[77] Liz Butterfield, above n 73, 12.
[78] Email to the author from Liz Butterfield, Director, NZ Internet Safety Group, 28 July 2004
[79] National Centre for Missing and Exploited Children, *Annual Report 2003*. <http://www.missingkids.com/en_US/publications/NC92part1.pdf> at 1 August 2004.

Similarly, the non-profit Internet Education Foundation runs educational and informative web sites for children and adults such as 'GetNetWise'[80] which offers internet safety information, and links to many other information sources. The Internet Education Foundation is 'dedicated to educating the public and policy makers about the potential of a decentralised global Internet to promote democracy, communications and commerce,' and while it is financially greatly supported by the internet industry, it also has significant input from non-industry groups.[81]

In regard to control of obscene content, organisations such as 'Morality in Media' receive complaints about what is believed to be illegal content, and lobby for prosecution of individuals and businesses acting illegally in this regard. Morality in Media offers an online hotline for reporting on their 'obscenitycrimes.org' website, and reports are forwarded to State or District Attorneys for investigation and prosecution. Morality in Media keep a watching brief on the results of those reports.

The 'CyberTipline,' run by the private, non-profit National Centre for Missing and Exploited Children, receives reports relating to child pornography, online enticement of children, child prostitution, child-sex tourism, child sexual molestation, and unsolicited obscene material sent to a child. The NCMEC take an interest in all child abuse issues, not just those which occur online. As the Centre has been running since 1984, it has a great deal of expertise in child protection, and not just in internet related matters. The NCMEC makes a very clear distinction between reporting which relates to danger to children, which is accepted by the CyberTipline, and that which amounts rather to complaints about obscenity, which the CyberTipline web site states should be reported instead to obscenitycrimes.org, and a link to that site is provided. Reports relating to child abuse or child pornography are analysed by NCMEC and then submitted to law enforcement agencies.[82]

---

[80] <http://www.getnetwise.org/about/> at 30 June 2004.
[81] <http://www.neted.org/> at 30 June 2004.
[82] National Center for Missing and Exploited Children, above n 79.

In the United Kingdom the Internet Watch Foundation is the body taking most responsibility for monitoring content on the internet. The IWF was initially an industry dominated body, but is now directed by a Board made up of four people from the industry, and eight others from outside the industry. The Board Constitution was changed in this way to ensure that the IWF was sufficiently independent of industry to make decisions which may not be thought to be in the industry's interest.[83] It operates a hotline which receives and investigates complaints regarding child pornography from anywhere in the world, and also receives and investigates complaints regarding other material illegal in the UK, such as obscene content contravening the UK *Obscene Publications Act* 1959, and racist content contravening the *Public Order Act* 1986.[84] The hotline, which receives about 400 complaints per week, specifically discourages complaints on the basis of individual taste, stating that IWF is 'concerned with the interpretation of the law, not personal taste, decency or morality.'[85] As the hotline co-operates with other hotlines around the world it is willing to investigate child pornography matters from anywhere in the world. However, regarding obscene adult content and racist content, the hotline is concerned only with content hosted in the UK, which can then be removed or prosecuted in the UK.[86]

As well as receiving complaints through its hotline the IWF actively monitors some newsgroups known to carry problematic material. Potentially illegal material gathered by the IWF is forwarded to UK police (when it appears a crime has occurred in the UK) or to the National Criminal Intelligence Agency.[87] The IWF also operates a 'notice & take down procedure' whereby illegal material hosted within the UK is notified to UK ISPs who then remove the offending material from their servers. Where the illegal material involves child abuse, discussions with police take place prior to notices being issued, both to confirm that the content is illegal, and to give police an opportunity of identifying

---

[83] About Internet Watch Foundation <http://www.iwf.org.uk/about/overview/index.html> at 30 June 2004.
[84] Ibid.
[85] Internet Watch Foundation Hotline, <http://www.iwf.org.uk/index.html> at 9 August 2004..
[86] Ibid.
[87] Ibid.

offenders before material is removed.[88] Where newsgroup material is identified as illegal, takedown notices are given as a matter of course, and ISPs co-operate fully with IWF in this regard. Some ISPs have even set up robots to automate the process of take-down in response to IWF notices. In addition, the IWF maintains a list of newsgroups which it recommends that no ISP should carry due to large volumes of illegal content, and compliance by ISPs with this recommendation has been 'virtually 100%.'[89]

The Internet Watch Foundation has two major functions beyond its hotline. Firstly, it encourages and promotes the development and use of voluntary rating systems, to allow users as far as possible to select or control the types of material they wish to access or restrict. Further, the IWF takes a community education role, for the protection of children and the community generally, providing information regarding safe use of the internet.

Policing is also a major factor in the UK and NZ. Vigorous and proactive investigation and prosecution of users of illegal internet material are another component of NZ's internet regulation. Because child pornography creates dangers for children in the making of the content itself, in creating a market for this material, and due to its role in 'grooming' children for sexual abuse,[90] the Censorship Compliance Unit of the Department of Internal Affairs focuses especially on this content. Even without internet-specific regulation, New Zealand police have identified over 500 New Zealanders involved with objectionable material on the internet. One hundred and three of those have been charged and convicted, while 25 cases are still pending. This unit in New Zealand also provides information to and receives information from overseas investigators and enforcement agencies.[91] Similarly in the UK, investigations into users of a particular paedophile portal in the US have led so far to 3537 arrests, 1679

[88] Peter Robbins, Chief Executive, Internet Watch Foundation, email to author 22 August 2003
[89] Ibid.
[90] Keith Manch and David Wilson, NZ Department of Internal Affairs, *Objectionable Material on the Internet: Developments in Enforcement* (2002).
[91] Ibid, and see also Jon Peacock, NZ Department of Internal Affairs, *Objectionable Material on the Internet and the Department of Internal Affairs Response* (undated).

prosecutions and 1230 convictions,[92] and 102 cases in which children were removed from the users / makers of child pornography.[93] Unfortunately in Australia the information regarding investigation and prosecution of internet crimes is not available.[94]

E. *Newer approaches.*

Finally, it is worth looking at recent approaches to internet content control introduced in Germany and Hong Kong.

In Germany content providers and the national internet industry association have both been given responsibilities recently for restricting content on the internet. When a German student - reported to have been an excessive player of video games - shot and killed several teachers and fellow students the German Government responded by amending and introducing legislation to reform the laws protecting children and young people.[95] The new law and amendments, which commenced in April 2003, are concerned with the availability of content overall, and not simply that available via the internet. However, along with content in other media, internet content is intended to be restricted by the changes.[96]

Under these laws, certain content must be kept away from children and young persons. Firstly, the Federal Office for Certifying Harmful Media is compiling a

---

[92] John Leydon, '102 kids saved from paedos.' *The Register,* 14 April 2004 <http://www.theregister.co.uk/2004/04/14/operation_ore_update/print.html> at 3 August 2004.
[93] Ibid.
[94] Requests for such information have been made to Australian Bureau of Statistics, Crime Statistics section; Australian High Tech Crime Centre; and Australian Federal Police, Media Section.
[95] *Jugendschutzgesetz* (*Juvenile Protection Act*) and *Jugendmedienschutz-Staatsvertrag* (*Agreement of the Federal German States Regarding the Protection of Human Dignity and Juveniles in Radio and Televised Media*), both discussed in Christoph Safferling, Mark Liesching, 'The Protection of Juveniles in Germany – A report on the New Legislation,' *German Law Journal* Vol 4 No 6 -- 1 June 2003 – Public Law, available at http://www.germanlawjournal.com/current_issue.php?id=279 at 18 August 2004.
[96] Christoph Safferling, Mark Liesching, 'The Protection of Juveniles in Germany – A report on the New Legislation,' *German Law Journal* Vol 4 No 6, June 2003, available at http://www.germanlawjournal.com/current_issue.php?id=279 at 18 August 2004.

list of harmful media, generally from complaints received. Secondly, content which is harmful or threatening both in an obvious way and to a high degree is prohibited whether or not it is listed. Such content can be made available over the internet in Germany so long as the content provider guarantees that children cannot access it, which requires the use of an age verification scheme. Simply clicking a mouse to state a user is over 18 is not sufficient for this purpose; the schemes which may be used are similar to the Australian restricted access systems.[97]

Less harmful content also requires access restrictions. For this content it is necessary, and sufficient, for providers to seriously impede the access of minors via a 'Youth Protection Program' (YPP). YPPs must be accepted as suitable by the Commission for Youth Protection in the Media, and the main form of YPP involves the use of content selection schemes and labeling of content.[98] To qualify as a YPP the labeling must use a rating system which differentiates content according to its appropriateness for specific age groups. Interestingly, filters based on site or keyword blocking do not qualify as Youth Protection Programs, as 'they do not pose a serious impediment to efforts by minors to access an Internet-site.'[99]

The German governments have devolved decisions relating to age limitations to the relevant industry bodies, and decisions of these bodies have a binding effect in this regard. Thus where providers consult their industry association for evaluation of the content being provided, and act in line with that, there will be no liability except in a case of 'grave misjudgement.'[100]

In response to these laws, ICRA reports a steady increase in the number of German sites using its labels.[101] The Managing Director of the German Internet Industry Association stated that the Association is 'sceptical of a lot of proposals

---

[97] Ibid. Restricted access systems are discussed above, Chapter Three: Methods of Internet Content Control, and Chapter Seven: Passage and Provisions of the Online Services Act.
[98] Such as Platform for Internet Content Selection (PICS) and Internet Content Rating Association (ICRA), discussed above in Chapter 3: Methods of internet content control.
[99] Christoph Safferling, Mark Liesching, above n 96.
[100] Ibid.
[101] Internet Content Rating Association, *Eco to be ICRA representative in German speaking countries*. (22 July 2003). http://www.icra.org/press/en_icradeutschland/ at 18 August 2004

made from time to time to create a child friendly Internet ending at German borders,' but supports the creation of a safer internet using multiple measures such as tackling illegal content at its source, and empowering users to regulate access from home computers.[102]

Labeling of internet content is also being heavily promoted in Hong Kong, but unlike Germany there is currently no legislative incentive involved. The Government of Hong Kong and the Hong Kong ISP Association (HK ISPA) have recently launched a joint initiative to encourage the voluntary labeling of content using the ICRA system. The project will include the translation and customization of the ICRA scheme for Chinese users.[103] In launching the project in June 2003 the Permanent Secretary for Commerce, Industry and Technology stated that 'the system can on the one hand protect young people and children from being exposed to offensive materials, on the other hand it can also ensure that freedom of speech and free flow of information will not be infringed.'[104] The labeling initiative in Hong Kong will be part of a program including community education and the provision of a hotline.

It should be noted however that Codes of Practice in Australia, New Zealand and the United Kingdom already encourage content providers to label content, but there appears to have been little uptake of labeling in these jurisdictions. In Germany, where there is legislative backing for labeling, the uptake has been greater. It will be interesting to see whether or not content providers in Hong Kong will embrace the system.

---

[102] Ibid, Harald Summa, Eco Managing Director.
[103] See Hong Kong ISPA, 'Objectives of ICRS Project' http://www.hkispa.org.hk/webpage.htm at 24 August 2004.
[104] Francis Ho, quoted in 'Internet content rating system is launched in Hong Kong.' Press release (10 June 2003). <http://www.info.gov.hk/gia/general/200306/10/0610207.htm> at 24 August 2004.

F. *Conclusion*

The above discussion of current overseas regimes for dealing with internet content leads to the conclusion that while the Australian scheme for internet content regulation has not been replicated, many aspects of the scheme can be found in varying forms in other jurisdictions. No country appears to have 'the answer' to internet content regulation, and no single scheme stands out as 'the most effective.'

It is clear that Australia is not the leader it is claimed to be. But equally it is not terribly out of step with other nations. Like Singapore, the Australian Government is more involved in content regulation than are governments in many countries, but in the operation of the scheme it is not dissimilar to many other nations. In fact the Australian scheme is out of step in its unrealistic aims far more than in its actual requirements. Nonetheless, in the light of the above it is clear that the Australian scheme, and specific aspects of it, could be improved upon, and suggestions for such improvements are examined in the following chapter.

CHAPTER FIFTEEN: RECOMMENDATIONS

Previous chapters have discussed the aims of the *Online Services Act* and the extent to which they have been achieved, the problems resulting from the current Australian regime, the continuing dilemmas of accessibility to inappropriate and illegal content, and a variety of methods used in other parts of the world to address internet content concerns. In the light of all of these, this chapter looks at where the Australian scheme might go in the future.

If the internet content control regime in Australia is to be improved, a fresh look at what the Government wishes to achieve would be the first step. Free from the hurried and hugely contentious atmosphere surrounding the enactment of the *Online Services Act,* the Government could now rethink the area in the light of what has and has not been achieved, and with more understanding of how internet technology has developed and is likely to develop. There is an opportunity for the Government to define more realistic objectives, prioritise competing aims, and develop a workable and effective regime in pursuit of those aims. However, having claimed that the *Online Services Act* is a great success, the Government is more likely to tinker at the edges than to overhaul the regime. But even tinkering at the edges may greatly improve the scheme, so long as that tinkering is intelligent and well informed.

It has become clear over the past four years that the need to regulate in a manner that 'does not impose unnecessary financial and administrative burdens on ICHs and ISPs'[1] is in fact a paramount concern of the present Government, and not simply a qualification to its other objectives. Government policy and consequent industry development over this period have made it clear that continued and increased technical and economic efficiency, and increased internet access and use, are most important aims in themselves. Thus, even if the Government wished more closely to regulate or restrict internet content, action conflicting with these aims is unlikely. Rather, it is probable that the Australian Government will

[1] *Broadcasting Services Act* 1992 (Cth) s 4(3).

continue to try to regulate internet content in an environment of broad penetration of inexpensive and efficient internet services. Broad penetration will include access for people from all walks of life, from young children to aged persons, in the city and the country, and from homes, schools, offices, libraries, cafes, and soon in fact anywhere a mobile phone can go. How best to manage internet content in such a setting?

As has been argued since the birth of the mainstream internet, unless all services are run through monitored or filtered servers, and perhaps not even then, real control over internet content originating outside the country will not be possible. The only chance of any such control is widespread international agreement. But as discussed in the previous chapter, there is little chance of a sufficient number of states agreeing on what content ought to be restricted, and restricting it. Even if a significant number of states did agree to restricting content, their limited jurisdiction would mean that content produced, hosted, or distributed from outside those states could not be made subject to these controls. Thus an agreement regarding content control, even between a large numbers of states, would be useless while other states were unwilling to comply, unless all material coming from non-complying states was blocked or monitored. If the states in question were small and 'unimportant' in the global scheme, governments may be willing to place blocks at gateways to exclude access to content from such states. But what happens where the USA, for example, is likely to be non-compliant?

The interpretation given by courts to the First Amendment of the United States' Constitution would ensure that the USA was not party to any agreement requiring effective content restrictions either on content produced, hosted or distributed in the USA, or on content coming into the USA from outside. Given that the USA produces such a significant proportion of internet content, no country embracing a strong and economically efficient internet would even contemplate blocking US content completely, and its sheer quantity would make its effective filtering or monitoring impossible. However, given that over 70% of the content notified to

filter makers comes from the USA,[2] there would be little point entering agreements to control internet content while continuing to allow free entry to material originating or coming through the USA.

It appears then that if Australia wishes to have any control over internet content, or at least any input into its management, it will need to act for itself and not to rely on agreements or changes at an international level. There are however many things which Australia could do for itself to improve the management of internet content. These are discussed in more detail below. They include active investigation and prosecution of those producing, using and distributing Refused Classification content; relaxation of restrictions on X-rated content; removing restrictions on R-rated content; removing the complaints scheme from the ABA to the police or the OFLC; classifying content according to its nature, rather than as film regardless of its nature; ensuring providers of content are involved in the scheme and as such are notified and given appeal rights when their content is questioned; researching and developing content management technologies; further pursuing the possibility of content labeling; and, most importantly of all, developing a wide-spread and effective community education scheme. Specific suggestions for change are discussed below.

A. *Specific Recommendations*

1. The internet industry.

Given that some form of co-regulation or self-regulation is the norm in other media and telecommunications industries in Australia, it is appropriate that the internet industry also should be subject to a co- or self-regulatory scheme. Given the ability of the industry to create and extend public knowledge and access to information, and its ability also to create harm through the hosting and carriage of illegal material, it is reasonable that the industry is overseen to some extent by a

[2] 71 out of 94 items; Fourth *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2001* Tabled in Senate by the Minister for Communications, Technology and the Arts (August 2002) 17.

governmental authority. The ABA is the appropriate authority to maintain such oversight. The general scheme for internet industry regulation fits well with those of similar industries, and as discussed above in Chapter Six, is to be preferred over both no regulation, and solely government regulation. The review of the *Online Services Act* found the co-regulatory framework to be well-supported.[3]

Industry codes should be required. They should continue to deal with matters such as the provision of information to subscribers, since the industry is in an excellent position to identify and give information to, especially new, internet users. The information given should preferably be realistic, and periodic rather than one-off. Codes should also continue to require ISPs to ensure their subscribers are over 18years old, as this attaches responsibility for internet use, and for younger users, to the adult who subscribed. This requirement should however be relaxed for institutions such as universities providing internet access to, for example, university students under 18 years, as the administrative burdens of such a requirement are enormous.[4] Codes of Practice should also deal with how ISPs and ICHs are required to deal with requests to remove content, or to block it (discussed further below). The Review of the *Online Services Act* also recommended periodic review of the codes to ensure that they continue to deal appropriately with technological and market developments.[5]

If the industry itself is to continue to be responsible for the drafting of Codes of Practice, it is essential that more of 'the industry' be involved. Membership and thus policy of the IIA are currently heavily slanted toward big business, which has both marginalised and alienated many in the industry.[6] Further, it makes research

---

[3] DCITA, *Review of the operation of Schedule 5 to the Broadcasting Services Act 1992; Report* (May 2004) 13.

[4] See Australian Vice-Chancellor's Committee, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (October 2002).

[5] DCITA, above n 3 45.

[6] A request by the author to an ISP list asking about how the IIA came to represent the internet industry in dealings with the government elicited the following responses: 'They simply declared themselves as such and started lobbying the Govt. In lieu of anyone else, the Govt seems to have accepted them as the 'representative body'.' 'I for one, welcome our new IIA overlords. not.' 'It appears they have the Telstra's and Optus' and their ilk as members, so therefore have such a large percentage of the total number of internet clients in Australia. Unfortunately the IIA appears to reflect the wishes ONLY of their big end of town players, and that's understandable because they do not have many of the medium and smaller ISP's as members. One would think it is because the

difficult; a number of requests for assistance or information from the author to the IIA have been either refused or entirely ignored. Interestingly, requests for similar information from the IIA's counterparts in NZ and the UK have elicited courteous and full responses within days. If we are to see the real potential benefits of co- or self-regulation, the Government and the ABA should try to ensure that the body 'representative of the industry'[7] is in fact representative of the industry. Possibly, there is a need simply to accept that there is not one truly representative body, and to deal with a number of representatives, possibly from various sectors of the industry. Small ISPs for example are in many respects a quite different constituency from the giant telcos.

While the internet industry should not be making *decisions* regarding content control, it should perhaps be asked to engage in real policy making. Unfortunately, in attempting to avoid regulation initially, much of the industry claimed simply that it was impossible to censor or control internet content. Had there been more engagement of industry and government in the lead-up to the *Online Services Act* a better scheme may have ensued. Even now it would be useful to have people in the industry (and not simply the IIA as representative), engage with policy makers, censors, educators, police, psychologists and child welfare authorities to discuss and formulate workable policy for internet content.

2. Receipt of complaints

It is undoubtedly a good thing to offer those worried about internet content a means to have their complaints and concerns heard. It may help to allay fears about the internet, encourage internet use, and prevent the need for these concerns to be addressed by individual politicians. It is entirely inappropriate however that complaints about content should be receivable only from Australian residents or

---

smaller ISP's can not get any benefit out of being member, and the membership fees used to reflect their target membership, didn't influence many to join. As a small ISP, I can not see any benefit to joining the IIA, as they do not cater for us small businesses. If there were to be Internet Industry Association that were there for us smaller end of town, I for one would be most interested in joining, but at this point of time I will never ever join the IIA as it stands.' All responses received by email 17/6/04 See also Kimberley Heitman, 'Vapours and Mirrors' (March 2000) 6 (1) *UNSWLJ Forum, Internet Content Control* 6(1) 30.

[7] As required by s 62(1) of the *Broadcasting Services Act* 1992 (Cth).

businesses, and that the complainant must be identified. Where concerns are raised regarding harmful, dangerous and illegal content it must surely be entirely irrelevant who is making the complaint or in what form. The concerns should be received and addressed regardless.

Furthermore, it is not clear that the ABA is the appropriate recipient of such complaints, for a number of reasons. The ABA has shown itself too ready to blur information to support government policy, and too reticent to view the scheme critically.[8] The ABA's use as recipient of complaints also unnecessarily adds an extra layer to the regulatory scheme. The OFLC for example, which is responsible for classification of content in all other media, would be a far more appropriate body to deal with this type of complaint. It has the ability actually to classify the content subject to complaint, and thus to make real (rather than interim) determinations about its classification. Alternatively, or as a next step, where complaints relate to illegal or dangerous material, police would be more appropriate recipients of complaints than the ABA. Police already have the 'Crime-Stoppers' hotline, to which complaints, anonymous or otherwise, can be and commonly are made. As with illegal content in any other medium, the police force is the appropriate body to investigate and prosecute illegal internet material, and certainly the most appropriate body where real danger is concerned, for example child pornography, and the stalking or grooming of children. While there may be advantages in all complaints or reports being addressed at least initially to one central recipient - for example to ensure uniform treatment of complaints, to maintain statistics and to allow trends to be identified - that recipient could well be a body other than the ABA.

The ABA's involvement in receiving and investigating complaints may in fact cause problems for the police and make meaningful investigation more difficult. ABA investigations may alert content providers of regulatory interest prior to the police becoming involved. Although the legislation provides for the ABA to stay

[8] See discussion above, Chapter 9.

investigation of complaints where the police are already investigating,[9] ABA investigations are likely to precede, rather than follow, police investigations. This could also be a concern if a body such as the OFLC were the original recipient of complaints. It is noteworthy that hotlines for reporting illegal or inappropriate internet content, in the UK, the USA, New Zealand, and many European countries, are run not by government regulatory bodies but by bodies set up for that or a related purpose. The receipt of complaints is not seen as a function of regulatory authorities. In each of those countries hotlines receiving reports of illegal content pass it on to policing or censorship bodies, not to the industry regulatory authorities.

A benefit however of using a government or quasi-government body as recipient of complaints is that this ensures funding for this activity. While funding overseas is often sourced through industry groups, private and community bodies, and individuals, the funding is often uncertain. This would need to be taken into account if another body were nominated to take over this role.

There has been some discussion as to whether the internet industry should itself be required to fund more of the various aspects of the regulatory scheme.[10] The suggestion is strongly contested by the IIA which claims that **'there is no reason to impose upon the industry any toughening of obligations, when most Australians online are served by ISPs doing all that is reasonable to support the current regime.'**[11] However, leaving the whole cost of complaints schemes and hotlines to government denies industry responsibility, and is not in line with a truly co-regulatory scheme. Requiring at least some contribution from the industry

---

[9] Broadcasting Services Amendment (Online Services) Bill 1999, Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 21 April 1999, 3960 (Senator Ian Campbell, Parliamentary Secretary to Senator Alston, Minister for Communications, Information Technology and the Arts).

[10] For example see Peter Chen, Centre for Public Policy, University of Melbourne, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (October 2002) 7: 'while the industry has a role in the development and implementation of the codes of practice, it has escaped any direct financial responsibility for community education.' 25; Young Media Australia, *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 7.

[11] Emphasis in original. Internet Industry Association (IIA), *Submission to Review of the operation of Schedule 5 to the Broadcasting Services Act 1992* (Nov 2002) 6.

would be in keeping with the aims of co-regulation.[12] While it is not the 'fault' of the internet industry that content may be harmful, it is the case that supply of content over the internet to subscribers creates possibilities for harm and addressing this requires funds. Individual content providers are of course most responsible for the content provided, but may also be the most difficult to identify and burden with costs. The ease with which users can also be content providers – an important attraction of the internet - would make it extremely difficult to hold individual content providers responsible for making financial contributions to hotlines or monitoring schemes. ISPs and ICHs on the other hand are in a good position from which to pass on costs to content providers.

It would be important to ensure also that the activities of any body taking on this role were subject to scrutiny and that the body could be called to account on this topic. While public bodies are generally more amenable to this kind of scrutiny, this has not been the case with the ABA's administration of the complaints and investigations process.[13] In fact, the recent addition of an exemption to the *Freedom of Information Act*, designed specifically to prevent such scrutiny, is one of the least satisfactory aspects of the Government's handling of the content control regime.

3. Restricting access to content refused classification (RC)

In every medium some content will be refused classification. While there has been occasional controversy over refusals to classify specific films, books and publications, the existence of such a category has not itself been a subject of major dispute. While this paper does not deal with the issue of censorship per se, it assumes that that content which is refused classification[14] is accepted in Australia to be a legitimate subject of censorship.

---

[12] Discussed above in Chapter 6.

[13] Discussed above in Chapter 9.

[14] Films or videos will be refused classification where they promote or provide instructions on paedophile activity, depict child sexual abuse or offensive depictions of child or apparent child, include detailed instructions in matters of crime, violence or illegal drugs, depict bestiality, or include detailed, exploitative or offensive depictions of violence, cruelty, sexual violence, sexual

If the federal government in fact wishes to censor RC material on the internet, which is subject to censorship in every other medium, then RC material which comes to the attention of the ABA, the police, ICHs or ISPs should be removed from Australian servers and possibly also blocked, as far as possible, by Australian ISPs. While a large proportion of potential RC communications occurring on the internet are likely to be well disguised, and its recipients well targeted, the nature of the material justifies serious, rather than symbolic, attempts at censorship. This most extreme material is likely to be less prevalent than, for example, X or R-rated material, and thus blocking any RC material would have a proportionally greater impact than blocking other content, as well as placing less burden on the industry. Well-hidden, well-targeted RC material is likely to remain accessible, but it may be argued that at least that which comes to the attention of the hotline, the police, or the industry, ought to be blocked to stop its availability in Australia. While the Review into the *Online Services Act* did not recommend any blocking, it did state that index filtering was now sufficiently developed to allow upstream blocking by IP or URL without significant degradation of networks.[15] It could be argued that content refused classification and known to authorities should not be accessible within Australia online, any more than in any other medium.

No doubt the internet industry would strenuously resist any requirement to block any content, citing cost to industry and to consumers, degradation of the network, and misplacement of responsibility when the industry does not provide the content, but only carries and hosts it. Libertarians may also argue that nothing should be blocked, that a little blocking is only 'the thin end of the wedge,' and that if once the Government saw that it could block, it would block more and more. Furthermore, it would be argued still to be pointless; blocking content at a particular IP or URL will not stop the same content being accessed from another

---

activity accompanied by offensive or abhorrent fetishes, abhorant or offensive incest or other fantasies. *National Classification Code (annexed).*

[15] DCITA, above n 3 23. The Review acknowledged that this was disputed by the industry which claims that any blocking would have a serious impact upon networks, particularly noticeable in broadband connections, currently favoured for their speed of access.

site. These arguments held sway in the drafting of the *Online Services Act*, and there is nothing to suggest that they will not continue to do so.

There is however another way of dealing with this content. Police should be far more involved in investigating complaints, and in pro-actively investigating the production, distribution, and / or use of this content. The development of uniform national legislation which was promised as part of the original scheme of content regulation but which has not yet occurred, could assist here. Such legislation is not entirely necessary, as each state does already have some legislation which allows prosecution of offences relating to content which is or would be refused classification.[16] But this legislation is varied and not always compatible, and thus uniform legislation seems beneficial.

It appears however that the Commonwealth is now trying to overcome the deficiencies in State and Territory legislation by introducing its own legislation in this area. The Crimes Amendment Bill currently before Parliament seeks to introduce internet-specific content offences including using a carriage service for child pornography, for child abuse, or for procuring or grooming a child for sexual activity.[17] The limits of Commonwealth power here are unclear however, which is why State and Territory legislation was intended initially to deal with these content offences.[18] State and Territory legislative power is more certain in this sphere, and it may be better again to seek agreement as to the offences created, and to attempt again to achieve a uniform scheme. The combination of Federal and State / Territory legislation should ideally provide for removal of RC content from Australian hosts and prosecution of those who knowingly make, provide, distribute, or carry RC content.

---

[16] Discussed above in chapter 10.
[17] Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004 Second Reading Speech, Cth, *Parliamentary Debates*, Senate, 24 June 2004, 24395 (Senator Ian Campbell).
[18] See discussion of limits of Commonwealth powers in Chapter 5: Censorship and freedom of speech, and Chapter 10: State and territory legislative provisions..

The Federal Government may be moving further toward a stricter approach to RC content. In addition to the Criminal Code amendments[19] discussed above, the establishment of a new 'national online child sexual abuse unit' has been mooted as a possible joint operation of the Customs Department and Federal and State police forces.[20] No such unit has yet been established. However, the 'Australian High Tech Crime Centre,' established in July 2003 to allow co-operative work by federal, state, and territory police, states on its homepage that 'high tech' crime includes 'traditional crimes which are largely facilitated by technology. Examples include fraud, illicit drug trafficking, child sexual exploitation, terrorism and money laundering.'[21] It may be that this Centre will take on some of the policing work related to RC material accessible online within Australia.[22]

While RC content may be difficult to detect on the internet, its detection is not impossible. In New Zealand for example a proactive campaign aimed at finding and prosecuting producers, distributors, and users of this content has been highly successful. By focusing on child pornography, because it involves abuse of children, the Censorship Compliance Unit of the Department of Internal Affairs has identified over 500 New Zealander internet users involved with illegal content on the internet. It has successfully prosecuted 103 of them, while 25 further prosecutions remain pending.[23] It is very important to note that NZ police also work closely with their counterparts overseas to ensure that investigations do not cease simply with the prosecution of New Zealanders, but continue in attempts to track down sources and users of the content overseas. Similarly in the UK, investigations into users of a particular paedophile portal in the US have led so far

---

[19] Senator Ian Campbell, above n 17.
[20] Simon Hayes, 'Online sex abuse police plan.' *Australian IT*, 21 July 2003 <http://australianit.news.com.au/common/print> (no longer available).
[21] Homepage of Australian High Tech Crime Centre <http://www.ahtcc.gov.au/> at 22 July 2004.
[22] It is unclear quite what this Centre will do. When the author requested information from the AHTCC the response was as follows: 'I would suggest that content of the internet is in the realm of governance by the Australian Broadcasting Authority. You may wish to consult their website...' Email to the author from AHTCC Operations Monitoring Centre (unnamed) 21/7/04.
[23] Keith Manch and David Wilson, *Objectionable Material on the Internet: Developments in Enforcement.* (2003) <http://www.netsafe.org.nz/downloads/conference/netsafepapers_manchwilson_objectionable.pdf > at 1 July 2004.

to 3537 arrests, 1679 prosecutions and 1230 convictions,[24] and 102 cases in which children were removed from the users / makers of child pornography.[25]

If it is accepted that RC material, and especially material such as child-pornography, really falls within the domain of police investigation, it would be sensible not to limit investigations and prosecutions to 'internet content' as defined in the *Online Services Act.* Peer to peer networks for example, while not web-based, are increasingly significant in allowing data transfer over the internet, and particularly the transfer of illegal or harmful content. Data transfer via peer to peer networks should be subject to investigation and policing similarly to web-based content.

Chat rooms appear also to be an area most in need of pro-active policing if children are to be protected and RC material found. A practical international approach in this sphere has recently been announced. Police in Britain, Australia, Canada and the USA are planning joint policing of internet chat rooms.[26] Although it is recognized as impossible to police all chat rooms all of the time, the joint approach involves police from the various countries visiting chat rooms and overtly announcing their presence. The aim is to deter the grooming known to occur in chat rooms, and to make internet chat users feel safer online. The joint project is not intended to 'catch' criminals but to deter them from using chat rooms to make contacts with children.[27]

Email also requires inclusion in any scheme of internet content control. The use of email either itself containing illegal material, or carrying links to illegal material, should be specifically included in legislation, and again should be subject to pro-active police investigation. It should not be left to anti-spam legislation, but should be included in any legislation which aims to protect children against

---

[24] John Leydon, '102 kids saved from paedos.' *The Register,* 14 April 2004 <http://www.theregister.co.uk/2004/04/14/operation_ore_update/print.html> at 3 August 2004.
[25] Ibid.
[26] Jill Lawless, 'Global hunt for pedophiles on net.' *Australian IT,* June 10 2004 <http://australianit.news.com.au/articles/0,7204,9800027%5e15318%5e%5enbv%5e15306,00.html> at 3 August 2004.
[27] Ibid.

exposure to dangerous, harmful and illegal internet content.[28] Deceptive labeling of sites so as to increase the likelihood of exposure to unsuitable content, and links from children's sites to illegal sites or even to content unsuitable for children should also be prohibited. Breach of such prohibitions would need however to be actively pursued and prosecuted if they were to make any difference at all. Again, jurisdiction would be limited to Australian sites, but co-operative policing would be worthwhile. In fact deceptive labeling in this area has now been specifically targeted by US legislation.[29]

It should also be noted that if the Criminal Code amendments referred to above are enacted, the offences created thereby will not be limited to 'internet content' as defined by the *Broadcasting Services Act*. Those offences relate rather to the use of a carriage service in a particular way, for a particular purpose, or with a particular effect, rather than relating to 'internet content' per se. This will allow prosecution for offences not covered by the limited definitions in the *Broadcasting Services Act*.

4. Restricting access to X-rated content.

Restriction of X-rated content is far more controversial, particularly as X-rated content is legal in Australia, and in fact supports a thriving industry. This is an example of content outlawed because of the medium; that is, illegal when carried on the internet, but not illegal generally. If X-rated content were permitted when

---

[28] The author received an unsolicited email offering 'horny child pornography,' which was then forwarded to the ABA, not as a formal complaint but 'for its perusal.' The ABA responded in part: 'Please note that the ABA's powers under schedule 5 to the Broadcasting Services Act 1992 (the Act) do not extend to investigating complaints regarding unsolicited email (SPAM). The government body, the Australian Communications Authority (ACA) is directly enforcing the Spam Act 2003, monitoring spamming activities, promoting public education and working internationally to combat Spam. The email address by which you may report Spam to the ACA is...' The ABA added that this particular content had previously been investigated and referred to police. Email to author from Libby Owens,
Assistant Analyst/Investigator, Content Assessment, ABA 16 July 2004.

[29] *Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act 2003.* 'The provision relating to domain names makes it illegal to use a "misleading domain name" with the intent to deceive a person into viewing obscenity or to deceive a minor into viewing "material that is harmful to minors" on the Internet. The law provides for fines and imprisonment for up to four years.' Doug Isenberg 'The wrong answer to child porn on the Net.' c/netNews.Com <http://news.com.com/2010-1071_3-1001105.html> at 1 July 2004.

hosted behind a Restricted Access Scheme (RAS), this would be more closely commensurate with the same content offline.

As well as being more controversial than attempts to restrict RC material, restriction of X-rated material is also more difficult, and less likely to have any impact, due to the quantity and availability of X-rated material. Those favouring a prohibition on X-rated content claim that even if it does not stop access to content, banning it from Australian servers at least sends a message.[30] But what message does it send? To the industry it sends a message that distributors of such material should operate from servers outside Australia. Tthat message appears to have been well accepted.[31] To those within Australia wishing to access this material the message is what? That X-rated content from overseas is to be preferred? That this content will not be tolerated on Australian servers, although via the post the content is fine? This part of the legislation was poorly thought out. It bans from Australian servers content which it is legal to own in Australia. It moves the online X-rated industry offshore, while doing nothing to restrict the access of Australian users to X-rated content. It is wasteful to continue investigating X-rated content for removal from Australian servers. The cost could be better spent investigating and prosecuting those responsible for RC content. In addition, and of more concern, the total prohibition from Australian servers of X-rated as well as RC material blurs the distinction between the two.

The *Online Services Act's* objective of 'restricting access to Internet content likely to cause offence to a reasonable adult,' should be re-evaluated, re-drafted, and made more specific. Provisions relating to RC content should be very clearly delineated from those, if any, relating to X-rated content. X-rated content, being content that is legal within Australia, should be subject not to prohibition but at most to restriction, as for other Australian content which is legal yet restricted.

---

[30] Elizabeth Handsley & Barbara Biggins, 'The Sheriff Rides into Town: A Day of Rejoicing for Innocent Westerners.' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 35.
[31] Peter Chen, 'Pornography, Protection, Prevarication: The Politics of Internet Censorship,' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 18.

5. R-Rated content

Where might R-rated material sit in all of this? R-rated material may be difficult to classify, and is often material which is not 'offensive,' simply 'unsuitable for a minor to see.' As such, the internet is full of material which may be classified R, or at the milder end MA, or at the stronger end X. 'R' is a huge and somewhat uncertain category. Under the *Online Services Act* it is illegal to host R-rated material in Australia unless it is subject to a Restricted Access Scheme, but if hosted overseas this content will not be subject even to reporting to filter makers. It is Australian-hosted R-rated material only with which the *Act* is concerned.

Due to the prevalence of this content on the internet, the difficulty of classifying it, its 'low impact,'[32] and the fact that no attempt is made to restrict its availability from overseas, the *Online Services Act* should not attempt to restrict this material in Australia. This is not the 'too hard' option, but rather a realistic option. R-rated content may be unsuitable for children, and it may also offend or disturb adults, but learning to protect oneself from this content and to deal with exposure is imperative, unless we are going to operate a 'closed' internet. As any internet user is almost certain to come into contact with R-rated material at some stage, it would be far preferable to concentrate on assisting people to deal with this content, than to pretend that it can be restricted. The policy of restricting R-rated content only when it is Australian-hosted is particularly ill conceived.

6. Research and Development

Australia should also take a more pro-active role in the development of tools and methods for internet content control by end users. While the ABA has claimed, for example, to be highly involved with developments such as ICRA,[33] there is little real evidence of this. Further, while the ABA and NetAlert have had funds for commissioning and conducting research, all of the research has been current or retrospective, asking questions such as the following. Do filters work? How do

---

[32] See Senator Ian Campbell, above n 9 3960, for reference to why R-rated overseas content is not subject to interim take-down notices.

[33] Australian Broadcasting Authority, *Submission to Review of the Operation of Schedule 5 Broadcasting Services Act 1992* (November 2002) 37.

they work? How many people are connected to the internet? How do families use the internet? We have not seen these funds used for research into or development of more effective filtering systems, more Australian oriented filtering systems, easier to use filtering systems, labeling systems suited to an Australian classification scheme, the application of labels in the Australian environment, or most importantly, research into and development of really effective user education. Rather than constantly claiming success, some action in this area, and evaluation of it, would be a real improvement.

The idea of internet content labeling could be pursued further in Australia. The ABA's 1996 report[34] encouraged the development of labeling as a useful tool for content management, and the ABA claims still to be involved in the development of ICRA labeling.[35] The ICH Code of Practice states that 'Internet Content Hosts will encourage Content Providers to use appropriate labelling systems...'[36] Even the review of the *Online Services Act* found that the ABA and the Internet industry should promote the take-up of labeling.[37] As discussed above,[38] labeling can be done by a content provider or by a third party (such as OFLC or similar) which rates content according to defined categories, and attaches labels to content. Filters then read the labels, and can be set up either to block content with certain labels, or only to allow content with certain labels, or in fact with any labels. Labeling can be done by classification: for example, content could be labeled X, R, M, PG, G, thus reflecting an accepted and well understood local system. Alternatively or additionally content could be labeled by topic, for example, sex, news, health, cult, education, teenage, entertainment, adult, sport etc. Categories could also be combined and ranked, for example sex / health; violence3 / news3; or even entertainment / news / M.

[34] Australian Broadcasting Authority, *Investigation into the Content of Online Services* (1996)
[35] Australian Broadcasting Authority, above n 33. There is no evidence available as to the prevalence of labeling of Australian sites.
[36] Internet Industry Association ICH Content Code 7.2(a).
[37] DCITA, *Review of the operation of Schedule 5 to the Broadcasting Services Act 1992; Report* (May 2004) 48.
[38] Chapter 3.

While such labeling systems were widely promoted during the 1990s, their use became rather controversial, as it was recognized that the labeling of sites to allow easy user selection allows also easy government selection, and thus enables censorship.[39] However, as with other internet content restrictions, the USA will not mandate content labeling, and thus there will always be a significant quantity of unlabelled content on the internet. As the Australian Government has shown an unwillingness to block content from overseas, the danger to Australia of censorship arising from the labeling of material is minimal. Those wishing to stop access to certain content could do so by filtering to allow only labeled content, but otherwise access would still be available to the huge wealth of material on the internet worldwide.

The ABA[40] and the IIA[41] claim to promote and encourage labeling, but it has been given far less prominence than other filtering technology as a means of allowing users better control over content selection. Perhaps some of the money currently spent administering the *Online Services Act* could be spent on labeling of Australian sites according to an Australian classification scheme. Australian parents, for example, could use filters to restrict viewing to labeled sites for younger children, or while they were unable to supervise, while still allowing access to the broader internet for older children and when they are able to supervise. While the use only of labeled content would greatly restrict the breadth of what could be viewed, it would also give parents peace of mind during those times they could not supervise. There would be no need for all or even most internet content to be labeled before such labeling would be useful.

---

[39] See for example L Lessig, *Tyranny in the Infrastructure* (July 1997) Wired News. <http://www.wired.com/wired/5.07/cyber_rights.html> at 3 August 2004; Graham, Irene; *'The Net Labelling Delusion: Saviour or Devil?'* (undated), <http://libertus.net/liberty/label.html> at 20 June 2004; and see Bohorquez, FA, 'The Price of PICS: The Privatization of Internet Censorship.' (1999) 43 N.Y.L. Sch. L. Rev. 523.

[40] 'The ABA particularly encourages Australian Internet content developers to contribute to the take-up of this scheme by appropriately labeling their content.' Australian Broadcasting Authority, above n 33 37.

[41] Internet Industry Association ICH Content Code 7: 'Internet Content Hosts will encourage Content Providers to use appropriate labelling systems...'

Approximately 100,000 sites world-wide are thought to be labeled already,[42] and this could be added to by the labeling of Australian sites.

7. Protecting children from exposure to unsuitable internet content

As long as the internet is easily accessible and its use is encouraged, protecting children from exposure to unsuitable internet content will only be achieved through education and supervision. We have seen over the past few years that if we are to have a fairly open internet, we will be unable to control access to unsuitable content. While the *Online Services Act* originally envisaged restriction of content to protect children from exposure, no such restrictions have occurred. As an alternative, filtering technology was seen as the appropriate way to protect children, and as such its use was heavily pushed by the IIA, the ABA and NetAlert. Filter technology may have developed a little over the life of the *Act.* But even when properly installed and configured, filters do not effectively protect children from exposure to unsuitable content, and, possibly as a result, few people in Australia use content filters.[43]

Although without constant supervision children cannot be protected from exposure to content unsuitable for them, they may nonetheless be protected from the danger or damage likely to arise as a result of that exposure. In this regard education is extremely important. Providing web sites containing safety information is useful, but nowhere near sufficient. While children may be familiar with searching web sites for information, their parents are less likely to be familiar with the internet, and less likely to see it as a source of protective information. It is imperative then that information is provided to parents and the community through broader means than online sites.

---

[42] About 100,000 sites have applied to ICRA for labels since 2001, but it is not clear how many actually use them. Email to author from Lynn Edwards, ICRA, 11November 2003.

[43] Possible figures for filter uptake are discussed above chapter 12, but no reliable figures exist. Low uptake may be due to difficulty in installation and configuration, lack of awareness of the existence of filters, or apathy. On the other hand, it may be that users understand that filters have many problems, which studies have shown to include bias and ineffectiveness.

Education regarding internet protection needs to be age-appropriate. Not only should education be appropriate for the age at which it is aimed, it is necessary also that adults are given information to help them appropriately protect various ages of children or young adults under their care. It would be ridiculous to think that constant supervision of a teenager using the internet is realistic, but it may be that exposure to some content would be more worrying, damaging or dangerous to a teenager than to a younger child. It is imperative therefore that education is undertaken to educate the broad range of people using or supervising internet use.

Internet safety education needs also to be constant or continuing, and what is taught should develop with age. For example, what a child is told on signing a school or library 'internet use agreement' in year 3 of school will not be appropriate for the same child in year 6, year 9 or year 12. Furthermore, such agreements often relate to the responsibilities of the child, who promises not to use the internet for X, Y and Z, but often fail also to give information regarding why that might be the case. For example, instructions never to give out personal information, addresses, phone numbers, parents' names etc might be just that to children - instructions, but not explanations. The more children, young people, and in fact adults understand the reasons for such instructions, the safer they will be in their internet use. Often though, schools and libraries do not feel a need to go further with instructions because they are providing a relatively safe environment for internet use; reasonably high levels of supervision or monitoring, coupled with high level content filtering. This is an environment where children are least likely to confront worrying internet content, but outside the school or library they are far less likely to have these levels of monitoring, supervision, and filtering. It is necessary then that when there is an opportunity to educate regarding internet safety, it is not assumed that internet use will always occur in this relatively cocooned environment.

Internet education should perhaps be more realistic and less euphemistic. Constantly telling children and young people to close any site which makes them uncomfortable may not be enough to prepare them for the content they may in fact see. It may be necessary in order to educate properly to explain dangers more

fully. Naturally, no-one wants to scare children or young people or give them exaggerated concerns over things which may never happen. On the other hand, studies suggest that children and young people who use the internet are likely at one time or another to come across internet content that worries or frightens them.[44] It is important also that adults are taught appropriate responses to children's concerns. A study in the US found for example that many children did not report worrying content they came across on the internet for fear that they would get into trouble, or have their internet use restricted.[45]

It is important also that education occurs not just in an industry setting, but in an educational setting. Although the internet industry Code of Practice requires ISPs to provide or link to internet safety information, and to make available internet filters or filtered services, the industry could not really be said to provide education. The industry is probably not the best group anyhow to be carrying out educational functions. It would be far better to use educators, with expertise in education, and with an understanding of age appropriate teaching methods and curricula. This is the same whether discussing education of children or adults, as simply providing information is often not sufficient to equip people with the skills they need.

Protecting children from exposure to unsuitable internet content is a difficult task yet one worth attempting. However, without operating a tightly restricted internet, protection from exposure can be minimised but not avoided. It is important therefore that action is taken to help adults to understand the best way to protect children, to help children understand the best ways to protect themselves, and to provide assistance for those who are exposed to unsuitable internet content. While detail of the latter is beyond the scope of this paper, interesting suggestions have been made for example by the Australia Institute, which advocates pornography

---

[44] See for example Aisbett K, The Internet at Home, A report on internet use in the home (2001) (Internet@Home) <http://www.aba.gov.au/internet/research/home> at 24 June 2004.
and see Clive Hamilton & Michael Flood, Australia Institute, *Youth and Pornography in Australia; Evidence on the extent of exposure and likely effects* (Feb 2003).
[45] Wired News *Scouts survey net harassment.* (14 February 2002)
<http://www.wired.com/news/culture/0,1284,50413,00.html> at 1 August 2004.

education for high school students.[46] The aim of such education would be to help children and young people understand and to deal with pornographic material they may be exposed to on the internet. While the Australia Institute's suggestion is narrowly framed to deal with pornography, young people equally require education about, for example, violence, racism and financial scams likely to be encountered on the internet. Anyone looking into the possibilities of pornography education would do well to broaden the scope of such an enquiry.

8. Classification.

There has never been an explanation as to why internet content must be classified as film. This requirement should be changed so that internet content is classified in the same way as its most analogous offline counterpart. While there have been discussions of whether a new classification scheme for 'online content' is needed, simply using the closest offline analogy for the specific content in question is logical, easy, and fits with government promises of commensurate restrictions.

B. *Conclusion.*

All of the above would go some way toward improving the Australian scheme for internet content control. Happily, most of these suggestions could also be achieved through tinkering; continuing the present scheme but making changes here and there. This is the type of change most likely to appeal to a Government which has repeatedly asserted that its scheme is successful, even in the face of clear failure to achieve its aims. An alternative government is also unlikely to dismantle the current scheme. While the ALP commonly criticizes the scheme,[47]

---

[46] Clive Hamilton & Michael Flood, Australia Institute, *Regulating Youth Access to Pornography* (March 2003) 11-15.

[47] See for example Senator Kate Lundy. 'Internet Regulation in Australia – an Opposition Perspective.' (Speech made at NetAlert Conference, Canberra, 4 December 2002); and Senator Kate Lundy 'The *Broadcasting Services Amendment (Online Services) Act* is largely symbolic and, I think, a lazy attempt to mislead Australians into believing that the coalition actually cared about and had met the objective of helping protect Australian citizens, especially children, from illegal and highly offensive material.' 'Internet Content – parent education is the key.' (*Cth* Senate Adjournment Speech 19 March 2004).

emphasizing rather the benefits of community education and user empowerment,[48] the Shadow Minister for Communications has not suggested unwinding the scheme or repealing the *Online Services Act*.[49] Thus suggestions aimed at improving the current scheme, rather than overhauling or repealing it, are more likely to influence any future government action in this sphere.

[48] Senator Kate Lundy, 'Internet Content – parent education is the key.' (*Cth* Senate Adjournment Speech 19 March 2004) and Senator Kate Lundy, *Internet User Education the key to protection from unwanted porn*. Media release (3 March 2004).

[49] At the time of writing the ALP has not yet released its relevant policy for the forthcoming election.

CHAPTER SIXTEEN: CONCLUSION

The internet had been accessible for a number of years before the federal Government introduced legislation aimed at controlling its content. However, while the internet had existed earlier, its take-up had been confined primarily to research, educational, and business use. By the late 1990's the use of the internet was increasing exponentially, not only in the amount of traffic the net was generating, but in the number of people who used it, the breadth of background of those users, and the ease of accessibility from homes, libraries, schools, internet cafes etc. The internet had, very suddenly, become hugely mainstream. It was in these circumstances that the Government acted to regulate internet content.

During the drafting and enactment of the *Online Services Act* there were predictions of severe limits on freedom of speech, of requirements for expensive industry action and intervention, of resulting slow and inefficient internet services, and a stifling of industry growth and development. On the other hand there were promises that child internet users would be protected from inappropriate material, that access to illegal content would be restricted, that community education would be provided for internet users, and that a uniform national scheme to deal with producers, distributors and users of illegal and/or harmful internet content would ensue.

It is now clear that the Australian regime for internet content control has not brought about the feared, or promised, changes. It does not restrict access to internet content likely to cause offence to adults, and does not protect children from exposure to unsuitable content.[1] It provides a means for addressing complaints about internet content but does not deal with the content complained of in any substantive way.[2] Furthermore, the Australian regime has failed to provide an effective community education scheme which could assist internet

[1] See above Chapter Twelve: Statistics and perceptions and Chapter Thirteen: The stated aims – have they been achieved?
[2] See above Chapter Nine: Complaints regime and Chapter Thirteen: The stated aims – have they been achieved?

users control content for themselves,[3] and has failed to create a unified national scheme which would ensure that internet content providers, hosts, and users were treated in the same manner everywhere in Australia.[4] As such, the scheme could be said to have failed.

On the other hand, the regime introduced for online services has also not had the negative consequences envisaged prior to its enactment. There is no evidence that it has stifled freedom of speech; those concerned about speech prohibitions are likely simply to host their content outside Australia.[5] Further, there is no evidence that industry development has been stifled by the internet content control regime. The proportion of Australians using the internet continues to grow,[6] the number of access lines continues to increase,[7] and the amount of data downloaded is still expanding.[8] The regime appears in fact to have had little real effect, positive or negative.

Despite this, and despite allegations of cynicism, and of the use of merely symbolic politics,[9] there is nothing to suggest that proponents of the *Online Services Act* really did not intend it to achieve its goals. Its goals fitted well, generally, with long term policy of both Labor and Liberal Governments regarding censorship and classification, and if effective, would have brought internet content more into line with the control of content in other media.[10] However, its goals have proven to be unachievable by the methods chosen.

---

[3] See above Chapter Eleven: Community education and Chapter Twelve: Statistics and perceptions.
[4] See above chapter 10: State and Territory legislative provisions.
[5] See above Chapter Nine: Complaints regime and Chapter Twelve: Statistics and perceptions.
[6] Nua Internet – how many online? 5.5 million, or 30.5% of Australians were online at May 1999, 10.63 million, or 54.38% were online at February 2002. Nua data drawn from Neilson NetRatings and Australian Bureau of statistics. http://www.nua.com/surveys/how_many_online/asia.html at 8 August 2004.
[7] Australian Bureau of Statistics, *Internet Activity Summary, Australia,* 8153.0 Data to March 2004.
[8] Ibid.
[9] See above Chapter One: Introduction and Chapter Seven: Passage and provisions of the *Online Services Act.*
[10] See above Chapter Five: Censorship and freedom of speech.

Thus in terms of internet content regulation Australia could not be seen as a world leader. As this thesis has discussed, no other country has followed Australia's lead, and even within Australia the *Online Services Act* has been quite ineffective. The Australian scheme could certainly not be held up as a model to which others should aspire.

But is Australia the village idiot of the internet world? In introducing the *Online Services Act* the Government certainly acted hastily, introduced legislation with unachievable aims, and put itself in a position of great conflict with the internet industry, civil libertarians, and many internet users. On the other hand, it did try to introduce a regime which would allay concerns about the availability of illegal and inappropriate content. Unfortunately, what the Government promised it could not deliver. While the Government tried to push the internet industry to deliver, the industry could not have done that without undue financial and administrative burdens, and possibly also considerable infringement on freedom of speech on the internet.

Australia may not be quite such an idiot however. By enacting the *Online Services Act* the Government bought time for the internet in Australia to grow and develop with little restriction, and to become more widely used and thus well entrenched within the Australian community. It created time and space to work out what really is and is not achievable, and what is and is not desirable, in attempting to control and allay concerns regarding internet content in Australia. If that time and space were to be used genuinely to evaluate not only the current scheme, but to investigate more broadly Australians' real needs in terms of internet content control, the *Online Services Act* could be said to have achieved something worthwhile.

Unfortunately however, there is no indication that this will occur. The current regime for internet content control appears entrenched, and discussion of the scheme and its alternatives is now uncommon. Only four six-monthly reports on the scheme have been issued in four and a half years, whereas nine would have been expected. A Review required within three years of the *Act's* operation was

not produced until nearly four and a half years had elapsed. The Review supported the scheme generally, suggesting minor changes only. The major industry players support the current scheme, and neither the Government nor the Opposition have signaled any intention to change it. The Review Report has not been mentioned in Parliament, despite having been tabled three months ago. It appears that internet content control has simply fallen below the radar of both the Government and the Opposition for now.

Consequently, it is unlikely that any significant change to the scheme will occur in the near future. With the current scheme in place Australia will never become world leader in this area, but if it fails to do what it can to improve the scheme, as it looks likely to do, it may well soon deserve village idiot status.

POST SCRIPT

The Australia Institute has recently 'declared' that there is no technical barrier to filtering pornography from the internet in Australia.[1] It bases its claims upon the Report of the Review of the *Online Services Act*, tabled in the Federal Parliament in May 2004.[2] Apparently the Australian Labor Party (ALP) has shown 'strong interest' in attempting to block pornography on the internet now that it is technically feasible.[3]

In fact the Review Report does state that upstream index filtering is possible, and would not cause significant time delays or network degradation.[4] However, it does not recommend upstream filtering,[5] noting that the task of compiling an index of sites for upstream filtering remains problematic,[6] and that the costs of the use of such filtering could not be justified.

It is worth noting that Senator Lundy, the ALP's Shadow Minister for Communications, Information Technology and the Arts, who is familiar with the content control regime, does not favour a requirement of upstream filtering. It is likely that other ALP politicians currently expressing an 'interest' in blocking internet pornography might also be less interested once they know what it entails, and that it is not as simple as the Australia Institute has suggested. It will be interesting to see what the ALP includes in its 2004 election policy statements.

---

[1] Australia Institute '*No technological barriers to ISPs filtering porn.*' Press Release (23 August 2004).
[2] DCITA *Review of the operation of Schedule 5 to the Broadcasting Services Act 1992; Report* (May 2004)
[3] Emma-Kate Symons, 'Labor bid to block net porn,' *The Australian,* IT Section, (16 August 2004).
[4] Ibid 17.
[5] DCITA, above n 2, 23.
[6] Ibid. Note also discussion of this above, Chapter 3: Methods of internet content control.

SELECTED BIBLIOGRAPHY

BOOKS AND ARTICLES

Abbate J, *Inventing the Internet* (London: MIT Press, 1999)

Alston Senator R, 'The Government's Regulatory Framework for Internet Content', (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 4.

Arasaratnam N, 'Brave New (Online) World.' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 10.

Arcioni E, 'Politics, Police and Proportionality, An Opportunity to Explore the Lange Test: Coleman v Power' (2003) 25 (3) *Sydney Law Review* 379.

Ayres I & Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (New York: Oxford University Press, 1995)

Baldwin R & Cave M, *Understanding Regulation: Theory, Strategy and Practice* (New York: Oxford University Press, 1999).

Berners-Lee T, *Weaving the Web* (New York: HarperCollins, 1999).

Bohorquez, FA, 'The Price of PICS: The Privatization of Internet Censorship.' (1999) 43 *New York Law School Law Review* 523.

Casimir J, *A Boy and His Mouse: More Postcards from the Net* (Sydney: Allen & Unwin, 1997)

Chen P, 'Pornography, Protection, Prevarication: The Politics of Internet Censorship,' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 18.

Chesterman M, *Freedom of Speech in Australian Law, a Delicate Plant* (Aldershot: Ashgate, 2000) .

Chin G, 'Technological Change and the Australian Constitution' (2000) 24 (3) *Melbourne University Law Review* 609.

Coleman P, *Obscenity, Blasphemy and Sedition; 100 Years of Censorship in Australia* (Sydney: Angus and Robertson 2nd ed 1974).

Coroneos P, 'Internet Content Control in Australia: Attempting the Impossible?' (March 2000) 6 (1) *UNSWLJ Forum, Internet Content Control* 28.

Coroneos P, 'The Operation of Australia's Internet Content Legislation.' (2001) 101 *Media International Australia* 73.

Dutton G & Harris M (eds), *Australia's Censorship Crisis* (Melbourne: Sun Books, 1970).

Fitzgerald B & Fitzgerald A, *Cyberlaw: Cases and Materials on the Internet, Digital Intellectual Property and Electronic Commerce* (Sydney: Lexis-Nexis Butterworths 2002).

Gomez J, *Internet Politics; Surveillance and Intimidation in Singapore* (Bangkok: Think Centre, 2002).

Graham I, 'Shrouds of Secrecy; The Operation of the Online services Act.' (2001) 101 *Media International Australia* 81.

Griffith G, *Censorship: Law and Administration* (Sydney: New South Wales Parliamentary Library, 1993).

Hafner K and Lyon M, *Where Wizards Stay up Late: The Origins of the Internet* (New York: Simon & Schuster, 1996).

Handsley E & Biggins B, 'The Sheriff Rides into Town: A Day of Rejoicing for Innocent Westerners.' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 35.

Hauben M & Hauben R, *Netizens, On the History and Impact of Usenet and the Internet* (Los Alamitos: IEEE Computer Society Press, 1997).

Heitman K, 'Vapours and Mirrors' (March 2000) 6(1) *UNSWLJ Forum*, (*Internet Content Control*) 30.

Johnson A, 'Key Legal and Technical Problems with the Broadcasting Services Amendment (Online Services Bill)' (1999) (unpublished).

Jones M, 'Free Speech and the 'Village Idiot.'' (March 2000) 6(1) *UNSWLJ Forum*, (*Internet Content Control)* 43.

Krol E, *The Whole Internet: User's Guide & Catalog* (USA, O'Reilly & Associates, academic ed 1996).

Kroll A, 'Any Which Way But Loose: Nations Regulate the Internet.' (Summer 1996) 4 *Tulane Journal of Comparative and International Law* 275.

Lee T, 'The Politics of Internet Policy and (Auto) Regulation in Singapore.' (2001) 101 *Media International Australia* 33.

Lee T, 'Internet Use in Singapore: Politics and Policy Implications.' (2003) 107 *Media International Australia* 75.

Lessig L, 'Reading the Constitution in Cyberspace.' (1996) 45(3) *Emory Law Journal* 869.

Lessig L, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

Lessig L & Resnick P, 'Zoning Speech on the Internet: A Legal and Technical Model' (1999) 98(2) *Michigan Law Review* 395.

Marr D, *The High Price of Heaven* (Sydney: Allen & Unwin, 1999).

Ogus A I, *Regulation: Legal Form and Economic Theory* (Oxford : Clarendon Press ; New York : Oxford University Press, 1994).

Post D & Johnson D, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367.

Reed K, 'From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce.' (Fall 2000) 13 *Transnational Lawyer* 451.

Randall N, *The Soul of the Internet ; Net Gods, Netizens, and the Wiring of the World* (Boston: International Thomson Computer Press, 1997).

Scott B, *The Dawn of a New Dark Age – Censorship and Amendments to the Broadcasting Services Act* (April 1999) (unpublished).

Scott B, 'Silver Bullets and Golden Egged Cheese: A Cold Look at Internet Censorship' (March 2000) 6(1) *UNSWLJ Forum, (Internet Content Control)* 14.

Smolla R, *Free Speech in an Open Society* (New York: Vintage Books, 1992).

Walker S, *Media Law: Commentary and Materials* (Sydney: LBC Information Services, 2000).

Wilcox M, *An Australian Charter of Rights?* (Sydney: Law Book Co, 1993).

THESES

Chen P, *Australia's Online Censorship Regime: The Advocacy Coalition Framework and Governance Compared* (PhD Thesis, ANU, 2000).

Glefjell S, *Governing the Internet: Australian Regulation of Internet Content* (MA Thesis, UNSW, 2001).

REPORTS AND CONSULTATION PAPERS

Aisbett K, *The Internet at Home, A report on internet use in the home* (Sydney: ABA, 2001).

Australian Broadcasting Authority, *Investigation into the Content of Online Services, Issues Paper* (Sydney: ABA, 1995).

Australian Broadcasting Authority, *Investigation into the Content of Online Services, Report to the Minister for Communications & the Arts* (Sydney: ABA, 1996).

Australian Broadcasting Authority, *The Internet and Some International Regulatory Issues Relating to Content: A Pilot Comparative Study Prepared for UNESCO* (Sydney: ABA, 1997).

Australian Broadcasting Authority, *Annual Report 2001-2002* (Sydney: ABA, 2002)

Australian Broadcasting Authority, *Annual Report 2002-2003* (Sydney: ABA, 2003).

Australian Law Reform Commission, *Censorship Procedure*, Report No 55, (Canberra: ALRC, 1991).

Computer Bulletin Board Systems Task Force, *Regulation of Computer Bulletin Board Systems* (Canberra: AGPS, 1995).

Department of Communications, Information Technology and the Arts, *A review of the operation of Schedule 5 to the Broadcasting Services Act 1992, Issues Paper* ((DCITA, September 2002).

Department of Communications, Information Technology and the Arts, *Report of the Review of the Operation of Schedule 5 to the Broadcasting Services Act 1992* (Canberra: DCITA, May 2004).

Electronic Frontiers Australia, *Internet Censorship – law and policy around the world.* Report compiled for Standing Committee on Social Issues, NSW Parliament (March 2002).

Greenfield P, McRea P, Ran S, *Access Prevention Techniques for Internet Content Filtering* (CSIRO, December 1999).

Greenfield P, Rickwood P, & Huu T, *Effectiveness of Internet Software Filtering Products* (CSIRO, Sept 2001).

Hamilton C & Flood M, *Regulating Youth Access to Pornography* (Discussion Paper 53, Australia Institute, March 2003). (Includes summary of Hamilton C &

Flood M, *Parents' Attitudes to Regulation of Internet Pornography* (Australia Institute: March 2003))

Hamilton C & Flood M, *Youth and Pornography in Australia; Evidence on the extent of exposure and likely effects* (Discussion Paper 52, Australia Institute, February 2003).

Lindsay D, University of Melbourne, Centre for Media, Communications and Information Technology Law, *Censoring the Internet: The Australian Approach to Regulating Internet Content.* Research Paper No 9 (Nov 1999)

McCrea, Smart & Andrews, *Blocking Content on the Internet: A Technical Perspective* (CSIRO, June 1998).

NetAlert Limited, *Annual Reports 2001 / 2002* (September 2002), *2002 / 2003* (September 2003) (Available at Net Alert website).

Ovum, *Internet Content Filtering: A Report to DCITA* (Available at DCITA website: April 2003).

Senate Select Committee on Community Standards Relevant to the Supply of Services Utilizing Electronic Technologies, Cth, *Report on Regulation of Computer On-Line Services* Part 1 (Sept 1995), Part 2 (Nov 1995), Part 3 (June 1997).

Senate Select Committee on Information Technologies, Cth, *In the Public Interest: Monitoring Australia's Media* (April 2000).

Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000 Tabled in Senate by the Minister for Communications, Technology and the Arts (September 2000).

Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2000 Tabled in the Senate by the Minister for Communications, Technology and the Arts (April 2001).

Six Month Report(s) on Co-Regulatory Scheme for Internet Content Regulation, January to June 2001 Tabled in Senate by the Minister for Communications, Technology and the Arts (February 2002)

Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, July to December 2001 Tabled in Senate by the Minister for Communications, Technology and the Arts (August 2002).

Standing Committee on Social Issues, NSW *Safety Net? Inquiry into the Classification (Publications, Films and Computer Games) Enforcement Amendment Bill 2001. Final Report: On-line Matters* (Sydney: NSW Parliament, June 2002).

INTERNET MATERIAL AND HOME PAGES

Australian Broadcasting Authority (ABA)
<http://www.aba.gov.au> at 24 August 2004.

AARnet, *A history of AARnet*
<http://www.aarnet.edu.au/about/history.html> at 27 August 2004.

Censorware Project, *Cyber Patrol and Deja News, Censorware product blocks an important research resource* (1998)
<http://censorware.net/reports/dejanews/> at 4 August 2004.

Censorware Project, *Passing Porn, Banning the Bible*
<http://censorware.net/reports/bess/> at 27 July 2004.

Clarke R, *Origins and Nature of the Internet in Australia* (2004) Principal, Xamax Consultancy Pty Ltd Canberra
<http://www.anu.edu.au/people/Roger.Clarke/II/OzI04.html> at 16 June 2004.

Department of Communications, Information Technology and the Arts (DCITA)
<http://www.dcita.gov.au> at 27 August 2004

Electronic Frontiers Australia
<http://www.efa.org.au> at 27 August 2004.

Electronic Frontiers Australia *Hoodwinking the Public: Australia's Internet Censorship Regime* (November 2002)
<http://www.efa.org.au/Publish/bsa_analysis2002.html> at 25 June 2004.

Electronic Privacy Information Center (Epic)
<http://www.epic.org/reports/filter_report.html > at 16 June 2004.

GetNetWise
<http://www.getnetwise.org> at 20 June 2004.

Graham I, *Comments on IIA Approved Filters and CSIRO Filter Evaluation Report* (Jan 2000)
<http://libertus.net/liberty/rdocs/apprfilters0001.html> at 27 July 2004.

Graham I, *The Net Labelling Delusion: Saviour or Devil?* (undated)
<http://libertus.net/liberty/label.html> at 20 June 2004.

Hasselton B, *Sites Blocked by Cyber Sentinel*
<http://peacefire.org/censorware/Cyber_Sentinel/cyber-sentinel-blocked.html> at 20 June 2004.

Haselton B, *SurfWatch error rate for first 1,000 .com domains* (2000)
<http://peacefire.org/censorware/SurfWatch/first-1000-com-domains.html> at 20 June 2004.

Internet Content Rating Association (ICRA)
<http://www.icra.org> at 24 August 2004.

Internet Hotlines Providers of Europe (INHOPE)
<http://www.inhope.org/> at 21 June 2004.

Internet Industry Association (IIA)
<http://www.iia.net.au> at 24 August 2004.

Internet Industry Codes of Practice
<http://www.iia.net.au/index2.html> at 23 June 2004.

InternetNZ
<http://www.internetnz.net.nz> at 30 June 2004>

Internet Watch Foundation (IWF)
<http://www.iwf.org.uk> at 30 June 2004.

Jansson E, & Skala M, *The Breaking of Cyber Patrol*
<http://www.snark.freeserve.co.uk/censorware/cp4break.html> at 4 August 2004.

Kristula D, *The History of the Internet* (1997)
<http://www.davesite.com/webstation/net-history.shtml> at 17 June 2004.

Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts & Wolff, *A Brief History of the Internet* <http://www.isoc.org/internet/history/brief.shtml> at 26 July 2004

Lessig L, *Tyranny in the Infrastructure* (July 1997) Wired News.
<http://www.wired.com/wired/5.07/cyber_rights.html> at 3 August 2004

Manch K and Wilson D, *Objectionable Material on the Internet: Developments in Enforcement* (2003)
<http://www.netsafe.org.nz/downloads/conference/netsafepapers_manchwilson_objectionable.pdf > at 1 July 2004.

National Centre for Missing and Exploited Children - The Cyber Tipline
<http://www.missingkids.com/cybertip/> at 21 June 2004.

NetAlert
<http://www.netalert.net.au> at 24 August 2004.

Netsafe, NZ Internet Safety Group
<http://www.netsafe.org.nz> at 1 August 2004.

Nua Surveys, *How Many Online?*
(2002)<http://www.nua.com/surveys/how_many_online/index.html>

Peacefire
<http://www.peacefire.org> at 16 June 2004.

Platform for Internet Content Selection (PICS)
<http://www.w3.org/PICS/> at 20 June 2004

Singapore Media Development Authority
<http://www.mda.gov.sg> at 30 June 2004.

UK Internet Service Providers Association
<http://www.ispa.org.uk> at 30 June 2004.

Robert Hobbes Zakon, *'Hobbes' Internet Timeline* (1993-2004), Zakon Group LLC <http://www.zakon.org/robert/internet/timeline> at 16 June 2004.

Internet Content Regulation in Australia; Perceptions Thus Far.

Carolyn Penfold*

Introduction

During the passage of the *Broadcasting Services Amendment (Online Services) Act 1999* (*Online Services Act)* and prior to its substantive provisions coming into force in January 2000, there was a great deal of criticism of the legislation, anticipation of onerous responsibilities being placed on the internet industry, and anticipation of huge changes to the internet in Australia. Industry Codes of Practice (Codes) were registered with the Australian Broadcasting Authority (ABA) prior to the legislation taking effect, and these Codes are to be read in conjunction with the *Online Services Act.* Due partly to amendments during the bill's passage, and partly to the provisions of the Codes of Practice, the concerns initially voiced over the scheme died down to some extent.

Information regarding the effects of the scheme can be difficult to access. The Internet Industry Association (IIA) reports periodically to the ABA on compliance with Codes of Practice,[1] and the ABA reports periodically on its activities under the scheme.[2] However, the reports available give little information about the industry's perception of the scheme, nor whether initial concerns have really been allayed.

Surveys

To gather more information regarding the effects of the *Online Services Amendment*, two surveys were conducted in July and August 2001, 18 months after the scheme for online content regulation came into operation. This paper looks firstly to the quantitative data gathered in that survey, such as: what proportion of respondents have changed policies as a result of the legislation or Codes; what proportion believe there have been changes in the internet content

* Lecturer, Faculty of Law, & Research Associate, Baker and Mackenzie Cyberspace Law and Policy Centre, University of New South Wales

[1] The IIA Reports to the ABA in letter form. These Reports were requested from both bodies by the author, but were not released.

[2] ABA *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000, July to December 2000, January to June 2001;* tabled by the Minister for Communications, Information Technology and the Arts, September 2000, April 2001, February 2002 respectively.

available; and changes in the methods of controlling that content and so forth. The paper then looks to the qualitative data gathered in the survey, which allows perhaps a more substantive insight into perceptions of the effects of the *Online Services Act.*

The surveys were not intended to test any hypothesis, and this paper makes no attempt to evaluate the *Online Services Act* on the basis of survey responses. Rather, the information collected in the surveys is intended only to throw further light on early responses to the *Online Services Act.*

Survey Method

The first survey, addressed to industry participants, was distributed electronically to members of the Internet Industry Association, and to members of two Australian ISP email lists.[3] The second survey was distributed in hard copy to those who had made submissions to the 1999 enquiry into the Online Services Bill undertaken by the Senate Select Committee on Information Technology. It was assumed that the former group would be familiar with changes online and within the industry, and that the latter group would have an interest in those changes. One hundred responses were received overall; 74 responses to the email survey, and 26 to the hard copy survey. Respondents to the email survey included content providers, content hosts, filter makers, ISPs, and users.

Not all questions were relevant to all respondents, and thus numbers of responses varied from question to question. Furthermore, it was sometimes difficult to categorise a response as a yes or no answer for quantitative purposes. Where responses could not be reliably grouped into yes / no categories, they were not included in figures given, or where appropriate were separately categorised as 'possibly,' 'maybe,' etc. In this regard the author has taken every care possible to ensure that the figures given are not skewed by forcing inappropriate categorisation.

[3] **isp-australia@lists.isp-lists.com** list and **aussie-isp@aussie.net** list.

Results

Changes to Practice or Policy in the Internet Industry

Industry respondents were asked whether or not they had changed their practices or policies as a result of the *Online Services Act* or Codes. Sixteen had made changes while seventeen had not. When asked how important the changes were, nine classed the changes as trivial only, six thought they were significant, while eight saw the changes as in between the two.[4]

The most commonly cited changes made to policies and practices were moving content overseas, using anonymous proxy servers, and ensuring compliance with the *Online Services Act* and Codes (such as ensuring subscribers are over 18 years of age or having parents sign application forms). A number of respondents put information on their own websites regarding the *Online Services Act* and Codes, or provided links to such information on other sites. Further changes included selling or advising on filter software, and in one case even producing a new filter. Other action included restricting web content in various ways, such as refusing to host anything controversial and removing public service web hosting. At least one respondent would have preferred to continue hosting in Australia rather than moving to an offshore content host.

Respondents were asked how the changes they made to practice and policy impacted upon their organizations, and on their subscribers, viewers, and audience. For their organizations seven respondents viewed the changes as positive, eleven as negative, five as neither positive nor negative, and three as in-between.

Where respondents saw changes as negative for their organizations, they mainly cited the higher cost and loss of control (for example being forced to carry advertising) associated with overseas hosting, which they had moved to as a result of the new legislation and codes. Others saw the changes as requiring additional work, and leading to more uncertainty. On the positive side, changes made as a result of the Codes were seen to increase industry credibility, and to give organizations an opportunity for self-promotion. Only two respondents remarked specifically on content issues in reply to this question; both were concerned about

[4] Some of those who made trivial changes may have answered that they had made no changes.

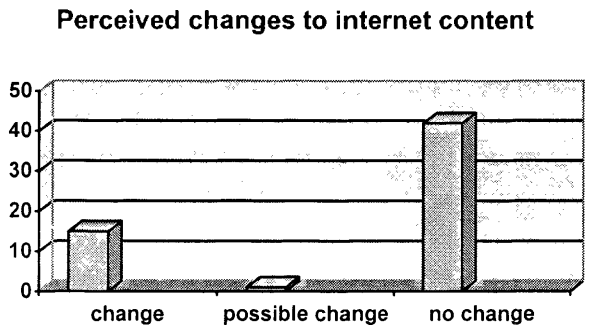
any content restrictions, but one accepted that some internet content does require restriction.

Seven respondents saw the changes as positive for their subscribers, viewers or audience, fourteen saw the changes as negative, and six as neither positive nor negative.

On the positive side, changes to policy and practice were seen to improve service to customers, to raise awareness, to encourage complaints if others were not doing the right thing, and to give users more options in controlling their own access to content. On the other hand, the changes were seen to restrict freedom of the internet and freedom of speech, force some Australian content - especially personal websites - to be removed altogether, or moved offshore when Australian hosts refused to carry the material. This was seen also to weaken the Australian internet industry, and to send Australian money offshore unnecessarily. There was also concern that only commercial filters had been approved, and that there was no disclosure of which sites had been blocked. One respondent also mentioned the potential for increased political control of internet content. Further, significant regulatory issues were seen to arise for young people and those providing services to them, for example, seventeen year-old university students.

Changes to internet content available within Australia

Respondents were asked whether they believed there had been any changes in the types of internet content available in Australia over the past 18 months, and whether or not they thought this was a result of the *Online Services Act* or Codes. Fifteen respondents thought there had been changes to the types of content available, forty-two responded that there had not been changes, and one respondent thought that there may possibly have been changes.



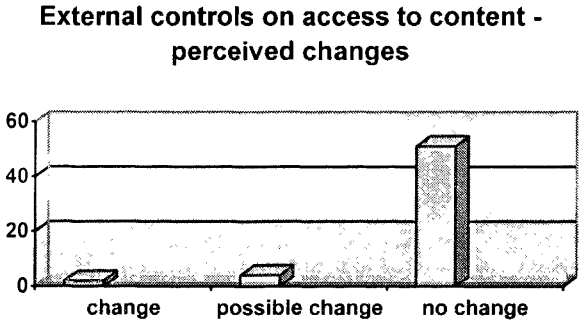
Only three respondents thought the changes were a response to the Online Services Act or Codes, one thought those partly responsible, and sixteen thought the *Online Services Act* and Codes were irrelevant to changes in internet content. The most commonly stated view was that the same types of material are still available, but that there is more of it, and that more material may now be hosted outside Australia. An increase in the use of peer-to-peer technology for distributing content was noted. Some respondents thought there may have been a mild "chilling effect"[5] on local content as a result of host concern about potential liability under the *Online Services Act,* and adult mailing lists and groups were seen to be under pressure, but as a result not of the *Online Services Act* but of overseas Christian lobby groups! A couple of respondents mentioned that overseas standards and legislation would have a far greater impact on available content than would Australian legislation or codes. A couple of respondents thought that the quality of content available had improved. Some thought there were increases in commercial content, more interactive e-business content, and more charging for previously free material. These changes were seen to result from good business planning. There was also seen to be more adult material available, with more aggressive marketing, but less 'mouse trapping' porn.[6]

[5] 'Chilling' was a matter of concern both in Australia prior to the passage of the *Online Services Act*, and in US opposition to the *Children Online Protection Act*. 'Chilling' refers to a situation where speech or communications are not directly censored, but where less is said or communicated to 'be on the safe side' or to ensure one is keeping within the law.

[6] 'Mouse trapping' causes a computer user to lose control over his or her mouse commands – each click opens another window of, in this case, pornographic material, rather than the mouse responding to the user's commands.

External controls on access to internet content

Respondents were asked whether there had been any change in the ability of Australian internet users to access internet material, as a result of external controls (such as filtering or password systems) introduced by ISPs, content providers, content hosts etc. They were also asked whether they believed any such change to be a result of the *Online Services Act* or Codes. Two thought that there had been such changes, with one mentioning a change to a specific site which now required membership and passwords. Four others thought there may have been a minimal change in accessibility, while fifty-one, the vast majority, thought there was no change at all in the ability of Australian users to access internet material.

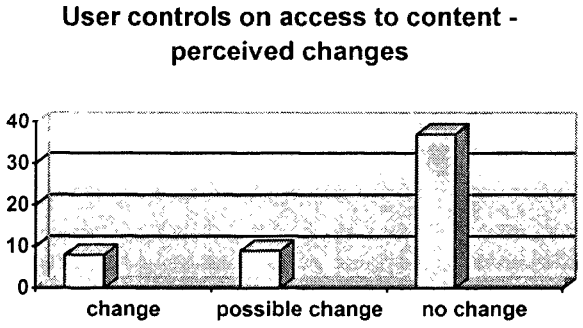


Five respondents attributed any change in content to the *Online Services Act* or Codes, three more thought that the changes were possibly due to the *Online Services Act* or Codes; two mentioned there may be changes as a result of media hysteria, and others mentioned tighter controls at top level users, for example corporations, to control workplace access to some internet content. One respondent thought ISPs may have introduced filtering.

Some respondents suggested that with internet access being cheaper and faster, more people were connected to the internet from home, and so may surf for 'problematic' material from home if blocking occurred at work or school. The *Online Services Act* and Codes may have increased awareness of the availability of internet content, but their most commonly cited consequence is to move sites off shore.

User control of access to internet content

Respondents were asked whether there had been any change in the ability of Australian internet users to control or limit exposure to internet content for themselves or for those under their care. Eight respondents thought there had been some change, nine thought there may have been some change, especially through increased public awareness of filtering products, and thirty seven, over two-thirds, thought there was no change at all.



Seven respondents thought that any changes were a result of the *Online Services Act* or Codes, three possibly so, and fourteen thought that the changes did not result from the *Online Services Act* or Codes.

A commonly made point was that filters had been available and had been used by those who wanted them long before the *Online Services Act* and Codes came into effect. One respondent claimed 'parents are not as stupid as governments think. There have always been sensible ways to use the internet.' Some respondents thought that the use of filters may have increased, with increased public awareness of them, and one respondent thought that filter technology had improved. Others, however, believed filter technology had not changed, that filters were generally ineffective, and often incorrectly installed. A number of respondents were concerned that the promotion of filters would give parents a false sense of security, and lead parents to abdicate responsibility when in fact there was no substitute for parental supervision. One respondent thought the *Online Services Act* and Codes superfluous: 'we don't need Acts or Codes to tell us to keep fireworks or medicines out of the reach of unsupervised children. In the same way we don't need an Act or Codes to tell us that about the internet.'

General Comments

In addition to answering specific questions regarding internet content regulation, both groups of respondents made general comments regarding the content regulation scheme. Submitters were responding to questions about their initial concerns, whether these had been allayed by the *Online Services Act* or Codes, and any continuing concerns. Industry respondents were replying to the more general 'Any other comments?' Responses from both groups overlapped considerably, and so have been collated together.

Very few respondents argued against censorship or content regulation *per se*. Many endorsed some type of regulation either of internet content, of the internet industry, or both. Many, however, criticised this particular legislation and its associated Codes of Practice.

There was criticism of the legislation as ineffective, and this came particularly from respondents who wished for more far reaching regulation. There was concern, for example, that the exclusion of email and chat from the legislation meant that these means could still be used for disseminating hate and racist material. Others were concerned that content restrictions were ineffective firstly because they did not mandate the use of filters or other blocking technology at any level, and secondly because enforcement was based solely on complaints. Some respondents suggested that active and random monitoring of internet content would be far more effective than the current passive 'complaints received' route.[7] Problems associated with relying on complaints included a lack of knowledge about how to complain, the inability of users to distinguish legal from illegal material which may discourage them from complaining, and limitations on the resources of those charged with responding to complaints. One respondent who thought many users were not motivated to complain, felt restrictions should not rely on the motivation of users; there should be proactive monitoring and blocking because the restrictions are not just to avoid offence, but to protect society. Broader but related concerns included questions of whether content to be

[7] The ABA is empowered to investigate material of its own volition, but 'it is not intended that this discretion will be used to monitor content actively.' The complaints mechanism was always intended to be the 'cornerstone of the regulatory framework.' Second Reading Speech, Senate, 21/4/1999 (Official Hansard No 5 19/23 April 1999) p3959-60.

restricted was sufficient and appropriate (for example should racism be more subject to restraint than currently), and whether the classifications scheme was discriminating enough and provided sufficient information about content (classifications should be used better to inform parents and carers and users about the types of material they may see, and what ages various types of material were suited to). While some respondents thought that more blocking should be required, one thought that the legislation, although ineffective in restricting content, was effective in sending out a message about the dangers of the internet, and that the establishment of Net Alert[8] to promote information for internet users was also a positive move.

Other respondents were more critical of the legislation. Commonly expressed criticisms included:

a) that the scheme introduced could not meet its objectives;

b) that the legislation could be more heavily enforced in the future;

c) that the promotion of filters could give internet users a false belief in their effectiveness; and

d) that the operation of the scheme was surrounded by secrecy.

(a) *The scheme*

Some respondents felt that the scheme overall demonstrated a lack of understanding of the technical issues of internet content regulation, and a failure to acknowledge the global nature of the internet. Thus the *Online Services Act* made Australia look reactionary, discouraged investment, embarrassed those in the industry, and insulted the public: "How stupid do politicians think we are? Or don't they think it matters what the public think?" "It has damaged Australia's IT reputation, it has forced traffic positive sites OS, and hasn't improved the safety of home surfers."[9] A number of respondents referred to the ease with which content could be removed from Australian servers and placed on overseas

[8] Net Alert is an independent body established to to conduct 'national education and awareness campaigns to promote the safe use of the internet as an educational and information tool, including by informing parents about filtering and other technologies and the Government's online content regime.' For further information see the NetAlert site at http://www.netalert.net.au/

[9] Quotations not otherwise referenced are taken directly from survey responses.

servers,[10] keeping content as readily available to Australians as prior to the *Online Services Act*. This made the provisions relating to Australian hosted material ridiculous, both practically and economically. As for the notification of illegal and offensive sites to filter makers, this was seen as subsidising, through Australian taxes, commercial operators and "particular vendors, at the expense of a more nuanced community education policy." Expert advice from overseas and from the CSIRO, advising against such legislation, had not been listened to by government.

(b) *Possible future enforcement*

Most respondents were pleased that threats to require ISPs to block content had not eventuated in the final versions of the *Online Services Act* and Codes. However, considerable concern remained that while the *Online Services Act* and Codes currently place minimal responsibility on the internet industry, the *Online Services Act* in fact allows for the placing of far more onerous responsibilities on industry, and thus leaves the industry largely unburdened but also uncertain for the future. One respondent described this as "a ticking time bomb."

(c) *Promotion of filters*

There was considerable concern that filters were being promoted as a means of restricting access to unsuitable material. Many respondents noted that children do need protection when using the internet, but the importance of filters in the current scheme was seen to encourage or develop a false sense of security in parents and carers who may be led to believe that filtering was effective in controlling access. The approval[11] of filters on bases other than effectiveness "brings the legislation into disrepute." One respondent suggested protection of children should be dealt with as a topic in itself, not confused with 'internet regulation' which focuses on the medium rather than the protection.

Filter applications were seen as both too broad and too narrow: not restricting all content they should and restricting some content they should not. There was

[10] Some sites were moved overseas in anticipation of the Amendment coming into force, others were moved in response to take-down notices issued by the ABA. See for example ABA *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation, January to June 2000,* p16 note 3.

[11] The Internet Industry Code of Practice has been amended and now refers to 'scheduled' filters rather than 'approved' filters.

concern most filter products were American, and thus developed for a more conservative market. The bluntness of filter technology worried many respondents further, the inability of filters to distinguish health or educational content from porn or adult content meant a great deal of useful information was wrongly blocked if filters were used. This was seen as a particular concern for isolated and minority groups and individuals who may rely on the internet for information and contact. Some suggested more focus on researching better filter applications and providing information about them, to allow more choice to users.

(d) *Secrecy*

Secrecy surrounding the operation of the scheme was criticised. Respondents said that the internet was the only medium where users where not allowed to know what was censored. Further, reporting on the operation of the scheme was not transparent.

Further responses included criticism of the *Online Services Act* as politically motivated, enacted not to solve problems of internet content, but to gain political favour from right-wing constituents, parliamentarians, and institutions. It was thus seen by some as unsurprising that the scheme should not work to achieve its stated aims.

The ABA's recognition of the IIA as an appropriate body to represent the internet industry and to draft Codes of Practice was criticised by some respondents, particularly those who felt the IIA had failed to take competing views into account in negotiating prior to the legislation, and in drafting the Codes of Practice.

A couple of respondents thought any censorship of the internet was unnecessary and undesirable, while one noted that restricting any material not seen universally as problematic was itself problematic in a culturally diverse society.

Other concerns less commonly noted included the inappropriateness of film classification guidelines for internet content, and the inappropriateness of the broadcasting model of regulation for the internet which is interactive and private.

Responses commonly emphasised the need for self-responsibility in terms of internet content. Many respondents thought it imperative that children were supervised on the internet, and that the community was educated about the internet. Many respondents were concerned that the *Online Services Act* suggested

that 'technical solutions' were available to the 'problem' of internet content, but that this was not really so. Respondents felt that the "attempt to wave a technical wand doesn't work."

Conclusion

Conflicting perceptions of the *Online Services Act* and its associated Codes of Practice are apparent in the results of this survey. However, both those arguing initially against the legislation, and those arguing initially in its favour, seem to have had their concerns somewhat allayed by the actual effects of the *Online Services Act* and Codes. For the former group the outcomes have been less draconian than anticipated, for the latter group any attempt to regulate internet content is a step in the right direction.

Quantitative responses suggest the impact of the legislation and Codes of Practice has been minimal only. Less than half of the industry respondents have made changes to their practices or policies, and most of the changes made have been trivial only.[12] Over seventy percent of respondents perceive no changes to the content available on the internet in Australia,[13] and the vast majority see no changes to external controls exercised over an internet user's access to content.[14] Over two-thirds of respondents also see no change in the ability of users to control content for themselves.[15]

Viewed against the backdrop of the *Online Services Act* and Codes of Practice, none of these findings are unexpected. The *Online Services Act* and Codes of Practice require little of industry members, and it is likely that most could therefore comply without significantly changing policies or practices. Further, it is to be expected than no changes would be found to internet content generally, given that only a tiny proportion of internet content is Australian-hosted, and only a tiny proportion of that content would be subject to the *Online Services Act*. Further, removal of content from Australian servers would not lead to removal of

[12] This mirrors the findings of a study into the response of the adult industry to the *Online Services Act,* where the most common response was to 'do nothing,' followed by 'moved content offshore.' Peter Chen, *'Australian Adult Industry Censorship Survey* 2002,' Centre for Public Policy, University of Melbourne.

[13] 42 of 58.

[14] 51 of 57.

[15] 37 of 54.

content from the internet.[16] The *Online Services Act*, when read in conjunction with current Codes of Practice, requires no external blocking or filtering of content and so it is to be expected that no additional external controls would be experienced. Finally, as filter products were equally available before and after the enactment of the legislation and Codes it is to be expected that respondents would not notice a change in the ability of users to control content for themselves. However, the higher profile given to those products through media coverage of the legislation, and information put out by NetAlert, the ABA, and by ISPs to subscribers, may have led to more awareness of content filtering and blocking devices. This may have led to greater usage of filtering devices, but there is no evidence that this is the case.

The qualitative data gathered in this survey tends to reflect arguments made prior to the legislation and Codes coming into force. There is continued concern, for example, that although the current scheme in fact has minimal impact on industry, and on freedom of speech, the current legislative framework could equally be used to support far harsher regulation. There is continued criticism of the *Online Services Act* as irrational, politically motivated, and a waste of resources. On the other side the concern is that although the legislation may help restrict some 'problematic' internet content, stricter enforcement of the legislative scheme, along with pro-active monitoring of content would be required for the scheme to achieve its stated aims.

The intention of this paper has not been to evaluate the Australian scheme for online content regulation, but rather to draw attention to some of the results of the regulatory scheme, and to highlight the perceptions of the scheme held by industry players and other interested parties. While the IIA reports periodically on Code compliance, and the ABA reports from time to time on the effects of the scheme, the IIA report is not publicly available, and the ABA reports are formal and statistics-oriented. Other information about the scheme, such as the results of a survey conducted for NetAlert by the Communications Law Centre, have not been made available. In such circumstances, it is important to ensure that any information collected on the topic is made accessible to those working, researching, or simply interested in the area. The author welcomes comments.

[16] See above note 10.