1-1-2001

Internet content control in Australia : data topology, topography and the data deficit

David Harte

Edith Cowan University

Internet Content Control in Australia: Data Topology, Topography and the Data Deficit

by

David Harte B.Sc. (Mathematics)

A Thesis Submitted in Partial Fulfilment of the Requirements for the Award of

Master of Science (Computer Science) by Research.

Department of Computer Science,
School of Computer and Information Science,
Edith Cowan University,
Perth, Western Australia.

Supervisor:

Mr. Mark Brogan.

Friday, 23 November 2001

USE OF THESIS

ABSTRACT

The success of the online adult industry has provoked a public policy controversy over the need for Internet censorship, and in recent times there has emerged a desire to protect minors from possibly unsuitable content.

On January 1st 2000, the *Broadcasting Services Amendment (Online Services) Act* (Cwlth, 1999) (BSA) was proclaimed. The Act purports to regulate and control Internet content in Australia. Operating in tandem with the Act is the Internet Industry Association Code of Practice, giving Australia a co-regulatory approach to Internet content control. The Australian Broadcasting Authority (ABA) is charged with implementing the regime. This study sets out examine the Internet content control problem in the Australian context.

The political issues surrounding the topic of Internet censorship and the lack of reliable operational statistics, revealed the difficulty of estimating the effectiveness of the current control regime. Pivotal questions for the study concerned the scope and scale of content control in the Australian context and trends in hosting. This study used website typology, as defined by data topology and data topography, to examine the scope and scale of the content control task, and the implications for the effectiveness of the BSA.

It was expected that if the BSA was to have an impact, that a discernable change in user download behaviour should ensue. This study used information provided by the adult Internet Content Provider (ICP) industry to gauge the BSA's impact on user download behaviour as a measure of the control regime's effectiveness.

It was suggested by some observers that the so-called 'data deficit' between Australia and the US would be exacerbated by the new content control regime, with possible negative implications for the conduct of e-commerce in Australia generally. A study of Australian adult website hosting arrangements and data topography was conducted to examine the implications of the control regime for the 'data deficit'.

This study suggests that most Australian online adult content is in fact hosted in the US. The reasons for offshore hosting are almost totally financial and pre-date the introduction of the *Broadcasting Services Act (Online Services) Amendment Act 1999*. The study also suggests that any effect on the 'data deficit' should be minimal, and that the typology of adult content websites is such that the current co-regulatory regime may prove ineffective in controlling access to adult content.

DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

i. incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

ii. contain any material previously published or written by another person except where due reference is made in the text; or

iii. contain any defamatory material.

Signature

Date 22/3/2002

ACKNOWLEDGEMENTS

There are many individuals who contributed to this thesis, providing guidance and support during this study. I would like to thank all those colleagues and friends who helped and encouraged me with this project. However, there are some special individuals to whom I owe a particular debt of gratitude and deserve special mention.

To my supervisor, Mark Brogan I thank you very much. I have learned an enormous amount from you. Your enthusiasm for this research area really drove this project to completion, but for your good counsel it would have died in infancy. Thank you especially for helping to transform my mediocre ramblings into something worth reading. I know this was often a frustrating chore for you.

To my initial supervisor Dr Timo Vuori, I express my thanks for directing me into this interesting research area and suggesting Mark as the excellent replacement supervisor.

I wish to express my thanks to the questionnaire and interview participants for taking the time to contribute to this study. In particular, I express thanks to the Eros Foundation for their kind cooperation, without which much of the fieldwork conducted as part of the study would not have been possible

I have left until last the ones that I love most dearly. To my wife Brenda especially, your love, support, patience and understanding all helped me through my university years. I could never have succeeded without you. To Emma, Eva, and Robert thank you for your understanding when family life could not be a priority. To my mother and the rest of my family, thank you for your support, and encouragement.

TABLE OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

CHAPTER ONE

1 INTRODUCTION

This chapter contains an introduction to this study of Government enforced Internet content control as defined within the Australian context. The problem addressed by the study is outlined, and the research questions, and hypotheses stated. It concludes with a synopsis of the other chapters of this thesis.

1.1 Background of the Study

1.1.1 Internet Growth and the Rise of Cyber Porn

The Internet is a network[1] connecting millions of computers across the globe. It has its origins in the United States (US) as a military and academic computer network, but has grown to become a global network (Kennedy, 1995, pp. 263-268). The last five years has seen a major increase in the size and complexity of the Internet (Zakon, 2000). The amount of information available via the Internet is increasing daily. In tandem with the growth of the Internet, the number of people accessing Internet content has also grown, and has been estimated by Nua (2001[2]) at over four hundred and eighteen (418) million users by December 2000. By July 2001, Neilsen-NetRatings (2001[3]) suggested that the global figure had increased even further to around four hundred and twenty six (426) million.

In Australia the rate of growth is also substantial, with the National Office for the Information Economy report revealing that half the adult Australian population had accessed the Internet in the twelve (12) months to November 2000 (NOIE, 2001, Executive Summary). In November 2000, the Australian Bureau of Statistics (ABS, 2000) estimated that forty seven per cent (47%) of Australian children aged five to fourteen had accessed the Internet in the previous year. It is

[1] Dodge, M (2002). An Atlas of Cyberspaces: Mapping Cyberspace Using Geographic Metaphors. Available WWW: http://www.cybergeography.org/atlas/geographic.html
[2] Vide Nua (2001) *How many online* (available WWW: http://www.nua.ie/surveys/how_many_online/world.html (20 September 2001)
[3] Vide Nielsen-NetRatings:Hot off the Net (available WWW: http://www.nielsen-netratings.com/hot_off_the_net.jsp (November, 2001)

clear that Australians in general are accessing the Internet in increasing numbers with the ABS also revealing that by 2000, eighteen percent (18%) of Australian homes were connected to the Internet. By September 2001 the Australian Internet population was estimated by Nielsen-NetRatings at over ten (10) million (http://www.nielsen-netratings.com/hot_off_the_net.jsp).

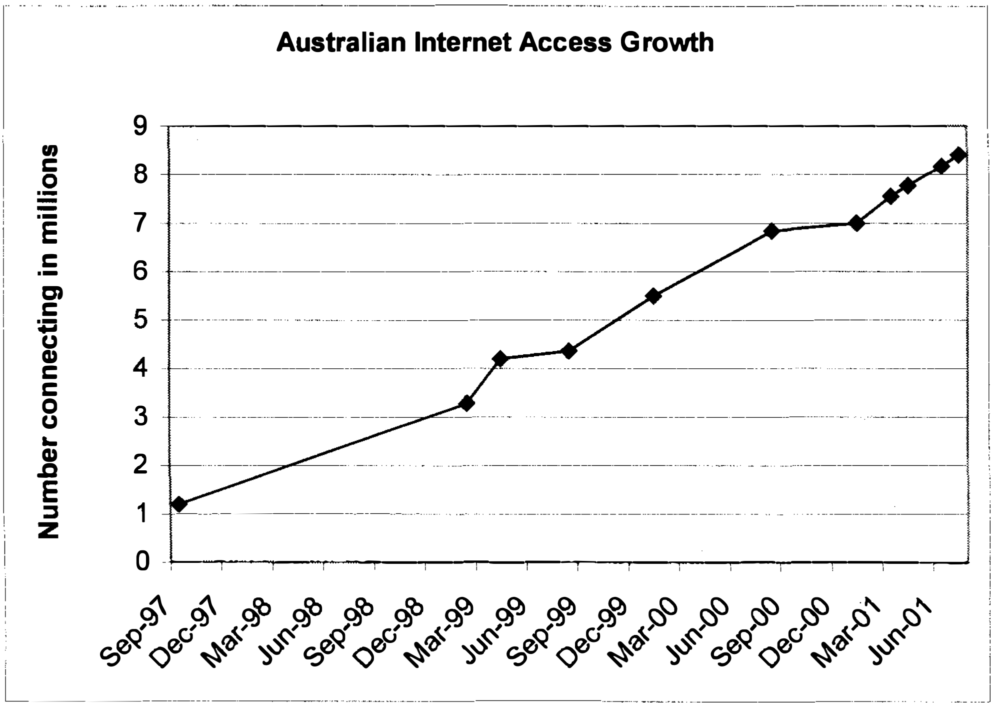

Figure 1-1. Australian Internet access growth (Note. produced from Nielsen-NetRatings data cited in Nua, 2001[2])

Just as it had with the advent of other emerging technologies like photography, cinematography, and video, the pornography industry was quick to grasp the opportunities presented by Internet growth. The development of the Internet allowed, for the first time, the ability to publish uncensored material globally, creating a vast market for the makers and publishers of adult content. As a consequence, erotica and pornographic content have mushroomed on the Internet.

According to Walker (1999) pornography on the Internet began with dial-up Bulletin Board Systems (BBS). The industry was limited until about 1996 when computers and modems capable of downloading and processing digital images became generally available. The adult content industry is now *the* e-commerce success story. Although relatively new arrivals in the adult content business, by 1997 the annual earnings of the top three adult sites were over one hundred (100) million dollars each (Buskin, 2000, Abstract); to put this figure into perspective, the total revenue for the adult publication giant Playboy in the same year was one hundred and thirty eight (138) million dollars (Judge & Green, 1998), and e-commerce giant *Amazon.com* lost over three hundred and seventeen (317) million dollars in one quarter of 2000 alone (Hansell, 2000). Koerner (2000) suggests that the online industry earned one (1) billion dollars in 1998, projecting a figure of three (3) billion dollars for year 2003 earnings (¶ 5); Greenfeld (2000) concurs and also cites research that the 1998 figure was up thirty percent (30%) on the 1997 earnings figure.

Some attempts have been made to estimate the number of adult web sites. Koerner (2000, ¶ 3) cites a Neilsen-NetRatings statistic that seventeen and one half (17.5) million 'web users' accessed adult websites in January 2000 alone. The success enjoyed by adult websites is such that they have been recommended as case study models for anyone wanting to sell content on the Internet (Glidewell, 2000). The number of adult sites on the Internet is not known precisely but Mark Tiarra, president of the industry group, United Adult Sites (UAS) cited in Buskin (2000, Abstract) suggests an educated guess at about two hundred thousand (200,000). This number of sites helps to illustrate the scope and scale of the task of controlling access to erotic content on the Web.

The success of the online adult industry has provoked a public policy controversy over the need for Internet censorship, and in recent times there has emerged a desire to protect minors from possibly unsuitable content.

1.1.2 Regulation and Control

On January 1st 2000, the *Broadcasting Services Amendment (Online Services) Act* (Cwlth, 1999) (hereafter referred to as the BSA) was proclaimed. The Act purports to regulate and control Internet content in Australia (BSA, s. 4(3)). The Australian Broadcasting Authority (ABA) is charged with the responsibility of enforcing the Act. (BSA, Schedule 5, Part 1, s. 2) The Federal Government has also established a 'community based', government appointed advisory body, NetAlert (DCITA, 1999a), to provide ongoing advice to the ABA.

Under the terms of the Act, Australian Internet Service Providers (ISPs) are responsible for ensuring that no "prohibited content" (BSA, clause 10) is hosted on their servers. More problematic, is the requirement in law to ensure that "potentially prohibited content" (BSA, clause 11) hosted on servers outside Australia, is not accessed by their clients via the Internet.

The BSA (clause 59) defines the Commonwealth's desire for a code of practice for the Australian Internet industry. On 16th of December 1999 (ABA, 1999a) the ABA approved an *Internet Industry Code of Practice* (http://www.iia.net.au/code6.doc) (hereafter referred to as the Code). The Code lays out a modus operandi for Australian ISPs in content filtering. Although much confusion abounds, it appears that while operating within the Code, ISPs are not required to review, filter or in any way control their client's access to web content (ABA, 1999b). The only requirement is to comply with the takedown notices (ABA instructions to remove content from servers) and to inform their clients of the availability, and use of client-side filtering software. The ISPs must also recommend to their content producers the use of content rating labels.

Since the introduction of the Act, the ABA has published operational statistics on the regulatory scheme, the most recent of which was in April 2001 (ABA, 2001). However the ABA's refusal to release raw data has been controversial. The cyber rights advocacy group Electronic Frontiers Australia (EFA) has sought access to ABA data under the Commonwealth's Freedom of Information Act (EFA, 2001a). The ABA's rejection of third party access to data, on which it bases its activity reports, has prevented rigorous scrutiny of the operation of the current content regulation regime. The absence of grounded, rigorous research on the impact of amendments to the BSA makes for poorly conceived public policy that may retard the growth of the Internet Industry and lead to increased costs to the industry, that are ultimately passed on to users. Within the scope of the research problem as defined, this research attempts to address the problem. Pivotal questions for the researchers concerned the scope and scale of content control in the Australian context and trends in hosting.

It was expected that if the BSA was to have an impact, that a discernable change in user download behaviour should ensue. What methods might be used to measure such a change? Payment for adult content on the Internet is almost exclusively made by credit card. Personal information including name and address is collected when registering with adult sites for credit card transactions. In some cases the IP address of the applicant is also logged. Therefore, the adult website operators have records of their client's transactions and most importantly their geographic locations. Any impact of the BSA should appear in these records. This study used information provided by a group of six (6) Australian adult website operators to gauge the BSA's impact on user download behaviour as a measure of the control regime's effectiveness.

1.1.3 Towards a Data Deficit

During debate regarding the Bill in 1999, the Internet industry argued that a likely consequence of this legislation would be that erotic content would be forced overseas resulting in losses to the local industry. It was also argued that erotic content would continue to be accessed by Australians. If large volumes of such content were shifted, from local .au domain download to intercontinental download, it would present a much higher cost to the service provider. The retrieval of content over the congested intercontinental telecommunications backbone is much more expensive than from a server within the Australian domain. Brendan Scott, an Australian lawyer specializing in this area makes a pertinent observation on this issue, revealing:

> "Forcing the content out of Australia also means that inbound traffic into Australia is increased. Australian carriers are currently forced to buy content from US carriers, but must give Australian content to the US carriers for free."
>
> (Scott, 1999a)

This imbalance, Scott (1999a) argues, is a direct consequence of the amount of traffic that is incoming to Australia from the United States. Forcing more Australian content offshore, he suggested, would only exacerbate the situation, adding to the so called 'data deficit' between Australia and the US. Further, the Federal Minister for Communications, Information Technology and the Arts, Senator Richard Alston suggests that the financial impact of the 'data deficit' resulting from current arrangements between Australia and the US is considerable, commenting:

> "It is estimated that the annual opportunity cost of the existing arrangement for Australia runs into the hundreds of millions of dollars....While per-megabit international Internet charges are falling rapidly, the current charging arrangements have meant that Australian Internet users pay more for Internet access than they would under a more competitive regime."
>
> (Aldred, 2000)

The current data exchange arrangements are a result of the imbalance or 'deficit' in data traffic between Australia and the US. The high cost of bandwidth in Australia that results from these arrangements place Australian Internet users, and in particular high bandwidth commercial Internet Content Providers (ICPs) at a disadvantage when competing with US hosted ICPs. Therefore, the 'data deficit' impacts on the conduct of e-commerce in Australia generally.

1.1.4 Internet Service Provider (ISP) Industry Issues

1.1.4.1 Effect on competition

The Australian Internet industry is now operating within a co-regulatory framework for content control. There is no guarantee that this situation will continue indefinitely. Operating within the co-regulatory framework may have financial implications for the industry, either those caused by the increasing 'data deficit', or simply a loss of revenue. The scope and scale of these costs is largely unknown. Gibson (2000, p. 10) suggests that the small ISPs might be affected most. It is unclear what the ramifications are for these small operators, but increased costs may present a barrier for entry into the market. Furthermore, established players in the market may find it impossible, to pass on increased overhead costs to clients. Barriers to the entry of new firms and increased overheads may cause a skew in the market towards larger ISPs capable of absorbing the increased costs. A decrease in overall price competition and the number of firms participating in the market might arise. The regime may have as yet unforeseen repercussions for the overall Australian Internet economy. This study examines the scope for cost impacts attributable to compliance with the amended BSA and industry code. The impact of the Internet economy on the economy generally is growing (NOIE, 2001).

Compliance problems for the Australian Internet economy may have increasing negative consequences for the economy as a whole.

1.1.4.2 Compliance costs

Controlling Internet content has many and various costs. The costs in terms of bandwidth, service degradation, hardware, and software are outlined in Greenfield (1999, pp. 5-8). If ISPs are forced into full, server-side, application level blocking, Budde cited in Gibson (2000, p. 6) estimates that the compliance cost to the Internet industry at $150 million. However, assuming a continuation of the present regime, infrastructure and administration costs should be minimal.

As already outlined, it was predicted that if large amounts of Australian hosted adult content was forced offshore by the legislation, then retrieval costs for ISPs would increase (Scott, 1999b, Problems with the Act). There is no reason to assume that under the current system, people who currently access sex sites will not continue to do so, but at an increased cost to ISPs. The measurement of these costs is problematic and complicated by the ISP industry structure and technical issues such as network content caches.

Another predicted cost to the industry was in terms of loss of revenue. Anecdotal evidence suggests that hosting costs in domains such as the US, are significantly less than in Australia. If the adult content producers were forced to remove their sites by the ABA, it is probable that they will host offshore. The download traffic generated by these sites would then be outgoing, and revenue producing for an offshore ISP. This would represent a double-hit for the local industry, an increase in retrieval cost, and a loss of revenue. This study examined the effects of the BSA on the data deficit and its possible impacts on the ISP industry.

1.1.5 Technical Considerations

In April 1999 the Commonwealth Scientific and Industrial Research Organisation (CSIRO) Division of Mathematical and Information Sciences released their report *Technical Aspects of Blocking Internet Content* (Greenfield, 1999), which was commissioned by the National Office for the Information Economy. In this report the CSIRO outlined the scale of the filtering problem revealing that, "A simple check using the Alta Vista search engine produced over 13,000,000 hits for pages containing the word 'sex'" (Greenfield 1999, p. 5). Controlling access to so many webpages is obviously problematic. However, the author of this study suggests that even this is not a valid representation of the true scale of the problem and that website typology reveals an even more complicated problem.

1.1.5.1 Website typology, topology and data topography

The author defines website typology as the study of website types, which is a product of two factors:

1. Website Topology is a multi-dimensional construct made up of a site's: -
   - Internet topology[4]: -

     How the site connects and presents itself to the Internet community;
   - Data topology: -

     How the individual components that comprise the website's content are interconnected (hyper linked); and
   - Industry topology: -

     An examination of industry practices and marketing techniques influencing website structure.
2. Data Topography: - a term the author suggests for a study of the geographic locations of website content and the volumes of data at these locations.

This study used website typology to examine the scope and scale of the content control task and the implications for the effectiveness of the BSA.

1.2 The Purpose of the Study

This study applies grounded research in the area of Internet content control in Australia. For the reasons already outlined, the availability of reliable, independent data in this area is scarce. The political climate has produced a proliferation of claim and counter-claim, both for, and against the implementation of the control regime.

[4] Dodge, M (2002). An Atlas of Cyberspaces: Topology Maps of Elements of Cyberspace. Available WWW: http://www.cybergeography.org/atlas/topology.html (27 February, 2002)

Operational statistics produced by the ABA to highlight the success of the scheme cannot be corroborated. In particular the ABA's refusal to allow public access to raw data on the operation of the regime for analysis impedes the conduct of grounded research on the regime's impact (EFA, 2001a).

The importance of the issues in public policy terms should not be underestimated. Claims of an ensuing deterioration in the data deficit, and predictions of increased compliance costs for the ISP industry as already outlined[5], have implications for the conduct of e-commerce in general in Australia. The study set out to gauge the size of the adult content control problem in Australia, and to measure the impact of the BSA on the adult content industry, the data deficit, and user download behaviour, as indicators to the overall effectiveness of the scheme.

1.3 Research Questions and Hypotheses

This study provides an insight to the scope, scale and cost of control of content on the Internet. The practical application of the legislation presents technical and financial issues, which are unprecedented in the Australian context. The research questions underpinning this investigation are:

1. What is the scope and scale of the content control task in the Australian context?

2. Did content from hosts in the .au domain shift to overseas hosts as a consequence of amendments to the Broadcasting Services Act?

3. Have changes in data topography contributed to the worsening of the 'data deficit'?

4. Can metrics be generated that indicate a change in end-user download behaviour attributable to the new content control regime?

[5] 1.1.3 Towards a Data Deficit and 1.1.4 Internet Service Provider (ISP) Industry Issues

5. What are the financial implications for the Australian ISP industry operating under the co-regulatory system?

6. Are there any implications for the operation of mainstream e-commerce in Australia arising from the introduction of Internet censorship?

The following hypotheses are *tested* in this study:

1. A significant Australian hosted adult content industry existed before the *Broadcasting Services Amendment (Online Services) Act* (Cwlth, 1999) came into effect on January 1, 2000;

2. Before or after January 1, 2000 Australian hosted adult Web sites moved offshore to foreign hosts;

3. Changes in hosting arrangements for Australian adult Web sites have contributed to a data deficit in Internet traffic; and

4. Current content blocking measures are effective in terms of the data topography and topology that characterise adult Web sites.

The following working hypothesis is held true and therefore untested:

Ceteris paribus, trends in data topography involving movement of high volume Australian hosted content to offshore hosting arrangements correspond to an increase in the data deficit.

1.4 Summary and Synopsis of the Study

In summary, this chapter has:

*provided an overview of the recent history and nature of the regulatory framework for Internet content control in Australia;

*outlined possible implications for the ISP industry and for the conduct of e-commerce in Australia more generally arising from the framework;

*described impediments to the conduct of rigorous research on impacts and challenges posed for research methods;

*described the construct of Website typology inclusive of the dimensions of data topology and data topography; and

*outlined the main research questions and hypotheses to be investigated in this study.

Chapter Two takes the form of a review of the relevant literature. The review seeks to add some background to the content control debate, the structure of the adult content industry and the technical aspects of Internet operations necessary for an understanding of the problem studied.

Chapter Three describes the research design, outlining the aims of the design, and reasons for the design chosen. Limitations of the design are acknowledged and discussed.

Chapter Four presents the results of the study detailing the findings. The results of the typology study are tabulated and the other research method's results stated.

Chapter Five concludes the study with a discussion of the research findings. The implications of the results are discussed in the context of the research questions and hypotheses and suggested further research areas explored.

CHAPTER TWO

2 LITERATURE REVIEW

2.1 General Literature

2.1.1 The Changing Focus of Censorship

In Chapter One it was argued that the online pornography industry is *the* Internet e-commerce success story. The numbers of people accessing pornographic material via the Internet is increasing, prompting an intractable public policy controversy over the need for online censorship.

The history of the online censorship debate is as old as the Internet itself. Cyber rights advocates have opposed cyber censorship, often questioning whose interests are actually being protected. Chomsky (Lumby, Cross & Mountford, 1997, pp. 67-70) and Kendrick (1995, p.253) see the portrayal of Internet as a warehouse for cyber porn and other objectionable material as part of a campaign to demonise computer networks, waged variously by anti-pornography feminists, right-wing pro-censorship elements, or the established print and broadcast media. However, such concerns are not mainstream, where positions have mostly developed around the effects of exposure to pornography.

Wallace (1999, p. 161) claims that "Some social scientists maintain that the use of sexually explicit materials is harmless, and that it can also be functional, healthy, and liberating in some contexts because it provides education, erotic enhancement, an outlet for exploration, and entertainment", whereas, "Others however, point to the ethical and moral issues involved — particularly the exploitation and objectification of women" (Wallace, 1999, p. 161). She suggests that men are "far and away the principal users of pornography" (Wallace, 1999, p. 161). However, this may be cultural specific. Within the Asian market, Viewpoint (2001, p. 1) argues that, "35%-50% of online users view adult material, and of these users 35%-40% are women" (Viewpoint, 2001, p. 1). Could it be that the perceived anonymity of what Lin (1996, section II) termed the "Net persona" has overcome social taboos and allowed women to access this material in increasing numbers? Whatever the case, the protection of children has become the main focus in the censorship debate.

2.1.2 The Child Protection Focus

The Meese Report (1986) cited in Tate (1990) noted that US law enforcement agencies had found that Internet bulletin boards were used for communication between pedophiles commenting, "pedophile offenders and child pornographers have begun to use computers for communications" (Tate, 1990, p. 209). An article published in Time magazine in July 1995, (Elmer-Dewitt, 1995) outlined the findings of a Carnegie Mellon University researcher Marty Rimm, who claimed that over eighty-three percent (83.5%) of images posted on the UseNet were pornographic and that his study "identified consumers of pedophilic and paraphilic pornography via computer in more than 2000 cities in all fifty states in the United States, most Canadian provinces, and forty countries, provinces and territories around the world" (Rimm, 1995, Section B. ¶ 4). The article went on to claim that the adult BBS market was "driven largely by a demand" for "deviant" material including "pedophilia ... hebephilia and what researchers call paraphilia—a grab bag of 'deviant' material that includes images of bondage, sadomasochism, urination, defecation, and sex acts with a barnyard full of animals" (Elmer-Dewitt,1995, p. 40). Wallace (1999, p. 158) and Kendrick (1996, p. 255) both revealed the bogus nature of Rimm's report on which Elmer-Dewitt had based the article. Time subsequently retracted the article, but the damage was already done with pro-censorship members citing the study's findings in the US Congress (Chapman, 1995, p. 11). The impact of the article was such that Weckert and Adeney (1997, p. 51), almost two years later in a more balanced study, wrongly suggested that "the most popular kind of pornography [on the Internet] seems to not be of the 'nicest' kind". Furthermore they suggested that "While it may not be good that certain sorts of things are communicated.... it may well be worse overall if this form of communication is restricted in ways that would limit the effectiveness of the Internet" (Weckert & Adeney, 1997, p. 55). Overall they said, " Censorship of Internet pornography is not justified, except perhaps in the case of children" (Weckert & Adeney, 1997, p. 56).

Kendrick (1996) suggested that children were deliberately included in the debate by pro-censorship elements. He proposed that children were the latest manifestation of what he termed the "Young Person", a metaphor for those individuals that society believed needed protection from pornography during the two hundred (200) years of what he called the "pornographic era" (Kendrick, 1996, p. 260). Notwithstanding the issue of pedophiles using the Internet, and the dangers they present to children, the record of quality research on the possible effects of children accessing pornographic material available on the Web is disappointing. Hawkins and Zimring (1998) argue that "there are very few empirical data available on the question of children as consumers of pornography" (Hawkins & Zimring 1998, p. 187), suggesting that there is more data on the effects of exposure to violent images because society considers this acceptable while exposure to pornographic images is not acceptable. They concluded, "a social context in which the existence of pornography is acknowledged and generally accepted by adult society might enable children to adjust more easily to their personal experience with it" (Hawkins & Zimring, 1998, p. 189). Societal taboos make rational research in this area difficult.

The emotive issues of pedophilia and child sexual abuse have been used to 'muddy the water' somewhat in the debate over the availability of adult content on the Web. Such activities are criminal acts in most jurisdictions. National child protection in this area is obligated under 19, 32 to 36 of the United Nations Convention on the Rights of the Child (Dionne, 1999, section 4, ¶ 1). Despite media hype, child pornography is not part of the commercial online adult content industry, but the application of the term 'illegal content' has blurred the distinction between legality of content in terms of a censorship classification, within a jurisdictional context, and content resulting from criminal activity that could never be classified.

Undoubtedly, there has been a major proliferation of adult content on the Internet. Whether the exposure of children to this material is damaging is a contentious issue beyond the scope of this study, but concerns in this area have led to a desire to implement some control. How this is to be achieved is the focus of where the debate on Internet content control has moved.

2.1.3 Legislating for Cyberspace

The problem for governments is that the ‘borderless’ nature of the Internet presents major jurisdictional issues. Nonetheless, the literature notes cases where Web users have fallen foul of national legal systems. Heaton (2000) outlines two notable cases. One case involved the giant Internet site Yahoo.com that operated an online auction system. A French court ordered Yahoo to “make it impossible” (Heaton, 2000, p. 109) for anyone in France to access Nazi memorabilia. It is interesting that the court placed the onus on Yahoo to block access, not French ISPs. The result of this case was that Yahoo banned the memorabilia from all its auction sites, Heaton (2000. p. 109) suggests that this “amounts in practice to the imposition of French law on Internet users worldwide”. Heaton also discussed the prosecution of German-born Australian Frederick Töben.

On a visit to Germany in 1999, Töben was arrested for posting material on the Internet in Australia claiming that the Holocaust was a fabrication, this is illegal in Germany. Even though the material was not hosted within German jurisdiction, Töben was successfully prosecuted and sentenced to ten (10) months imprisonment. This, Heaton argues, represents a precedent confirming “German law applies even to foreigners who post material on the Internet in other countries”(Heaton, 2000, p. 110). The precedent is limited to the authors of the material; the hosting ISPs have no liability.

In Australia there have been many notable successful prosecutions for illegal use of the Internet particularly in the area of child pornography. Sullivan (1997, p. 233) outlined several prosecutions for obtaining child pornography via the Internet, and maintained that this suggests that existing laws can be used to deal with Internet pornography, Sullivan also suggests that the debate has shifted to focus on the protection of children from the perceived threat of the Internet. Clarke (1998, pp. 76-77) revealed the somewhat tragic case of an Australian Capital Territory resident prosecuted after contacting police *himself* regarding a child pornography image he had downloaded on the Internet.

Despite these notable successful legal actions, jurisdictional issues and the differing legal, moral and ethical standards around the world still present major problems for the law in this area. Interestingly, the issue of pedophile content is perhaps the only one with a universal standard response, with as already outlined, a record of successful legal control and sanctions. In spite of this there has been a move towards content control regimes in many countries.

2.1.4 Towards State Control of the Internet

Content control regimes are now in place to some extent in many countries including Australia, UK, Singapore, Ireland, and to some extent the US, with draconian control regimes in China, Saudi Arabia and Myanmar (Endeshaw, 2001, pp. 158-161) where total state control over Internet access is exercised. The results of a survey into consumer attitudes to Internet content blocking cited in McCrea, Smart & Andrews (1998, p.43) concluded that Internet users have little concern for indecent material. The same study showed that only fifteen percent (15%) of non-Internet users were concerned. In the absence of proof of community concern, Governments have nonetheless demonstrated that they are more than ready to regulate for the control of content.

Nolan and Gibson (1974) cited in Westphal and Towell (1998) assert that the adoption of new technology follows four stages:

- Early Success
- Proliferation
- Control of Proliferation
- Mature Use

Westphal and Towell (1998) reported the results of a survey of five hundred and ten (510) ISPs in forty (40) different countries. This study was designed to examine issues of "Control of Proliferation" in terms of content and "acceptable uses" of the Internet. They suggest that the rapid growth of the Internet indicates that it is in the "Proliferation" stage. They further suggest that government moves towards content control indicates the Internet is entering the "Control of Proliferation" stage. The report concludes that pressure to regulate the Internet is primarily from government and that "censoring indecent and potentially criminal material were the main reasons chosen for regulation" (Westphal & Towell, 1998, p. 30).

In an examination of content control in the Asia Pacific Region, Connolly (2001, pp. 129-131) suggested that although adult content was an issue, the focus of attention was Internet gambling, and commented “Governments in Asia take this issue more seriously than general content regulation (such as for adult material) because of the serious revenue implications involved” (Connolly, 2001, p. 129). Governments in this region tend to take a pragmatic approach to content control, even in Singapore where a control regime has been in place since 1996. The control regime in Singapore was examined in a study by Yee (1999).

According to Yee, the Singapore Broadcasting Authority (SBA) administers the scheme. All Singaporean groups or individuals wanting to post material to the Internet, must register with the SBA, and are held responsible for the content. In the case of political or religious groups, they must apply to the SBA for a license to post content. Although commenting on one major prosecution under the scheme, Yee maintained that the “implementation of internet [sic] regulations in Singapore ... has generally been regarded as mild” (Yee, 1999, p. 45), and suggested that competition between Singapore and Malaysia to become the Asia Pacific hub of the Internet was a prime consideration. Businesses are exempt from the Singaporean scheme. Similarly, Malaysia, which also has a control regime, has exempted the Multimedia Super Corridor, a specialized Information Technology industry zone from any censorship (Yee, 1999, p. 46).

The Singapore scheme is interesting as it received favourable mention by ABA officials, in submissions before the Select Senate Committee investigating content control. The facts that the number of websites hosted in Singapore had increased from nine hundred (900) in 1996 to five thousand five hundred (5500) in 1999, and revenues from online business had quadrupled in the same period were suggested as proof that e-commerce can flourish within a control regime (Senate Hansard, 1999a, IT 14, p. 18).

On the other side of the Pacific, in North America, divergent approaches to the issue of content control are apparent. In an analysis of the Canadian administration’s view, Connolly (1999, p. 43) reported on the attitude of the Canadian Radio Television and Telecommunications Commission (CRTC). The CRTC declared that it would *not* impose content control on the Internet to regulate offensive and illegal material. They noted that existing criminal law, industry self-policing, filtering software and increased media coverage of the problem should all have a role in monitoring Internet content. The Vice-Chairman of the CRTC was quoted saying, “The CRTC has no role to play in the development of the internet [sic] in Canada — not now, not later” (Connolly, 1999, p. 43).

In the US, the hub of the online adult content industry, the child protection issue assumed prominence. The *Communications Decency Act* (1996) was the US Government's response to the calls for censorship and control. The act was an amendment to the federal *Telecom Deregulation and Reform Act (1996)*:

> “the amendment—known as the Communications Decency Act of 1995-would impose criminal penalties on anyone who ‘purposefully makes available’ indecent online material to a person under the age of 18. Violators would face fines as high as $100,000 [Later increased to $250,000] and convicted offenders could face two-year jail terms.”
>
> (Hellwege, 1996)

The US Supreme Court however, ruled (*Reno Vs ACLU,* 1997) that this law contravened the First Amendment to the US Constitution. In 2000, Congress passed the *Children's Internet Protection Act (CIPA)* (2000), which received presidential approval on December 21, 2000. This legislation restricts federal funding to schools and libraries that do not meet content blocking policy and technology requirements. The scheme came into force in April 2001 (ALA, 2001). The American Civil Liberties Union (ACLU) has challenged the constitutionality of this act also, on the grounds that it contravenes First Amendment rights (ACLU, 2001).

The content control debate in Australia has followed a similar pattern, with the rationale that content control protects children. However, Australian citizens do not currently enjoy comparable constitutional protection in terms of freedom of expression and association.

2.1.5 The Australian Commonwealth Government Response

In Australia, in the federal sphere, the history of content control investigation by the legislature may be traced through the operation of two Senate select committees: the *Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies*, and the *Select Committee on Information Technologies.* Since 1994 these enquiries have produced three main reports including: *Report on the Regulation of Computer Bulletin Board Systems* (DCA, 1994), *Report on Regulation of Computer On-Line Services Part 2* (Senate, 1995), and *Report on Regulation of Computer On-Line Services Part 3* (Senate, 1997). All of this activity culminated in the formulation and promulgation of the *Broadcast Services Amendment (Online Services) Act 1999*, the BSA.

Some witnesses were concerned by the proliferation of adult Web content concurrent with a rapid increase in the numbers of Australian children accessing the Internet. This growth has continued apace since with almost half of all Australians aged five to fourteen (5-14) accessing the Internet in 1999-2000. In Western Australia, the leading Australian Internet-using state, during the June quarter 2001, twenty eight percent (28%) of children in this age group had accessed the Internet from home (ABS, 2001a).

The call for legislation to protect children from Internet content and criminal activity was a recurrent one during submissions to the Senate Select Committee (Senate Hansard, 1999a, 1999b, 1999c, 1999d). It was argued by members of the committee that the computer literacy of Australian children was so high that client-side filtering could not be reliable as the under-age users could easily circumvent it. This echoed what Kendrick (1996, p. 254) called the "alarm caused by the sense shared by many adults that their computer-wise offspring were already sophisticated enough to evade any attempt to protect them". This attitude suggests that the fear is not of children accidentally finding adult content on the Web, but actively seeking it. Kendrick also suggested "Innocent or depraved, children handily wielded a power denied to their elders, and no one could dictate what they did with it"(Kendrick 1996, p. 264). This was one of the prime reasons that the Australian legislation involved Internet Service Providers (ISPs) in an attempt to remove the problem at its perceived source.

2.1.6 The Broadcasting Services Amendment (Online Services) Act

The *Broadcasting Services Amendment (Online Services) Act 1999* (hereafter referred to as the BSA) regulates Australian Internet content by use of a complaint and classification protocol (BSA, Division 4). Internet content is rated within the same classification guidelines as film and video (BSA, Clause 13). However, the ABA does not operate an active classificatory program. Rather, a passive approach to regulation has been taken which operates on the basis of third party submission of complaints to the ABA concerning Australian hosted content that does not meet

Office of Film and Literature Classification (OFLC) guidelines. Under these procedures, still picture images and text available on the Internet are classifiable as if they were motion pictures, and are therefore potentially subject to a much more stringent censorship protocol. The *Classification (Publications, Films and Computer Games) Act 1995* provides the umbrella legislation. The classification scales applied to films are defined in the act (Part 2. s.7 (2)) as well as the classification guidelines to be applied (Part 2. s.12). Application results in different censorship rules applying to the *same* content depending on the medium used to publish it. For example, images and text classified as legal content and available in magazines unrestricted may be deemed illegal content if the magazine pages were scanned and published to the Internet. This classification task would appear to be one of mammoth proportions given the size of the Internet, and its present and projected rate of growth (Nua, 2001[6]). The Commonwealth is presently involved in a review of the classification guidelines that apply in this area (OFLC, 2001), partly in response to the dynamic nature of new media subject to classification.

For material hosted outside Australia, the ABA is empowered to classify the material (BSA, Division 4, s. 40 (1)). Australian hosted content found to be unsuitable becomes the subject of a takedown notice issued by the ABA to the Internet Content Host (ICH), usually an Internet Service Provider. A takedown notice is an official notification to the Internet Content Host (ICH) that the offending material (not the content owner) has failed the classificatory test and that the website must to be removed from the server. Non-compliance with such a notice carries considerable monetary penalties (Scott, 1999a).

As already noted, service providers are responsible for ensuring that no "prohibited content" (BSA, clause 10) is hosted on their servers, and the more problematic requirement in law to ensure that "potentially prohibited content" (BSA, clause 11) hosted on servers outside Australia, is not accessed by their clients via the Internet. The BSA also provides protection to the content hosts in respect of any civil proceedings arising from compliance with the Act (BSA, clause 88). While the BSA sets out a framework for future Internet content filtering and restriction, it does not specify how this may be accomplished, neither logistically nor technically. This then

[6] Vide Nua: charts and analysis. Available WWW: http://www.nua.com/surveys/analysis/graphs_charts/index.html

is the legal framework within which the Australian Internet industry and content providers must operate.

The approval of the present industry Code by the ABA has resulted in a co-regulatory framework. The adoption of this framework, and in particular the fact that server-side filtering is not mandated, has resulted in minimal compliance costs for ISPs. For the present at least, the financial imposts forecast by industry commentators in Senate submissions prior to BSA enactment have been forestalled. It should be noted however, that this situation might change at any time by simply changing the Code. The ABA has the power, under Clause 4, to override any access control measures already put in place by an ISP, and impose its own access controls, such as requiring Personal Identification Numbers (PIN) or other access controls (Endeshaw, 2001, p. 175). Full compliance with the BSA and the imposition of a mandatory server-side content management regime could prove problematic for some ISPs.

Child protection in the area of pornography and especially child pornography was already accomplished, it may be argued, by section 85ZE of the C*rimes Act* (1914). In a submission to the Senate committee, an official of the Department of Communications Information Technology and the Arts (DCITA) suggested that prosecutions under this section were not assured as it did not classify 'offensive' material sufficiently (Senate Hansard, 1999c, IT124, p. 9). The BSA (BSA, Schedule 2) has amended section 85ZE and defined offensive material in clauses 10 and 11.

The estimated cost to the Commonwealth for the co-regulatory scheme is $1.9 million with an estimated $1.25 million of this going as fees to the OFLC to classify content (Senate Hansard, 1999c, pp. 29-30).

The Commonwealth does not have total jurisdiction in relation to content control. The States are required to have complementary legislation in place. Various state governments introduced content control legislation prior to the introduction of the BSA (EFA, 2001b) and the South Australian government is set to introduce the *Classification (Publications, Films and Computer Games) (Miscellaneous) Amendment Bill (No. 2) 2001* to bring their legislation into line with Commonwealth legislation. The introduction of this new content control legislation in South Australia has helped to maintain the debate somewhat in Australia. The South Australian legislation has been highly contentious. Internet Content Providers, under the proposed legislation, act illegally if they post content that fails the classification test, even if it has not been previously classified. It has been suggested that this could lead to individuals unknowingly breaking the law (EFA, 2001).

The need for child protection, balanced with freedom and privacy for adults, was expressed by the Australian Computer Society (ACS) in their Senate submission (Argy, 1996, Section 4, ¶ b). In his submission for the ACS, Clarke states:

> "The principles which ACS accepts are:
>
> - freedom of expression
> - protection of children from material which is harmful
> - the need to establish appropriate levels of privacy for personal communications between adults and for commercial transactions
> - the need to promote freedom of choice for consumers "
>
> (Argy, 1996)

The extent to which such principles sit compatibly with the current co-regulatory regime is the subject of controversy in the policy community. How cross frame dialogue about the principles and their implementation can be facilitated is not the focus of this research. What has been documented is a brief survey of recent legislative activity and the positions of members of the policy community.

2.2 The Technology in Literature

2.2.1 The TCP/IP Protocol Suite

According to McCrae, et al. (1999, p.9), the Internet is a *packet switched network*. Communications are conducted by breaking the message stream into individual pieces known as *packets* or *datagrams*.

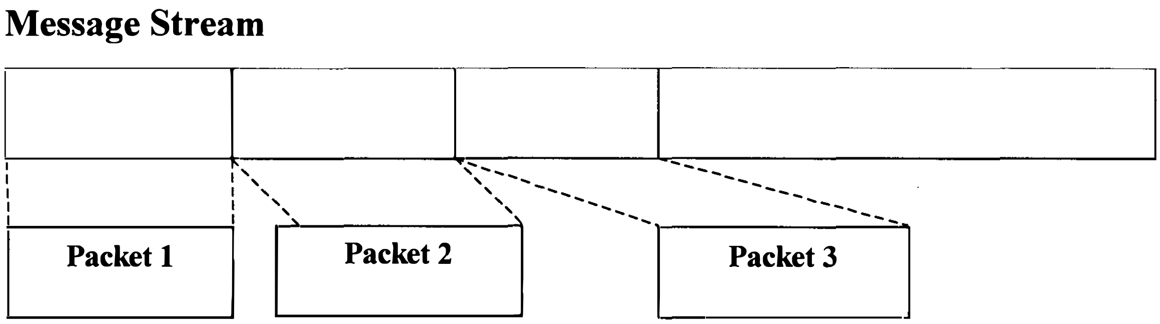

Figure 2-1. An Internet message is broken into packets. (Note. Adapted from McCrea, et al. p. 9, Figure. 2)

The packets are then switched or *routed* from their source, to the target destination, using computers known as *routers*. Routers are usually, high-speed computers optimized for packet routing. They use the Internet Protocol (IP). Operations involving IP are *packet level* operations. IP uses a connectionless datagram (packet) delivery protocol. It performs the addressing, routing and control functions needed to transmit packets over the network. Every packet contains addressing information detailing the source and destination of the packet.

IP Header: Destination IP Address Source IP Address Sequence Information	Information Payload

Figure 2-2. IP Datagram format (Note. Adapted from Feit, 1996, p. 31)

Also included in the packet are the control information and the actual data that is passed from the source host to the destination host. As a connectionless protocol, there is no fixed connection from source to destination. The address information contained in the packet is used to compute the best route to the destination host. It is important to note that this process takes place for each packet sent. Different packets from one session of communication between two computers may, and probably do, take different routes from source to destination. This ability to re-route packets was deliberately designed into the protocol to deal with possible damage to the Internet. Figure 2-3 illustrates the process, with a message that has been broken into 10 packets. Three packets travel via Router 1 on Path A, four via Router 2 on Path B, and the remaining three, via Routers 3, and 4 along Path C.

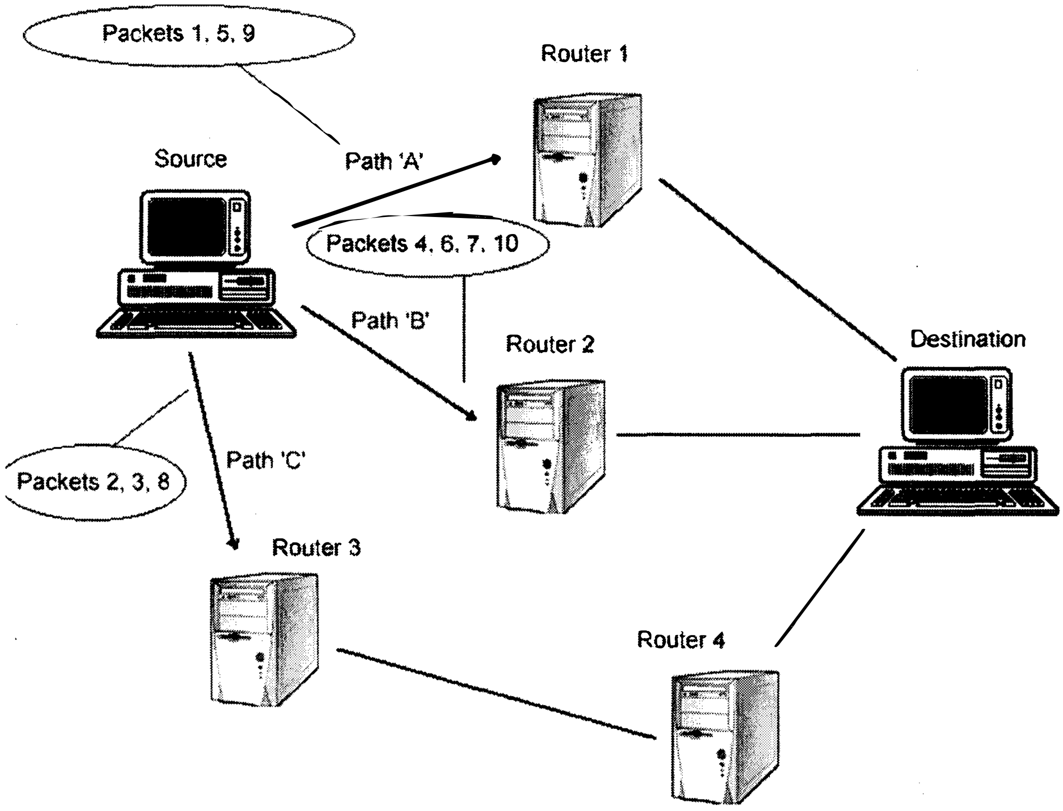

Figure 2-3 Routing packets from source to destination.

Allowing packets to take different routes to their destination presents some problems. Some packets may arrive before others that should be ahead of them in the communication stream; some packets may not arrive at all, perhaps due to a router failure. The TCP component of the Internet communications protocols is designed to cope with these problems. TCP ensures that the packets are properly sequenced at the receiving end, and requests the re-transmission of any missing packets. As already mentioned, the ability to re-route packets provides a robust architecture for the Internet. In the previous example, even if Router 1 malfunctioned, the TCP would detect the missing packets (1, 5, and 9 in this case) and request re-transmission. The missing packets could then be routed via the remaining routers. The addressing format used by the Internet Protocol (IP) is called the dotted decimal notation (Kuo, 1997, p. 57). For example the Edith Cowan University server address on the Internet is 139.230.128.5; the Microsoft Corporation address is 207.46.197.101. These are unique addresses, rather like a postal address. Any packets for these IP addresses will be automatically routed via the Internet to the target destination. However, IP addresses in their raw form are inconvenient for users to remember. Instead meaningful symbolic names such as, cowan.edu.au or microsoft.com are used. The system that performs this name to IP address conversion is called the Domain Name System (DNS).

2.2.2 Domain Name System (DNS)

The DNS is defined in Request For Comments (RFCs) 1034 and 1035 (Goncalves, 1997, p. 40). It is a data query service used on the Internet to translate hostnames into IP addresses. IP addresses are defined in the form WWW.XXX.YYY.ZZZ where each group of Ws, Xs, Ys, and Zs define integer values in the range 0 to 255. The four groups of integers in this range define the size of the IPv4 address scheme, 32-bits. The WWW.XXX.YYY part defines a particular subnet on the Internet. The ZZZ defines a particular host, or computer on the subnet. Another advantage of using a symbolic name structure is that if, for example, ECU wished to change the IP address of the webserver; this may be accomplished in a way that is quite transparent to the user. In fact this situation occurs often on the Internet. These symbolic names are known as domain names.

The DNS is a hierarchical system, and its structure is illustrated in Figure 2-4.

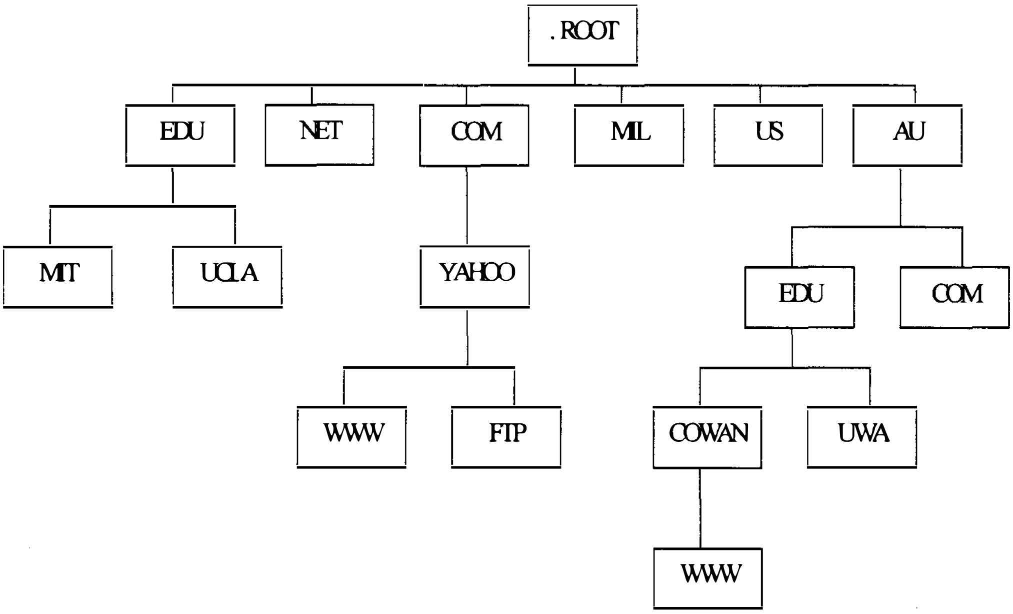

Figure 2-4. Domain name system hierarchy (Note. adapted from Kuo, 1997, p. 58)

The hierarchy is composed of the top-level domains below the root, with sub-domains emanating from these domains. The sub-domains may, in turn, have other sub-domains below them. Database servers within the domains contain information on the IP addresses, and domain names of registered websites. Converting a symbolic name to an IP address usually involves passing the name up the DNS hierarchy chain, until a domain server with an IP address entry corresponding to the domain name is reached.

Country domain designations are intended to identify the country of registration of a website[7]. The use of individual country domain designations such as .AU, .UK etc does not guarantee that the website is hosted within these countries (Australia and the United Kingdom in the example). The geographic location of the website is completely decoupled from the domain name. However, it is apparent that the use of country domain designations helps to promote the popular misconception of Internet domains, which map directly to geographic domains.

2.2.3 Virtual and Non-virtual Websites

The designation of a website depends on how it presents itself for access to the Internet. A *virtual* website is one that is accessed through a domain name, for

[7] Vide InterNIC FAQs http://www.internic.org/faqs/authoritative-dns.html

example, www.mydomain.com. A *non-virtual* site may be of two types, a subdomain name, www.mydomain.somedomain.com, or a subdirectory of a domain, www.somedomain.com/mysite. The choice of virtual or non-virtual domain names makes very little difference to the way the site is administered or maintained (McComb, 1998, p. 11). The use of virtual domain names has become popularised by the rush to establish a 'dot.com' presence on the Internet by many businesses. A virtual domain name allows the establishment of product recognition and also facilitates a high degree of portability of the site.

2.2.4 The User Datagram Protocol

Recall from the earlier discussion of the Transmission Control Protocol (TCP) that the fact that communication stream packets are missing is detected and re-transmission requested. In the case of what are known as *streaming technologies* this protocol is unsuitable. Data streaming is a method used to supply large multimedia files, such as video, via the Internet. Normally, a resource is sent from its source to the destination and when all the packets are retrieved, and properly sequenced, the resource may be activated. For large multimedia files, this may result in long download times before the content may be used. Using streaming technology, the downloaded data is made available as soon as it is retrieved and sequenced. TCP may be used for streaming, but Microsoft (2000) describes the problem:

> "TCP's goal is to maximize the data transfer rate while ensuring overall stability and high throughput of the entire network. To achieve this, using an algorithm called slow start, TCP first sends data at a low data rate, and then gradually increases the rate until the destination reports packet loss. TCP then assumes it has hit the bandwidth limit or network congestion, and returns to sending data at a low data rate, then gradually increases, repeating the process. TCP achieves reliable data transfer by re-transmitting lost packets. However, it cannot ensure that all resent packets will arrive at the client in time to be played in the media stream."
>
> (Microsoft, 2000, Data Delivery)

As a result the protocol used for streaming is usually the *User Datagram Protocol* (UDP). According to Microsoft (2000), UDP is "a fast, lightweight protocol without any re-transmission or data-rate management functionality. This makes UDP an ideal protocol for transmitting real-time audio and video data, which can tolerate some lost packets".

Streaming technology has implications for content control under the *Broadcasting Services Amendment (Online Services Act)* (BSA), so a closer examination is required. Data streaming may be subdivided into two types:

1. Live streaming: - where the data is transmitted as soon as it is produced, rather like live TV or radio broadcasts; and
2. File streaming: - where the data is first stored in a file, and may be transmitted at any time.

In its strictest sense, live streaming produces no vestigial resource at the data destination (not technically true because of temporary data storage called buffering); file streaming always involves a content resource. The following case may help to illustrate the differences and their ramifications for the BSA.

The author was recently engaged by a company that used data streaming to provide online training broadcasts via the Internet. The company based in Western Australia, has a dispersed client base in the Australasian region. Two problems emerged:

1. Live streaming to the dispersed client base presented time zone issues. Clients in New Zealand especially, were disadvantaged with unsuitable broadcast times; and
2. Problems with inadequate data links to clients in rural areas produced unacceptable packet losses, producing seriously degraded media delivery.

The problem was solved by switching from live streaming to file streaming. This required the broadcasts to be recorded and saved to streaming files. This solved the time zone issue, as the files are now available on demand. Switching to file streaming also solved the packet loss problem by using the more reliable TCP protocol instead of UDP. The use of TCP increased the reliability of file download by detecting when packets were missing and requesting re-transmission.

In the context of the BSA, if the content streamed by this company were X-rated, pornographic media, the file-streamed content would be illegal. The live-streamed media would not be defined as 'prohibited content' under the present legislation.

2.2.5 TCP/IP Application Level Services

TCP/IP provides what are known as application level services for applications using the Internet delivery system. Services that use the TCP/IP delivery system include:

- World Wide Web
- Network News
- File Transfer
- Electronic Mail (E-mail)

These are known as application-level services, and use their own protocols that in turn use the Internet protocols for communications. Operations implementing these protocols are *application level* operations. These include such protocols as:

- Hyper Text Transfer Protocol (HTTP): -
  Used by World Wide Web services
- File Transfer Protocol (FTP): -
  Provides file transfer services
- Simple Mail Transfer Protocol (SMTP): -
  E-mail delivery system
- Network News Transfer Protocol (NNTP): -
  A system for the delivery of newsgroups

To enable TCP or UDP to transport different types of application data using the same IP address, each header includes a port number. In this way one Web server can support FTP and HTTP for example. Pfleeger (1996, p.384) points out that in addition to addresses for nodes within a network there are also addresses for particular applications running within a network node. These application addresses represent a unique communications channel number by which two computers may route packets. The application address is known as a *port*, and is defined by Gaskin (1997, p.1427), as "a *software po*rt is the memory address that specifies the transfer point between the microprocessor and a peripheral device". For example, HTTP traffic normally uses port 80. This is the default port number used if a port is not specified. At the port address, a software application known as a *daemon* (Dyson, Kelly-Bootle & Heilborn, 1999, p.569), 'listens' for requests. Another term, s*ocket,* is used to define a network address and a port at that address; "a socket is the network address of an application" (Pfleeger, 1996, p.385).

At the application level, content is retrieved via the Internet, using Universal Resource Locators (URLs). This is the addressing form probably most familiar to Internet users. Kuo (1997, p. 71) describes the anatomy of a URL thus:

method://host.domain[:port]/path/filename.ext

which may be simplified to:

Method://Server name/Path

The components of the URL are:

- **Method**

  The first part of the URL before the colon identifies the protocol to be used for data transfer.

- **Server name**

  This is the second part of the URL, and comes after the two forward slashes. It identifies the server machine in DNS format. It may optionally include a port number.

- **Path**

  The last part of the URL follows the server name. It denotes the location of the target resource. The path follows the UNIX path delimiter syntax, a forward slash (/) (Dyson et al, 1999, p. 861).

For example, the URL for the Edith Cowan University library home page is http://www.cowan.edu.au/library/index.html. This URL specifies that the HTTP protocol is to be used for transferring the target resource, the domain name of the server with access to the resource is www.cowan.edu.au, and the path to follow from the root directory of this machine is library/index.html. This URL will retrieve the file named index.html to the user's browser. Since domain names are resolved to an IP address, it is perfectly acceptable to use the URL: http:// 139.230.128.5 to access the ECU homepage, replacing the domain name with the IP address. This domain name to IP address interchangeability has implications for content control using URLs as it effectively doubles the number of possible paths to a Web resource.

Although websites may use alternative protocols to deliver content, in the context of the adult online industry this study concentrates on the HTTP protocol.

2.2.6 The World Wide Web

It is important to differentiate between the Web and the Internet. The Web is not the Internet. Kuo (1997, p. 4) explains, "the Web is a globally distributed and seamlessly networked information retrieval environment. In this environment all information—text, images, video, and audio—is accessible from the Internet", and reveals, "the Web is a vast collection of interconnected documents and resources, spanning the entire network... they have the effect of a spider web that encompasses the world. Hence the name, World Wide Web". This environment of interconnected Web content uses the Internet as a content delivery system. An Inktomi-NEC study, suggested that by 2000 the Web had come to comprise over 1 billion unique webpages. The number of websites was estimated in the same study at 4,951,247 (Inktomi, 2000). Pastore (2000) cites a Cyveillance study estimating the number of pages added daily at around 7 million. Clearly, the Web is a dynamic environment.

2.2.7 Web Content

As already mentioned Web content may take many forms, with the most prevalent being *Hypertext Markup Language* (HTML) documents. An important distinction must be made between traditionally published documents and Web documents. A Web document or webpage is not a monolithic entity in the same way that a magazine page is. A webpage is usually composed of different, individual components. These components all have their own URLs and are downloaded via the Internet independently. In fact these components, may not reside on the same machine, or in the same geographic location. In fact the document may not exist at all, other than programmatically. For example, the content retrieved by a particular user may be produced by an application in response to parameters supplied by the user's Web browser software. Another user accessing the same webpage may be supplied completely different content. Put another way, it is possible, and probable, that Web content may exist *uniquely* in the context of the user accessing it. This publishing paradigm is quite unlike anything before. We cannot say that a particular document exists at all in the same way that a book or journal article may exist.

This study suggests that websites may be defined in terms of their topology and data topography. The topology is a product of the interaction of the hyper linked document components and the content structure of the site. The topography is defined by the data volumes accessed, and the geographic locations of that data. The ideas of 'data topology' and 'data topography' furnish the locus of this study.

2.2.8 Connecting to the Internet

Most domestic users access the Internet through an ISP using a modem and a telephone line. When connected, their ISP allocates an IP address for Internet traffic. The Web server executes requests to this address from the client browser, and retrieved packets are routed back to the requesting socket, and via the telephone line, to the client's machine.

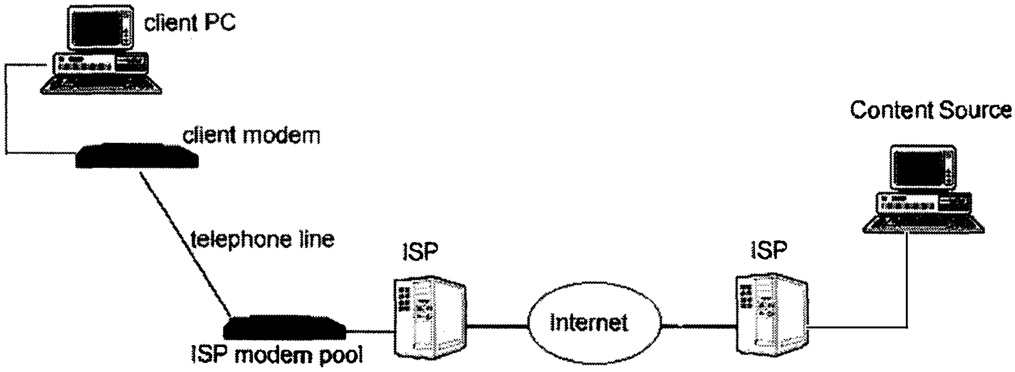

Figure 2-5: Accessing content via an ISP.

It is important to note that although there is a popular misconception that users are somehow 'visiting' websites, the client is only ever connected to their ISP's modem pool. The dynamic content environment enjoyed on the Internet is accomplished by programs executing on the client's machine. In reality the website 'visits' the client.

Some ISPs are now offering connectivity using technologies such as Asymmetrical Digital Subscriber Line (ADSL) (Telstra, 2001[8]). This technology offers increased bandwidth with resulting high-speed download, up to 30 times faster than normal 56Kbps modems. Until this technology is economically accessible, the supply of high-quality multimedia Web content will be restricted in Australia.

[8] Telstra Broadband. Available WWW: http://www.bigpond.com/broadband/

2.2.9 Adult Traffic Volumes

Some estimates of the proportion of Internet traffic devoted to erotic content are as high as seventy percent (70%). Much of the apparent high level of erotica retrieval on the Internet may be explained by an examination of how the HTTP protocol works. HTTP is a stateless protocol, no connection is maintained between hosts; requests are sent, files retrieved and the connection is broken. As an example, to access a webpage, a request is sent to the computer hosting the required file. The browser then examines the composition of the page and if it contains graphic files, a separate connection and request is made to retrieve each graphic on the page. If a webpage consists of an HTML document and ten (10) graphics (GIF, JPEG, etc) the host server will receive eleven (11) requests. This situation is somewhat complicated by caching of webpages on browsers and servers, but as a general rule graphics laden webpages generate multiple requests.

Sex sites are big suppliers and hosts of graphics files. A rudimentary preliminary study of a random sample of fifteen (15) non-erotic websites, in the .com, .net, .gov, and .org domains, revealed an average of slightly more than fourteen (14.26) requests per page. A similar study of fifteen (15) adult websites produced an average of over forty-seven (47.3) requests per page. If we use the non-erotic average as a benchmark, dividing the request level for individual webpages by this figure generates a request index for webpages. Using this method for example, the ECU homepage has an index of 1.89 and Webcrawler.com's front-page index is 0.35. The index range for the non-erotic site sample is 0.07 to 2.24. The index range for the sex sites is 1.05 to 16.48. The average sex site page generates more than three times the request and retrieval traffic of an average webpage. Add to this the fact that graphics files may be large (50 Kbytes is not uncommon) depending on bit depth, size and image resolution and it can be seen that adult sites can generate a very large proportion of Internet traffic. Misconceptions about the nature of adult traffic volumes on the Internet, the technology issues that underlay such volumes and patterns in user behaviour that traffic patterns represent are common in public discourse on content blocking

2.3 Industry Related Literature

2.3.1 The Structure of the Internet Service Provider Industry

McCrea, Smart & Andrew (1998) identify and define the main players in Internet data services in Australia as:

- Backbone Service Providers (BSP)
- Internet Access Providers (IAP)
- Internet Service Providers (ISP)
- Internet Content Hosts (ICH)

A Backbone Service Provider (BSP) is usually a telecommunications company providing connectivity to the international telephone system. In Australia, companies such as Telstra and Optus provide this service. These companies, as well as supplying their own customers, act as 'wholesalers' of access to smaller telecommunications companies, IAPs and ISPs.

An Internet Access Provider (IAP) provides different organisations with access to the Internet only, providing packets of information via the network. It does not provide or have any interest in any other services.

An Internet Service Provider (ISP) provides their customers with the access of an IAP but with additional services such as Web access, e-mail, newsgroups, ftp, etc.

An Internet Content Host (ICH) hosts content that is available on the Internet but does not provide an Internet connection.

The data services industry maintains a hierarchical structure with BSPs providing connectivity to ISPs and the ISPs in turn providing access to smaller ISPs. In addition large ISPs will allow access to their webpage caching systems to smaller operators. The use of these caches is a primary source of the unreliability of Internet statistics. For example, a webpage may be requested by hundreds of clients from multiple ISPs, but the target website will only receive one request for the resource, the other requests being satisfied from the caches of the large ISPs.

As of the end of the June quarter 2001, there were 628 ISPs in Australia; this represents a contraction of six percent in the quarter. This followed a four percent contraction in numbers during the March quarter (ABS, 2001b). This industry is characteristically volatile with larger ISPs competing for market share by buying smaller ISPs.

2.3.2 The Structure and Practices of the Online Adult Content Industry

A preliminary pilot study of the Australian adult content industry revealed that its structure mirrors that of the US adult content industry. Adult websites employ a large amount of both virtual and non-virtual configurations. Adult websites are essentially pay-to-view sites with the content housed behind a security infrastructure. Access to content is only granted after online payment by credit card. Websites selling content of any type must protect their content from unauthorised users. This may be accomplished by methods as simple as placing the content in a blind directory (a directory with no links from another webpage) or by sophisticated access restriction by user authentication using password protection (Garfinkel & Spafford, 1997, pp.275-292).

2.3.2.1 Search engine manipulation

One significant problem for commercial adult websites is advertising their presence on the Web. As indicated earlier, the Web is growing at a rapid pace and the problem of website promotion is being exacerbated by this growth. Some studies (Coopee, 2000) have shown that most users find content on the Web using search engines, and a prominent listing on search engines is vital. With this fact in mind, successful webmasters devote considerable time, and effort to make sure their site features prominently in search engine query results (Glidewell, 2000). This is not a trivial task as the success or failure of a website may depend on a high rating from a search engine. Figure 2-6 shows a segment of the referral log from the Australian registered site Palomino.com.au. The referrer log indicates the website from which the user hyper linked to Palomino.

```
Referrer Report
pages: #reqs: URL
----- ----- ---
http://www.excite.com.au/search.gw?lk=msftau_au&c=web.au&lang=en&start=16&showSummary=true&s=asia
n&perPage=8&next=next&MSNURL=http://www.ninemsn.com.au/&gotoMSN=goto_NineMSN.gif
http://www.anzwers.com.au/cgi-
bin/process_search.pl?pageid=search&firstresult=0&query_type=all+the+words&numperpage=10&result_type=
detailed&query=pantyhose&location=Australia
http://www.alltheweb.com/cgi-bin/search?query=-sex+-gay++young++nudist
http://www.excite.com.au/search.gw?search=sex+thumbnails&look=msftau_au&c=web.au
```

```
http://www.anzwers.com.au/cgi-
bin/process_search.pl?firstresult=10&pageid=search&query_type=all+the+words&numperpage=10&result_type
=detailed&query=young+naked+girls+&search=GO&location=Australia&x=5&y=13
http://www.anzwers.com.au/cgi-
bin/process_search.pl?pageid=search&firstresult=0&query=fucking&location=Australia&query_type=all+the+w
ords&numperpage=100&result_type=detailed&search.x=5&search.y=17
http://www.anzwers.com.au/cgi-
bin/process_search.pl?firstresult=0&pageid=search&location=Australia&query_type=all+the+words&numperpag
e=10&result_type=detailed&query=amatuer+nudes&search.x=16&search.y=17
http://excite.au.netscape.com/search.gw?lk=ncenter_au&c=web.au&lang=en&start=10&showSummary=true&s=
woman+nude&perPage=10&next=next
http://www.anzwers.com.au/cgi-
bin/process_search.pl?firstresult=0&pageid=search&query_type=all+the+words&numperpage=10&result_type=
detailed&location=Australia&query=sample+slut
http://www.anzwers.com.au/cgi-
bin/process_search.pl?pageid=search&firstresult=0&query_type=all+the+words&numperpage=10&result_type=
detailed&query=hot+body&search=GO&location=Australia
http://www.anzwers.com.au/cgi-
bin/process_search.pl?firstresult=0&pageid=search&location=Australia&query_type=all+the+words&numperpag
e=10&result_type=detailed&x=7&y=10&query=tits&search.x=27&search.y=9
http://www.webcrawler.com/cgi-bin/WebQuery?mode=summaries&maxHits=25&searchText=anal+sex
http://www.anzwers.com.au/cgi-
bin/process_search.pl?pageid=search&location=Australia&query_type=all+the+words&numperpage=10&result_
type=detailed&query=australian+women+looking+for+men
http://www.anzwers.com.au/cgi-
bin/process_search.pl?pageid=search&firstresult=0&query_type=all+the+words&numperpage=10&result_type=
detailed&query=black+women&search=GO&location=Australia
http://www.search.freeserve.net/cgi-
bin/pursuit?matchmode=and&mtemp=main.freeserve&etemp=error.freeserve&query=Pleasure+zone&cat=lycos
&x=13&y=13
http://www.anzwers.com.au/cgi-
bin/process_search.pl?firstresult=50&pageid=search&query=mature+women&location=Australia&query_type=a
ll+the+words&numperpage=25&result_type=detailed&x=8&y=11
```

<u>Figure 2-6:</u> Website referrer log (Palomino, 2000)

The log contains the URLs of the sites from which the user was referred to Palomino.com. Also included are any search parameters the user entered in a search text box. The referrer log indicates the sites referring to Palomino and the text entered by the user to generate this referral. Even this small segment of the log indicates the importance of search engines to adult websites.

The number of search engines on the Internet is over 1000 (Kahaner, 2000) with the top sites Altavista, Yahoo, Go.com among the highest profile sites on the Internet. Search engine is a generic term used to describe two web search paradigms:

- *Search Engines*

Genuine search engines use automated searchers called web crawlers or spiders to trawl the Web for information on websites. The information they return is then sorted and categorised by people. Websites are periodically revisited and their profile updated. Any changes in the content will be reflected in search engine database. HotBot and Altavista are examples of true search engines (Sullivan, 2000a); and

- *Directories*

A directory depends on individuals submitting descriptions of their website. The search then tries to match criteria with the submitted descriptions. Changing content in a website will not change the directory rating. Yahoo is an example of a directory (Sullivan, 2000a).

Adult content websites use many techniques to manipulate search engines to gain a prominent position in a query listing. The search algorithms of popular search engines are deduced by submitting multiple pages and studying the success rate for different techniques (Glidewell, 2000, Attack Those Search Engines).

2.3.2.2 Push technology

Push technology facilitates the supply of web content that is not explicitly requested by the user. Prevalent in adult websites is the use of what is known as client-push. Using JavaScript and HTML it is possible to open another webpage completely independent of the user. The implementation is quite simple and the following JavaScript code segment illustrates the point:

```
var flag = 1;
function dontGo(){
   if(flag==1)
       open ("http://www.nextpage_to_visit.com");
}//end function dontGo()
```

and including: - *OnUnload = "dontGo()"* in the script.

This code is activated by the *OnClose* or the *OnUnload* event that is triggered by the closing of the webpage in which the code is embedded. The effect is that when the user attempts to close a webpage, another unrequested webpage is accessed. This method is used extensively in adult content websites, and may be another contributing factor to high adult traffic volumes.

2.3.2.3 Marketing and business models

The marketing strategies employed by adult sites depend heavily on website referral. This is a major contributing factor to the prevalence of two particular type of website:

1. Referrer sites: - usually simply URLs which resolve to the address of the main site or use programming to jump or bridge to a website. They usually contain no content only hyperlinks; and
2. Portal sites: - more sophisticated sites with many hyperlinks to other sites. Usually containing banner ads and some graphics. The more sophisticated are known as Thumbnail Gallery Portals or TGPs that contain thumbnail (very small) versions of content hosted on other larger websites.

For the purpose of this study we will refer to both types as portals, but it is important to note that a referrer site may not exist in the sense of a website that may be accessed in its own right, it might only provide a connection to a main website. These portals then provide referred clients to the larger sites. The larger content rich sites then pay the portal websites for successful referrals that result in a subscription. This marketing strategy is employed extensively in adult websites on the Internet. It is usually implemented in the following way:

- A large adult site in the US offers to supply some content (usually about 200 images) to a smaller portal site, for marketing purposes.
- The portal site uses the supplied images to attract customers and maintains a hyperlink to the main mega site(s). The only content on the portal is the supplied images.
- The large site operator pays a royalty to the portal operator for every referral that results in a membership transaction.

Use of the strategy has resulted in a large percentage of adult websites being mere portals with hyperlinks to many of the large mega sites, with very little content hosted by the portal sites. The literature also describes so-called 'Link-Back' agreements (Glidewell, 2000) that are commonly found in business models. 'Link-Back' works as follows:

- An agreement is made between two large content providers to hyperlink each other's site within client-push JavaScripts.

- When a customer accesses a site, each attempt to leave the site activates a JavaScript to open another of the site's webpages.
- When the website has exhausted all its possible content offerings, it activates the hyperlink to the other website in the link-back agreement.
- The new website follows the same protocol and may eventually link-back to the original referring site.

This kind of business model has two important implications:

1 It maximizes the possibility of making a sale and therefore a profit; and

2 It increases the Internet download volume generated by adult content sites considerably.

In addition to link-back agreements, membership fees enabling authenticated account access are typical. The larger sites charge typically US$20 to US$30 per month for access. Another model is employed by so called "free" sites. These offer free access to content, usually with a limited supply of images. Images are often supplied by large websites in return for banner ads and referral scripts (HotGold, 2000[9]). In some cases these sites are nothing more than pages of hyperlinks and banner ads. The most minimal are mere referrer or 'bridge pages' that use the REFRESH command in the HTML metatags to jump to the main site, earning income from any membership-generating referrals (Sullivan, 2000b).

Cooperatives are also common. For example, Adult Verification System sites charge credit-card holders a flat annual fee for access to sites participating in the cooperative. Participating sites pay a percentage of the membership to the cooperative. In most cases, payment is by credit card only. There are a very small number of operators on the Internet that allow other payment options[10]. The existence of credit card transaction records was considered in this study as an excellent source of data on user download behaviour patterns. If behaviour had changed since the introduction of the BSA, evidence might be found in these transaction records.

[9] A good example of an adult webmaster banner ad registration site at http://www.hotgold.com

[10] For a report on a cashcard for online adult content vide *Web porn: No credit, no problem* available at: http://www.proquest.com/

2.4 Content Control Issues

2.4.1 Filtering

Opponents of online censorship have argued that efficient, affordable content blocking may be impossible on the borderless Internet. Concerned about the cost and usability implications of content blocking, the National Office of the Information Economy commissioned the Commonwealth Scientific and Industrial Research Organisation (CSIRO) Division of Mathematical and Information Sciences in 1998 to report on the feasibility of various technology options. In its report, *Blocking Content on the Internet: a Technical Perspective* (McCrea, Smart & Andrew, 1998), CSIRO outlines the problems of blocking Internet content.

The report found that content blocking could effectively be implemented at two levels:

1. The packet level
2. The application level

Blocking at the packet level involves BSPs and IAPs programming their routers to compare the source addresses of packets with a blacklist of undesirable addresses. If a packet from a blacklisted source is found the packet is blocked and not passed on to the client (McCrea et al, 1998, p. 28).

Blocking at the application level (McCrea et al, 1998), would force the ISPs to provide Internet access through 'clean' proxy servers. The server compares the user requests for access with a blacklist of banned websites and refuses access to such material. The level of capital investment for some ISPs to acquire suitable servers could be significant.

McCrea et al (1998) concluded that content blocking at the packet level was not feasible. It was too indiscriminate; blocking access to complete sites rather than just banned content. It was also concluded that filtering at the application level was problematic. The measures to block content could be easily circumvented and it was far from foolproof. A subsequent report (Greenfield, McCrea & Ran, 1999) concluded that application level filtering using Universal Resource Locator (URL) blacklists, was feasible. The use of application level filtering facilitates the complaint, review and takedown structure of the co-regulatory system. The URL of any website, which becomes the subject of a takedown notice, will be added to the blacklist of all the filtering packages included in Schedule 1 of the Code.

It is unclear what effect the use of filtering technology will have on system performance. The implementation of server-side content control would require the use of proxy servers. Kuo (1997, p. 299) reveals that a proxy server is also known as "An application-level gateway". The proxy server provides access to the Internet with all communication outside the network originating from the proxy server's address rather than the individual client addresses. Some ISPs such as AAPT, mandate the use of a proxy necessitating the configuration of their client's browsers to the proxy setting, others such as iiNet use a more recent development known as a transparent proxy with no configuration required, described in Greenfield, McCrea & Ran (1999, pp. 24-26) and Greenfield (1999, p.6). If an ISP was forced to mandate a proxy, it could generate considerable client support costs caused by users experiencing difficulties configuring their browser software. Another problem could be introduced for software applications that use the Internet with their access URLs defined in their source code, this was outlined by Professor McCrae from the CSIRO in his Senate committee submission (Senate Hansard, 1999d). When using a proxy the requested URL is not sent directly to the web server but is appended to the URL of the proxy server application as a program parameter. For example, consider a client requesting the Edith Cowan University home page at *http://www.cowan.edu.au* using the AAPT proxy at *http://proxy.smartchat.net.au*. The client's browser automatically appends the target URL to the proxy URL as a request parameter resulting in the following URL:

http://proxy.smartchat.net.au?page=http://www.cowan.edu.au

A software application using the ECU URL defined in source code could not access this resource via the proxy unless the software could perform the append process. The author was recently involved in an upgrade of a software application which suffered from this problem resulting in a considerable financial impost on the company concerned.

The use of proxy servers may actually improve some systems. However, the overall effect may be detrimental. It takes time to filter content, compare requests with blacklisted entries, etc. On already overloaded systems this extra overhead may cause problems (Greenfield, 1999, 7-8).

Consider the scenario of a service provider implementing a filtering policy by using a database of blacklisted Universal Resource Locators (URLs). Most commercial software filtering packages using blacklists, maintain a database of well over 100,000 banned URLs (SurfControl, 2001[11]). Any client requests for access to a webpage are checked against the entries in the database and access is granted or refused. Figure 2-7 illustrates the sequence.

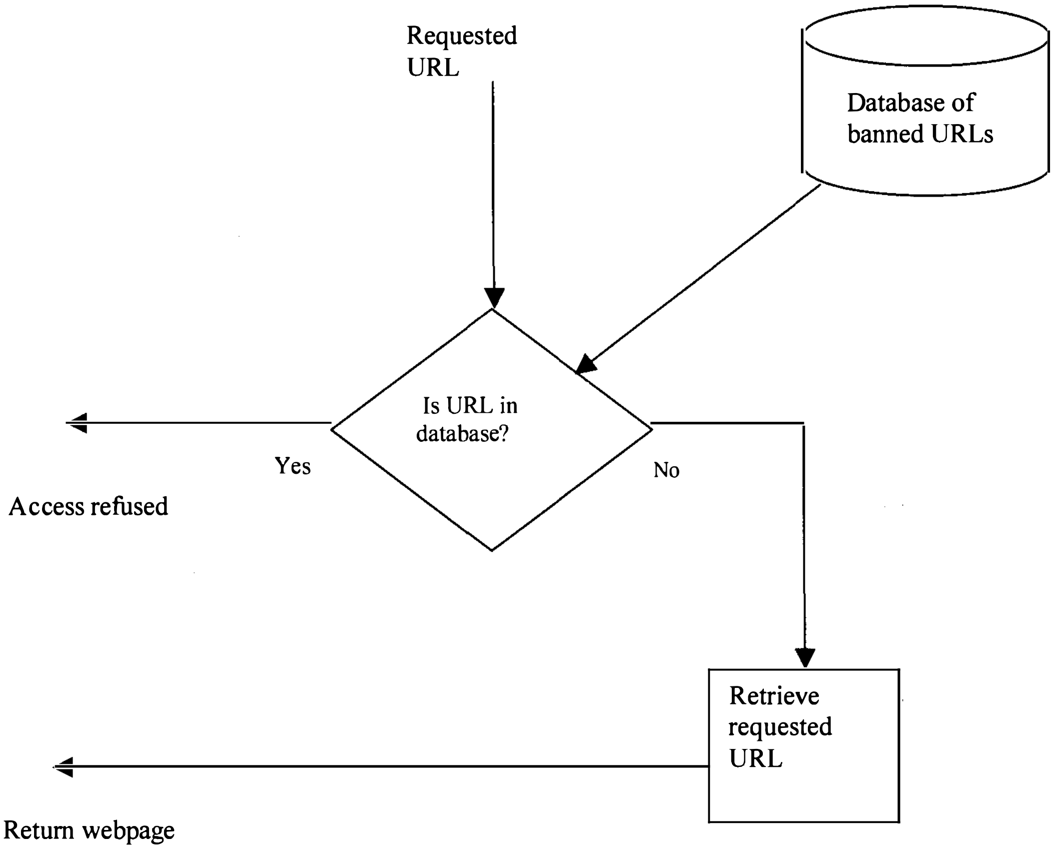

Figure 2-7: URL filtering sequence

A full evaluation of the various methods of content control was examined by Greenfield et al (1999, pp. 18-32), concluding that access control by URL matching did not seriously impact system performance but resulted in large, difficult to

[11] Comprehensive documentation on several SurfControl products is available at http://www.surfcontrol.com/resources/business/index.html

maintain blacklists of URLs. This study proposes a rigorous examination of the topology and data topography of adult websites. A detailed understanding of how their technical models interconnect and their business models inter-react, was needed to reveal the true scope and scale of the content control problem, and the implications for the size of the blacklist required for effective control.

In general however, it seems apparent that the efficiency of any filtering solution will depend greatly on the number of possible illegal URLs. Greenfield (1999, pp. 7-8) explores the possible requirements of a system implementing full Internet content filtering and control, concluding that the system required to adequately filter content would be very technically advanced, possibly not yet in existence. He concluded the system specification would include approximately 120 of the fastest processors then available (350MHz Intel Pentium processors). Even given that the available computing power has increased since 1999 (1GHz plus processors presently), it may also be assumed that the scale of the filtering problem has probably also increased in this time. It is apparent that any system built to incorporate full Internet content control would need to be large, fast and technically highly advanced. Greenfield (1999, p. 7) suggests this extreme specification should ensure that such a system might be also very expensive. What is certain is the fact that a requirement for full filtering would be extremely technically problematic

Many claims are made (SurfControl, 2001; Pearl Software, 1999) for the usefulness of current software solutions, but there is little evidence of how they would cope in the Australian context. Most current software solutions employ blacklists of over 100,000 sites that are updated daily. These blacklists are usually provided in binary files, encrypted for protection. Greenfield et al (1999) outlines evaluations conducted by CSIRO of twenty-two (22) filtering products on behalf of NOIE. As already mentioned ISPs are expected to recommend the use client-based filters to their customers, anecdotal evidence from the ISP industry suggests that the take-up rate has been less than two percent (2%).

2.4.2 The Platform for Internet Content Selection (PICS)

So much emphasis has been placed on regulation, and the use of blocking technology, that a potentially more useful area has been significantly neglected. Resnick and Millar (1996) offers the Platform for Internet Content Selection (PICS) as part of a comprehensive solution to the problem of content filtering. If properly implemented, it could prove very useful. The idea that the producer of the content should really be the responsible party is valid. If the producers properly rated all content on the Internet, the problem of content filtering would be much simplified. Section 9 of the IIA Code of Practice refers to rating technologies, but far more emphasis could be placed in this area.

The PICS technology has the potential to provide a useful solution for all parties including the adult content industry, and combined with other technical solutions, may prove extremely useful. Nachbar (2000) suggests that "The key to efficient and effective government regulation of mature content on the Internet is the use of power-conferring, instead of proscriptive rules" (Nachbar, 2000, p. 214), maintaining that, "PICS divorces the choice of *method* for filtering to the *ratings system* applied to content .... consumers can choose to view content rated under which ever ratings system they think best reflects their values" (Nachbar, 2000, p. 226). Contained in the PICS specification is the requirement to ensure that the contents of a site have not changed since it was labeled. This is achieved by including an encrypted checksum on the contents of the document (W3C, 1999). However, it is possible to alter or remove a label. The effective use of PICS requires the full cooperation of publishers and handlers of rated content. If the publisher of an X-rated sited wanted to give it a G-rating, there would be no means of preventing this. However, it would be a better strategy to try to attract the kind of clientele that wanted to access an X-rated site, PICS makes this possible. With third-party agents rating sites it would be much better to play fair than risk ending up on a blacklist of unrated sites.

One major drawback however, is coping with the different ethical standards of a culturally diverse world, but some form of rating conversion protocols could possibly overcome this. These protocols could be negotiated between governments to facilitate the exchange of rated material e.g. converting an Australian G-rating to an appropriate Indian rating. Many of the current software packages offer the ability to use PICS rating labels.

2.5 Summary

With reference to the literature, this Chapter has elaborated the nature of the co-regulatory regime for Internet content blocking that currently exists in Australia and some of the concerns that underpinned its adoption. It has also provided an introduction to responses to the problem of content management in other nations. Most importantly, with reference to the literature, the Chapter has set down the Internet and technology basics essential to understanding the research design and methods of this study. The structure of the Internet Service Provider (ISP) industry and the adult content industry have been outlined, along with views from the literature of how these might impact on content control regime and its effectiveness. Various filtering technology options were introduced and an alternative solution to content blocking in the form of content ratings explained. Some of the complexity concerning Web content delivery was documented, hopefully dismissing the misconception of websites as islands of content in an Internet ocean, and providing some basic understanding of the dynamic, topologically complex nature of the Web.

CHAPTER THREE

3 RESEARCH METHODS AND DESIGN

3.1 Research Questions and Hypotheses

Concisely, this research addresses the following questions concerning content control in the Australian context, and the impact of the *Broadcasting Services Amendment Act (Online Services)(1999)* (BSA). To reiterate, they were:

1. What is the scope and scale of the content control task in the Australian context?

2. Did content from hosts in the .au domain shift to overseas hosts as a consequence of amendments to the Broadcasting Services Act?

3. Have changes in data topography contributed to the worsening of the 'data deficit'?

4. Can metrics be generated that indicate a change in end-user download behaviour attributable to the new content control regime?

5. What are the financial implications for the Australian ISP industry operating under the co-regulatory system?

6. Are there any implications for the operation of mainstream E-commerce in Australia arising from the introduction of Internet censorship?

The following hypotheses are *tested* in this study:

1. A significant Australian hosted adult content industry existed before the *Broadcasting Services Amendment (Online Services) Act* (Cwlth, 1999) came into effect on January 1, 2000;

2. Before or after January 1, 2000 Australian hosted adult Web sites moved offshore to foreign hosts;

3. Changes in hosting arrangements for Australian adult Web sites have contributed to a data deficit in Internet traffic; and

4. Current content blocking measures are effective in terms of the data topography and topology that characterise adult Web sites.

The following working hypothesis is held true and therefore untested:

Ceteris paribus, trends in data topography involving movement of high volume Australian hosted content to offshore hosting arrangements correspond to an increase in the data deficit.

3.2 Overview of Research Methods

The research method of this study employs multiple methods, forming an example of 'triangulation' (Sarantakos, 1993, pp. 155-156), combining experimental, empirical and naturalistic methods. Data gathering for the empirical study employed survey questionnaires available online, and also used in telephone interviews with the subjects. The purpose of this study was to provide a profile of the adult website operations including hosting arrangements, marketing strategies, and the impact of the BSA on the industry. The naturalistic research component was developed around field interviews undertaken in tandem with the telephone survey. Interviews were used to explain the objectives of the project and to establish its bona fides in the eyes of web site owners. They were also used to gather information, enabling explanation of trends emerging from experimental data. The interview was self consciously developed with the aim of establishing 'trust', a pre-condition for the communication of reliable, usable data on hosting patterns and other responses to the BSA. The experimental part of the study attempted to accurately identify the geographical, topographical (in terms of amount of content per location) and topological factors of Australian erotic websites.

3.3 Research Protocol

Due to issues of privacy and confidentiality, as well as the commercially sensitive nature of the survey data, a protocol on third-party data access, partial responses and disposition was required.

It was decided that no individual or organisation be identified in the thesis, or in any subsequent publication unless authorised in writing by the subject or organisation concerned. It was also decided that partial survey responses (some questions unanswered) and refusal to answer interview questions was acceptable. All survey and interview data will be retained for two years only, and then destroyed.

Development of the protocol was recognized from the outset as important because reliability of data had the potential to be affected by:

- Privacy Issues[12]
- Disclosure of commercially sensitive information
- Political bias

System operators have an obligation to protect the privacy of their clients and comply with the *National Privacy Principles for the Fair Handling of Personal Information*[13]. The Internet Content Providers (ICPs) are Australian registered companies and are held responsible in this regard, even though, because of the nature of their business, client complaints may be less forthcoming.

The disclosure of commercially confidential information was a major issue for the study. For example, because Internet Content Providers (ICPs) advertise their access charges, the size of their client base could be used to accurately calculate their income from online services. This was a major issue with regard to the ICPs

The political issue was one that was identified as significantly problematic with regard to data reliability. The issue of cyber censorship can be a highly

[12] Current Australian legislation and information relating to privacy and IT issues may be found at: http://www.privacy.gov.au/issues/index.html

[13] Available online at: http://www.privacy.gov.au/publications/npps01.html

emotionally charged one, and when coupled with possible financial ramifications for operators, the research design had to account for this. Subjects biasing their responses to support their side in the debate could lead to errors of misattribution. For this reason it was decided to ensure the veracity of responses by gathering detailed information on the ICP subjects to build a profile on them prior to contact for data gathering.

3.4 Research Design

3.4.1 Methods for Empirical Evaluation of the Impacts of the BSA

3.4.1.1 Measuring adult traffic trends: Volume and topography

It was expected that if the BSA was to have an impact, that a discernable change in user download behaviour should ensue. What methods might be used to measure such a change? The following methods were identified in early discussion:

1. ISP server logs could be analysed to detect any change. Since the server logs contain information relating to website traffic, an examination of the log could reveal changes in retrieval patterns following the introduction of the BSA.
2. Gross revenues from credit card transactions could be analysed. All financial transactions within Australia, with adult websites are conducted using credit cards. The credit card records of adult website operators are an excellent indicator to user behaviour. A change in download behaviour from clients within the .au domain can easily be measured by a corresponding change in credit card revenue from Australian clients. However, because of the privacy issues involved, it was envisaged that raw data would probably not be forthcoming and the study would rely on information supplied by the operators' own analysis of their client data.

It was recognized that the gathering of reliable data for the purposes of user traffic analysis using either or both of these methods would require extensive industry cooperation, that might not be forthcoming for reasons of privacy and commercial confidentiality. It was resolved to 'test the waters' of possible levels of industry cooperation by:

1. designing and deploying a pilot instrument aimed at measuring costs associated with introduction of the BSA (thought not to involve significant issues of privacy and confidentiality); and
2. entering into negotiations with an ISP sympathetic to the project to determine the scope for server log file access and analysis.

3.4.1.2 Pilot study: Cost and bandwidth modeling

The pilot study on ISP cost and bandwidth utilization was operationalised as an online survey mounted in conjunction with ECUbit 2000, a conference on online censorship law conducted by the *School of Computer and Information Science* of Edith Cowan University, and made available at (http://www.scis.ecu.edu.au/ecubit/datcol.htm). It was hoped the data from this survey would prove useful in quantifying ISP and client costs as well as the extent of takedown requests. The ISP survey was a three-part survey to measure: -

1. Fixed compliance costs (hardware, software) incurred.
2. Variable compliance costs (administration, filtering, outsourcing, bandwidth related) incurred.
3. Extent of takedown compliance requests.

3.4.1.3 Pilot study outcomes and implications for methods

About three hundred (300) ISPs were contacted by telephone and e-mail, but despite repeated requests, only one (1) ISP responded to the survey. At the same time a major Perth ISP was approached to supply log data, and while unwilling to allow any examination of their logs for privacy reasons, they agreed to supply the results of specific queries on their logs. This cooperation did not eventuate and no data was supplied by any ISP.

Internet Service Provider Industry non-cooperation was a feature of this study, therefore this component was abandoned.

Failure of the pilot study to elicit cooperation from Internet Service Providers, suggested a revised approach to methods and design would be required or the proposed research would have to be abandoned. Investigations revealed that *content providers* might provide an alternative source of quality data.

As discussed, changes in gross ICP revenues from credit transactions might be used as a nominal index of user reaction to the regime. Early in the study, the ICP industry peak body, The Eros Foundation, was contacted and made aware of the aims of the research. Over a six-month period a rapport was established, leading to favourable introductions to industry insiders. This opportunity led to a revised methodology and design.

3.4.1.4 Revised methodology and design

As a consequence of the review the following revised instruments reproduced in Appendices A and B were adopted:

- A content provider survey; and
- A content provider interview script

Non-cooperation from Internet Service Providers also required re-evaluation of experimental methods and in particular abandonment of bandwidth measurement based on changes in ISP traffic patterns contained in data sourced directly from ISPs. Revised methods utilized techniques in data topology and topography. The nature, modus operandi and limitations are discussed in section 3.4.2 in the Chapter.

3.4.1.5 Research design: The Content Provider (ICP) survey

The ICP survey[14] was three-part survey comprising: -

I. A participant profile- used to gather information on independent variables such as number of employees, size of subscriber base etc. Most importantly information on changes in user download behaviour was sought.
II. A Technology profile- used to gather information on the technical aspects of an ICP's websites including their hosting configuration, services provided and future technological changes to their sites; and
III. A financial profile- used to gather information on the costs associated with running their websites in particular information on their hosting charges and bandwidth data allowances.

This survey of Internet content providers was conducted by telephone. The original design used an e-mailed survey, but the response was so poor that it was decided that direct contact by telephone might improve the response rate. This approach was proved correct.

[14] Vide Appendix A

The technology profile (Part II) was designed to reveal impending development in technology employed within the industry. For instance, a large-scale shift towards the use of streaming media technology would have implications for the operation of the BSA. As outlined in chapter two[15], much streaming media is regarded as a 'broadcast' technology and is not covered under the Act, which would leave large amounts of content outside the purview of the content control regime. The use of cutting-edge technology is a feature of adult websites. The technological direction these sites take is often a pointer to where the mainstream e-commerce industry should move. The technology profile could be used to assess the usefulness of emerging technologies for conducting e-commerce in general.

The financial profile (Part III) was used to estimate ISP revenue lost to offshore hosts as well as providing an indicator of the comparative costs of Australian versus offshore hosting arrangements. Anecdotal evidence suggested that Australian hosting could cost twenty (20) to thirty (30) times more than hosting in the United States. Accurate information in this category would be useful for gauging the economics of Australian e-commerce generally.

3.4.1.6 Research design: Operationalising content control effectiveness

For reasons outlined in Chapter One[16], measurement of the *effectiveness* of ABA operations under the BSA was extremely problematic. As already mentioned, the participant profile (Part I) attempted to identify changes in user retrieval patterns that may be attributable to the new legal framework. It was expected that any impact of the new regime should be apparent to the Adult content providers in the form of changes to credit card transaction income from Australian sources. This provided an opportunity to operationalise *effectiveness* in terms of this indicator.

3.4.1.7 Research design: The Content Provider (ICP) interview

Fieldwork comprising scripted interviews[17] with data subjects was undertaken in conjunction with the survey. Questions invited ICPs to elaborate on the structure of the Australian Adult content provider industry, in particular its:

- Geographical structure: - identifying the geographic locations of their websites, and their reasons for hosting at these locations;

[15] Chapter 2, Section 2.2.4 *The User Datagram Protocol*
[16] Chapter 1, Section 1.1.2 *Regulation and control*
[17] Vide Appendix B

- Topographical structure: - revealing levels of content hosted at the identified geographic locations, and levels of outgoing download traffic. This data was used to provide a data profile for adult websites; and
- Topological structure: - indicating how the website is interconnected within the adult content industry. An interaction of the content topology (large numbers of URLs per page), and the contrived industry topology generated by website link back agreements produces an extremely convoluted Web topology. This topology has implications for URL filtering and the effective conduct of content control under the BSA as it gives the industry a robust topology, rather like the Internet itself, providing many alternate routes to content.

The interview also explored industry attitudes to content control in the context of the BSA, marketing issues and the future directions of the industry.

3.4.2 Experimental Design

The experimental component of the study had to be in place prior to the introduction of the BSA in January 2000. It was necessary to find which websites were in Australia before commencement of operations by the ABA in order to track the effects of the regime on hosting arrangements. This was vital to avoid errors of misattribution. This study commenced in the final quarter of 1999.

The experimental study has two main objectives. Namely, to:

1. Identify the site ownership, company details and contact information; and
2. Construct site typologies based on their topography (where they are hosted) and their topologies (their file, directory structure, and content hyperlinks).

As discussed, ICPs are well positioned to describe the impact of the new content regulation. For example, if the BSA had been responsible for a change in user behaviour involving, for example a reduction in online download activity or site subscription, then ICPs would experience this in terms of a reduction in gross income from credit card transactions. Since ICPs are also billed by ISPs for bandwidth used, they could also be expected to report on changes in traffic patterns.

The experimental design had to account for the fact that an Internet search for erotic content originating within the .au domain will locate hundreds of sites and web pages. An added complication arises where one individual owns several websites. It was discovered that reducing the URLs to the root website and identifying the registered owners of the websites using the InterNic domain name registry (available http://www.internic.net/), site owners could be reliably identified. It is interesting to note that most operators were unaware that their details were available so freely, and expressed surprise at how easily they were identified.

3.4.2.1 Geographical domain mapping: Defining Australian adult Web content

Any study intended to measure the impact of a national online censorship regime will sooner or later face definitional issues concerning the 'borderless' Internet. What exactly is an Australian Adult Web site? For the purposes of this study, Australian websites were defined as those sites hosted on Australian Content Hosts (ICHs) or registered with the AUSNIC Internet registry, carrying the .AU domain designation, and owned by Australian registered companies. It must be pointed out that there may be many other websites owned, and operated by Australians that are registered offshore with other registries, but it would be impossible to identify these sites. This represents an acknowledged limitation of the experimental component of this study.

3.4.2.2 Site typology: Data topography and topology

Important research questions for this study concern:

*whether the BSA initiated a change in Web hosting arrangements involving an exodus of adult content from Australian Web servers to offshore servers; and

*secondly, if such a changed existed, what were its implications for Australia's so-called 'data deficit'.

An untested working hypothesis was also adopted, namely, that:

Ceteris paribus, trends in data topography involving movement of high volume Australian hosted content to offshore hosting arrangements correspond to an increase in the data deficit. The technique of data topography was used to answer these questions.

Data topography can be thought of as an exercise in geographical domain mapping. Geographical domain mapping describes the physical location of hosted content. For the reasons already discussed[18], the decoupling of geographic location and Internet domain means the domain names can be misleading as an indicator of content location, and these names cannot be used reliably to determine the place of content hosting.

Anecdotal evidence from the ICP community had shown, that in many cases Australian adult websites hosted within the .AU domain, are merely portal sites to offshore content. It was vital that the geographic locations of Australian adult content be identified and the amount of content at these locations quantified.

The data typography study used two software applications:

1. ***NeoTrace***

   NeoTrace (available http://www.neoworx.com/) is a packet-tracking application. It is a sophisticated version of the UNIX Traceroute program (Feit, 1996, p. 142). As in Traceroute the path to a particular website is mapped by identifying the routers used to route the packets from source to destination addresses. In the NeoTrace program, the geographic locations of these routers are stored in a database of known backbone and service provider servers. This information may then be used to map websites to geographic location. As was pointed out earlier, there is no direct mapping of cyberspace to geographic space, and the domain name of a website does not guarantee its location within a country's geographic domain. The NeoTrace application projects the packet routes onto a global map, precisely identifying the location of a website, and the path taken to reach it.

2. ***SiteMapper***

   This application (available http://www.trellian.com/mapper/) automates the process of identifying the topology and data topography of websites. It scans the site file structure, following the entry and exit hyperlinks to reveal the topology. The topography is identified by classifying and quantifying the content found in the site. This application is used to reveal how a website is connected to the global Internet, what it contains and how much content there is at a particular location.

[18] Chapter 2, Section 2.2.2 *Domain Name System (DNS)*

An area of experimental uncertainty exists with the use of such software applications. In particular the use of NeoTrace assumes that the application's router database is sufficiently accurate. This uncertainty was alleviated somewhat by checking the accuracy of the software by tracking websites of known location and comparing the router information with that provided by the Traceroute application. As it was only necessary to track a website to within a jurisdictional boundary (Australia, US, UK, etc), it is assumed that the geographic granularity of the application is sufficiently accurate.

3.5 The Experimental Sample

The experimental sample consisted of all the owners of erotic content websites registered in Australia. An Internet search for erotic content originating within the .au domain will locate hundreds of sites and web pages. An added complication arises where one individual owns several websites. As already mentioned, using the InterNic registry twenty three (23) individuals were identified. It was envisaged that the secretive nature of these subjects may lead to the adoption of what Sarantakos (1993, pp.139-140) refers to as 'snowball sampling' if the initial response rate was poor, with respondents perhaps identifying other target subjects. It was hoped that the use of 'snowball sampling" would ensure that the sample was a large proportion of the target population.

3.6 Reliability

Acknowledged limitations in the study arise from several factors, including:

- Issues of confidentiality and privacy for content providers affecting the nature and extent of data gathering. In particular relying on the website operators' analysis of their raw credit card transaction data;
- Content provider reluctance to provide information that might be used to estimate income. (Since these operators advertise their up-front fees, any information on the size of their subscriber base could be used to calculate an estimated income.); and
- Political bias introduced by individuals using the study to promote their own agenda with regard to Internet censorship.

Triangulation (Sarantakos, 1993, pp. 155-156), combining experimental, empirical and naturalistic methods, enabled findings arrived at with one method (e.g. fieldwork) to be compared against findings in relation to the same matter achieved with another (e.g. experimental). In this way, the reliability of the study was improved in the light of sample size and other issues affecting reliability.

3.7 Summary

This chapter reiterated the research questions and the working hypotheses. It presented an overview of the research methods employed in the study and the research protocol was described. The initial pilot study was outlined with some discussion of the problems encountered leading to a revised design and methodology. The revised design and methodology was detailed. The experimental sample was defined and finally the reliability and limitations arising in the study were discussed.

CHAPTER FOUR

4 DATA ANALYSIS AND FINDINGS

4.1 Research findings on the Australian Adult Industry

4.1.1 Extent of Australian Registered Adult Content: Discrete URLs

Substantive research began in last quarter 1999, i.e. a full three months before implementation of the Broadcasting Services Act Online Services Amendment Act was promulgated on 1 January 2000. A variety of search engines (GoEureka, Anzwers, Yahoo, Altavista) were used to identify Australian adult content. All searching was confined to the .au domain. It is important to point out that this restriction in no way confines the search to the Australian geographic domain. Searching resulted in an average of about fifteen hundred (1500) response hits. It must be pointed out that this figure is quite dynamic due to the nature of the Internet and the content provided. Repeated tests using different search engines revealed variability in this figure of about thirty percent (30%).

These results required considerable refining and sorting to remove multiple page hits from the same website and discontinued links. This yielded a total of eight hundred and ten (810) discrete search engine hits. This figure was further processed to yield the URLs of discrete websites whose owners could be traced using the Internet registries. The final total of discrete website URLs was two hundred and fifty five (255).

Using the NeoTrace application, each URL was tracked to its geographic location. The IP addresses were collected for cross matching of websites and owners. The websites were categorised as virtual or non-virtual.

The Sitemapper application was used to identify the amount and type of content housed in the public areas of the website this information was used to classify the type of content hosted applying the OFLC classification guidelines

(OFLC, 2001). The sites were categorised as main, portal or referrer sites based on the structure of the site.

All of the information gathered on the websites was stored in a database for SQL query analysis, cross-matching URLs, IP addresses and Internet registry data, that enabled the original fifteen hundred search hits to be directly traced to only twenty three adult website operators with the geographic locations and types of sites clearly identified.

4.1.2 Case Studies in Topology

4.1.2.1 Bridging (referrer) site

Case study showed that referrer or bridging pages are extremely common. The simplest implementation found consisted of a single webpage with a target website in the REFRESH command embedded in a HTML metatag. The individual owning this page had several others of this type pointing to different adult sites, all in the US. This individual had hyperlinks to several third-party referral statistics sites allowing access to check income for successful referrals. Referrals resulting in subscriptions attract commission earnings for the page owner. The results of the topology study for all .au sites are summarized in Table 4-1.

Table 4-1

Breakdown of Website Topologies for All .AU Sites Found in the Study.

Topology	Number	Percentage of total
Referrer (bridging)	192	75.29%
Portal	40	15.58%
Main sites	23	9.01%
Total resolved (discrete) URLs	255	

The data presented in Table 4-1 indicates the prevalence of referrer and portal sites; these two categories comprise over ninety (90.99) percent of all the sites found.

4.1.2.2 Search engine spoofs

One website mapped using Sitemapper was found to contain two hundred and three (203) pages containing nothing but keywords (e.g. catalog asian bondage, free pics black women bondage rape, nude black women etc.). Analysis revealed over eleven thousand (11,000) keywords per page. This represents a considerable effort to attract search engine hits. Again it was found that this site was a portal to adult sites in the US. However, this is an exceptional case, no other website was found that used keyword seeding to this extent, with a random sample of twenty five (25) sites showing an average of slightly more than twenty two (22.25) keywords per page.

4.1.2.3 Virtual .au domains

An interesting case study finding was that of an operator who had organised six (6) virtual domain names, all using the .au domain designation. This was the most sophisticated arrangement found. All of these domains resolved to one IP address of a server in the US. The six domain names were further subdivided into one hundred and sixty four (164) subdomains and subdirectories again all pointed at the server in the US. Given that each subdomain contained over twenty (20) .html pages, this amounts to a large amount of web content. It must be emphasised that all of this content exists outside of any security infrastructure and may comprise only a small fraction of the total content involved. Extensive use of Common Gateway Interface (CGI) and JavaScript programming was used to implement this structure.

This individual is extremely successful in manipulating search engine query results, obtaining prominent positions for his website. The sophisticated nature of this site, its extreme topology in terms of the number of incoming and outgoing hyperlinks and its geographic location would make it extremely difficult if not impossible for the present control regime to have any effect at all on this website.

4.1.2.4 Finding: Extent of adult content hosted within the .au domain

In this study of over fifteen hundred (1500) search engine response hits, not one commercial website hosting significant levels of adult content was located within Australia. Most of the content found was usually that provided by the large US hosted commercial sites in return for referrals. As Table 4-2 shows two hundred and nineteen (219) of the two hundred and fifty five (255) websites are hosted in the US with almost ninety percent (89.49%) configured as portal or referrer sites. For content hosted in Australia, Table 4-3 indicates that no commercial adult website was found, and all (100%) the sites were portal or referrer sites.

Table 4-2

Breakdown of Website Topologies for US Hosted .AU Sites

Topology	Number	Percentage of total
Referrer (bridging)	167	76.25%
Portal	29	13.24%
Main sites	23	10.50%
Total resolved URLs	219	

Table 4-3

Breakdown of Website Topologies for Australian Hosted .AU Sites

Topology	Number	Percentage of total
Referrer (bridging)	24	66.66%
Portal	12	33.33%
Main sites	0	0%
Total resolved URLs	36	

4.1.2.5 Finding: Content classifications and pedophile sites

Websites were examined to determine the nature and extent of content. The OFLC classification guidelines were used to categorise the content (OFLC, 2001). Table 4-4 summarises the key findings:

Table 4-4

Classification of Content Found Using OFLC Classification Guidelines

OFLC Classification	Number	Percentage of total
X-rated	174	68.23%
RC (pedophile, etc)	0	0%
Other	81	31.76%
Total resolved URLs	255	

Much publicity surrounds the use of the Web for pedophile activity. The protection of minors from unsuitable content and the activities of pedophiles is ostensibly the raison d'être for the BSA (BSA, Section 3). During the course of this study, no pedophile sites were encountered, and no RC content of any kind was found on .au-registered websites. Of the X-rated sites, one hundred and sixty four

(164) of these were created programmatically by having the URLs resolve to the same IP address using webpage redirection scripts. The sites in the 'other' category were simple hyperlink referrer-type sites with no images or sites with R-rated content.

4.1.2.6 Findings: Site topology and topography

Based on the .AU domain, as of last quarter 1999, Table 4-5 shows the hosting locations of the websites. The .AU websites were predominantly located in the United States.

Table 4-5

Website Locations

Host Location	Number	Percentage of Total Sites
United States	219	85.49%
Australia	36	14.11%
Total resolved URLs	255	

Of the thirty-six (36) sites hosted in Australia, seventeen (17) or 47% were hosted on Ozemail servers.

The use of non-virtual configurations is highly prevalent to maximize search engine listings. Table 4-6 shows ten (10) times as many non-virtual than virtual sites.

Table 4-6

Domain Types: Virtual and Non-virtual

Domain Type	Number	Percentage of Total Sites
Virtual	23	9.01%
Non-virtual	232	90.98%
Total resolved URLs	255	

All of the commercial sites identified use third-party credit card validation services, again hosted in the US. There is virtually no content apart from images used for marketing, website referral, and site promotion, hosted on Australian servers. The actual content for sale is hosted on, mainly US servers.

4.1.3 The Internet Content Provider (ICP) Survey and Interview

The Internet Content Provider (ICP) surveys and interviews took place in January 2001, a full year after the introduction of the control regime. This was primarily to allow any impact of the BSA on adult website operations to become apparent, but also because it took over six months to establish the bona fides of the study within the industry. The survey and interviews were conducted by telephone, and the subjects were supplied with the Statement of Disclosure[19] by e-mail or facsimile.

4.1.3.1 Participation rate

A target population of twenty three (23) operators was identified in the experimental study. It is important to reiterate that this figure only represents owners of Australian registered websites operating within the .AU domain. There may be many Australians operating websites registered in other domains but they would be impossible to identify. The 'snowball' sampling method outlined in the *Research method and design* chapter was unsuccessful, with none of the respondents willing to identify others within their industry.

Of the 23 identified:

- Six (6) participated, representing over 26% of the target population.
- Six (6) were not accessible having supplied bogus registration details to the registry.
- Two (2) were no longer involved in the industry.
- Nine (9) declined to participate.

4.1.3.2 Participant profile results

The responses to questions in the *Participant profile* section of the survey revealed:

- The total number of Australians employed was 19.
- Six (6) operators (100%) reported no change in user download behaviour by Australian subscribers.

[19] Vide Appendix C to this document

- One (1) respondent further qualified user download behaviour as unchanged but still rising.
- Only (1) operator was willing to reveal the size of his subscriber base at about 100 subscribers. This was the smallest operation in terms of reported traffic volume, and based on average industry subscription charges, would produce a monthly income of about US$3000.
- Two (2) operators claimed to have moved offshore because of restrictions imposed by the BSA. However, the experimental website tracking during the last quarter of 1999, revealed that their websites were already offshore before the introduction of the BSA.
- Five (5) respondents were familiar with the BSA, and its implications for their industry. One (1) operator claimed no knowledge of the BSA at all.

4.1.3.3 Hosting arrangements results

The responses to the questions in the *Hosting arrangements* survey section revealed:

- Two (2) (33%) operators had previously hosted in Australia. The operators with Australian hosting experience reported a hosting charge level in the US at between 50% and 25% of Australian hosting charges. However, the difference in outgoing volume charges was substantial with one operator claiming his Australian volume costs were over 27 times more than in the US.
- All six (6) (100%) operators hosted in North America, five (5) in the US, and one (1) in Canada.
- Five (5) operators had their own servers in US ISP server farms; one (1) operator used ISP disk space.

4.1.3.4 Technology results

The responses to the *Technology* section of the survey revealed:

- Four (4) operators supply streaming media at present, the remaining two (2) intend to implement this technology soon.
- Three (3) (50%) operators suggested the broadband cable market in the US as a potential market for their business.

4.1.3.5 Internet Content Provider interviews

The ICP interviews were loosely scripted[20] using bullet points to provide a flexible topic framework for discussion. An 'unstandardised' and 'open' interview type as defined by Sarantakos (1993, pp. 179-181) was adopted. The use of open questions, asking the respondents to comment on the topic rather than precise questions, helped to reduce interviewer bias. The interview explored three (3) main areas:

- Industry structure
- Attitudes to content control
- Future directions

None of the respondents was willing to be audio taped, and the interviewer recorded their responses using keywords below the topic headings, updating the notes immediately after the interview.

Internet Content Provider interview: Summary findings on topography and site hosting

The following is a summary of findings from interview regarding topography and site hosting arrangements.

- The Australian adult content industry is based predominantly in North America.
- The geographic location of the sites is primarily determined by hosting costs. In particular, high volume charges make it economically infeasible to operate a commercial adult content website in Australia. The cost of hosting in the US was one quarter (25%) to one half (50%) of the cost in Australia. However the volume charges were significantly higher, with one respondent with Australian hosting experience claiming that his volume charges were one hundred and ninety dollars (A$190) per Gigabyte in Australia and seven dollars (US$7) per Gigabyte in the US. Another consideration was the collocation of the dominant US pornography industry as a source of content.
- The adoption of the .au Australian domain designation is merely a marketing ploy. It was explained that because many consumers are concerned about divulging credit card details on the Internet, the .au designation presents the illusion of dealing with a locally based Australian company.

[20] Vide Appendix B

- Revenue from Australian sources makes up a very small proportion of Australian ICP income. One respondent gave the following breakdown of his subscriber base locations:
    - 87% from the US
    - 7% from the UK
    - 2% from Japan
    - 4% from the remaining global market with France at the top of this list.

  This respondent suggested, "Australia doesn't figure in the global market".
- Adult sites generate large traffic volumes. One (1) operator interviewed at approximately 3:00pm AEST revealed that the outgoing volume from his website was already over ten (10) Gigabytes for that day alone.

Internet Content Provider interview: Summary findings on content control and the ABA

Interviewees were not significantly concerned by the BSA and attempts by the Australian Government to block objectionable content. The following is a summary of findings regarding content control.

- The adult content industry is not concerned with censorship in Australia but is very concerned with similar moves in the US. The operator hosting in Canada claimed this was his motivation for locating there.
- None of the operators thought that ABA operations under the BSA could be effective. Their rationale being that even if all of the portal sites were removed from Australian hosts, the content is untouched and remains available by other avenues.
- The consensus was that no content control regime could be effective against their industry. One interviewee suggested that even if restrictions became draconian, that encryption techniques such as Virtual Private Networks and tunneling could be used to circumvent content blocking. This echoed a statement made by a content provider in an unsolicited e-mail, he suggested "the pornographic downloads of the future will simply become encrypted – people will develop plug-ins to encrypt porno images in real time an decrypt them in the computer's browser, and the packets intercepted by the

authorities would be useless as they couldn't decipher them." (Name withheld, personal communication, January 18, 2000).

- Most operators thought content control would be best implemented using industry cooperation; they did not want minors accessing their websites, but thought parental control rather than industry control was needed.
- Australian ICPs are more concerned about the operations of the Australian Tax Office than the Australian Broadcasting Authority.
- When asked if he would be willing to host in a special 'adults only' domain to make access restriction easier, one operator revealed that he had devoted considerable time and effort setting up his site topology to maximize search engine hits. He argued that if restricted to a special domain, he could not compete with the large US operations.

Internet Content Provider interview results: Future directions

Operators were asked for their opinions on where the future of their industry lay with a particular interest in new media and marketing strategies. Their views revealed:

- Most operators saw the future of their industry in the broadband cable market in the US, supplying video on demand and interactive adult content.
- All operators were optimistic that their industry would continue to grow, but two (2) were apprehensive about the intentions of the Bush administration in the US, with one (1) operator locating in Canada because of these fears. It was possible to check the veracity of this claim with reference to the database of URLs[21]; it was found that he had indeed moved from a US host to a Canadian host.

[21] 4.1.1 Extent of Australian Registered Adult Content: Discrete URLs

4.2 Summary

This chapter presented the study's findings on the Australian online adult industry. Three (3) case studies were introduced to elaborate on the range of site typologies found. The results of the experimental study were tabulated and examined. Finally the results of the Internet Content Provider (ICP) survey and interview were summarized.

CHAPTER FIVE

5 CONCLUSIONS

In Chapter Four, data analysis was undertaken and key research finding were revealed. This Chapter concludes this discussion, discusses limitations of the work undertaken and explores some areas for future research. The findings of this study will be discussed in the context of the research questions and specific hypotheses. Each of the questions and hypotheses will be addressed. The limitations of the study are discussed and future research areas explored.

5.1 Undoing the Gordian Knot: The Scope and Scale of the Content Control Task in the Australian Context

The scale of the content control problem has already been suggested by Greenfield (1999) and Buskin (2000). This study suggests that the task might be complicated by the topology of the adult websites. The results of the topology study suggest that adult websites to have an extreme topology when compared to mainstream e-commerce websites. In particular, 'link-back' agreements and search engine manipulation have produced a very robust architecture that greatly amplifies the problem of content blocking. It results in larger numbers of pathways to content, and even if one URL is blocked there are many other avenues to access it. This structure is reminiscent of the structure of the Internet itself; as long as one access route remains the content is unaffected and accessible.

The sophisticated use of search engine manipulation has another consequence. As discussed, many search engines employ automated software systems (crawlers or spiders) (Sullivan, 2000a) to track websites for inclusion in their databases. The intensive attention to attracting search engine hits has effectively supplied the adult sites with an automated website promotional tool. Search engines are working round the clock adding URLs to their listings and the adult sites use this technology to proliferate URLs thereby ensuring additional pathways to content. If filtering technology is to keep pace with this growth of URLs it might be achieved by similarly automating the creation of the URL blacklists. At present most filtering software vendors claim to use manual classification of websites (SurfControl, 2001; NetNanny, 2001[22]). Given manual processes, it is obvious that filtering blacklists will always have problems with currency and comprehensiveness. A move to automated classification listing by filter manufacturers will require the use of keyword filtering with all the inherent consequences of this approach. The inadequacies of keyword filtering technology is well documented (EPIC, 1997; Simms, 1998; Wallace, 1997), leading to often indiscriminate and inaccurate website blocking.

In the context of the BSA, and in particular ABA operations, the study suggests that the regime will probably be ineffective. Despite ABA claims of success in removing adult websites, in the absence of ABA raw data, this study suggests that any URLs blocked will probably leave the content untouched and available by other routes. One case study shows an operator with one hundred and seventy access URLs to his main website with unknown numbers via 'link-back' URLs. Clearly, the topological structure of this *one* website renders it extremely difficult to block; every access URL would need to be found and blocked. If we consider these facts in the context of the size of the industry itself, put at two hundred thousand (200,000) websites (Buskin, 2000), we have a window into the *true* enormity of the content blocking task with millions of pages of content to control.

5.2 Exodus: Did Content from Hosts in the .au Domain Shift to Overseas Hosts as a Consequence of Amendments to the Broadcasting Services Act?

The 'triangulation' of data from the experimental study and the fieldwork study were used to address this question. As outlined, the topography study commenced in the final quarter of 1999, months before the implementation of the BSA. In this study of over fifteen hundred (1500) adult website URLs not one commercial adult website hosted in Australia was found. As Table 4.3 shows, Australian .au hosted sites comprise portals or referrer sites with limited content.

[22] A full description of the NetNanny filtering software may be found at http://www.netnanny.com/home/net_nanny_4/how_we_filter.asp.

Only two (2) adult website operators were found with Australian hosting experience and both of these had located offshore prior to the introduction of the BSA. In this context, the hypothesis that:

'A significant Australian hosted adult content industry existed before the Broadcasting Services Amendment (Online Services) Act (Cwlth 1999) came into effect on January 1, 2000.'

is therefore refuted. Since no significant pre-existing adult industry existed, the hypothesis that:

'Before or after January 1, 2000, Australian hosted adult Web sites moved offshore to foreign hosts.'

likewise, cannot be sustained. Those operators with Australian hosting experience confirmed that the high costs associated with Australian hosting, in particular volume charges of twenty (20) to thirty (30) times those charged by US hosts was the main factor influencing adult website data topography.

As streaming and Real technologies become common place, such a finding raises significant uncertainty about the future of Australian hosting and the consequences of high bandwidth costs for the growth of the Australian Internet economy. With reference to case study, the worrying implication of uncompetitive bandwidth pricing is discussed later in these conclusions.

5.3 Whither the Data Deficit: Have Changes in Data Topography Contributed to the Worsening of the 'Data Deficit'?

The topography study shows that as of the last quarter of 1999, and months before the introduction of the new censorship regime, in excess of eighty five percent (85.9%) of adult websites identified are hosted in the US, beyond the control of Australian law. Of the remaining Australian hosted sites, only portals or referrer pages were found. Any claim that the new regime would substantially add to the data deficit is unsustainable given that very little content appears to have existed on Australian servers by late 1999. For this reason, the hypothesis that:

'Changes in hosting arrangements for Australian adult Web sites have contributed to a data deficit in Internet traffic'

is refuted.

The topography data shows that there is virtually no large scale hosting of adult websites in Australia. The packet tracking revealed the commercial .au websites were all located in North America, despite their domain designations. The only 'sites' hosted in Australia are simple portals or referrer pages comprising a little over fourteen percent (14.11%) of discrete URLs. Even for the portal sites, almost eighty six percent (85.88%) are hosted on US servers. The implication here is that since the *real* content was already offshore, the removal of the portals and referrers will have a minimal effect on the deficit; the content has always been downloaded from the US and that situation remains unchanged.

5.4 Measuring Control Regime Effectiveness

This study suggested that if the content control regime was effective that a measurable change in user-download behaviour should ensue. As part of the initial research design, it was proposed to analyse Internet Content Provider (ICP) revenues and Internet Content Host (ICH) Server Logs to generate the required metrics. However, considerations of privacy and commercial confidentiality blocked access to the required data and an alternative method based on a content provider survey and fieldwork was adopted instead. The results of the fieldwork suggest at best no change in user-download behaviour or a possible increase in download activity since January 1, 2000. The sources of unreliability in terms of this finding concern the number of ICPs that participated (26% of the population) and possible bias. However, prima facie corroboration of the finding came from one of Australia's top four ISPs that reported 'off the record' that the pre-existing trend of increasing traffic flows of erotic content had continued post January 1, 2000 unabated. While ICPs were not prepared to quantify revenue trends, those who participated in interviews consistently maintained that no change in credit card income from Australian subscribers was detected, with one suggesting an increase in income.

Coupled with the suggested scope and scale of the content control problem and the issue of search engine manipulation outlined earlier, these results cast considerable doubt on the effective operation of the present co-regulatory scheme. Accordingly, the hypothesis that:
Current content blocking measures are effective in terms of the data topography and topology that characterise adult Web sites.

cannot be supported.

5.5 Costs to Industry

In Chapter One[23] it was revealed that ISPs are not required to implement server-side content control measures (ABA, 1999b). It was outlined that while this situation remains, that the financial implication from BSA compliance should be minimal. The removal of the Australian hosted portals and referrer sites implies a loss of *revenue* to Australian ISPs not an increase in overheads as was suggested prior to BSA introduction (Budde, 1999). However, it must be re-iterated that any attempt to move to a server-side mandatory control regime may have major financial and technical implications for the industry, particularly in the context of the content control problem outlined in the discussion of Question One (1).

5.6 Censorship Rules: Implications for the Operation of Mainstream E-Commerce in Australia Arising from the Introduction of Internet Censorship

Prior to the implementation of the BSA, there was debate whether ABA operations would be detrimental to the conduct of mainstream e-commerce in Australia, with some suggesting that overseas companies would not locate in Australia because of the restrictions (Senate Hansard, 1999b, p. 4, p. 16, p. 59). There is no evidence that BSA implementation has adversely affected e-commerce in Australia, in terms of regulatory interventionism and increased industry costs. However, as suggested by Glidewell (2000), the adult content industry has lessons for mainstream e-commerce. Why are they predominantly located offshore in the US? The content providers maintained that it was not feasible to operate a commercial high volume website in Australia revealing volume charges in Australia of twenty (20) to thirty (30) times more than in the US. This fact has major implications for the conduct of e-commerce in Australia and is discussed in detail below with reference to a case study in which the author is involved.

[23] Chapter One: 1.1.2 Regulation and Control

5.6.1 Case Study: Implications of Volume Charges

The case study concerns a small Western Australian company supplying share market analysis software. One of the company's software applications requires a daily database update via the Internet. Each daily update file is approximately seventy (70) Kilobytes. Their website is hosted on a large ISP based in Brisbane, Queensland. They have a volume amount (3 Gigabytes per month) included in their quarterly ISP charge with additional volume charged at thirteen (13) cents per Megabyte.

The company's subscriber base has been growing steadily and has now reached a 'critical mass' where they regularly exceed the monthly volume allowance. As a result they have now relocated their website to an ISP in Palo Alto in the US that provides ten (10) times the volume allowance (30 Gigabytes per month), but more importantly for subscriber base scaling, additional volume attracts a charge of *only seven US dollars (US$7) per Gigabyte*. Even allowing for currency exchange rates this represents a considerably saving to the company.

The change of location is not noticeable to this company's clients. The latency or communication delay is remarkably similar with a ping-time (packet round trip) of about four hundred and sixty (460) milliseconds to the US, and four hundred and thirty (430) milliseconds to Brisbane, from Perth. Interestingly the difference is quite marked using more advanced technology such as ADSL[24] with ping-times of ninety (90) milliseconds to Brisbane and two hundred (200) milliseconds to the US.

The implication is clear, as more Australian mainstream websites become increasingly sophisticated generating higher traffic volumes, they may follow where the adult websites have already gone, North America. The cause of the substantially higher charges in Australia is beyond the scope of this study, but it is clear that unless the problem is addressed, the conduct of sophisticated multimedia-based e-commerce in Australia will be severely limited.

[24] Literature Review, section 2.2.8: Connecting to the Internet

5.7 Acknowledged Limitations

The limitations of this study mainly stem from two areas. The highly charged political debate surrounding censorship of the Internet and the self-interest of the adult content providers leaves some doubt as to the veracity of survey and interview responses. The design of the study took this into account and attempted to minimize this factor. The profiling of the operators before data gathering commenced was useful in checking the veracity of responses, and given that no subject was found to be untruthful in any other area it must be assumed, in fairness, that their contribution was reliable.

The other main area of limitation lies in the fact that this study was restricted to adult websites with the .au domain designation in their URLs. As already pointed out their may be many other Australian owned and operated adult websites with the .com designation, but given the data on Australian volume charges the author considers it is unlikely any commercial adult sites are hosted on Australian servers with a .com designation. Therefore, this limitation does not affect the claim that no commercial quantities of adult content exist on Australian servers.

5.8 Directions for Future Research

From the earlier discussion of the data topography study, and with reference to the marketing strategies of the adult content websites, three (3) further research areas are suggested.

1. Using the same technology as the topography study i.e. packet tracking software, it would be interesting to measure the amount of Australian registered websites that use the .au designation compared to those using .com designations and exploring the rationale for either designation. Recall from Chapter Four that the adult websites use the .au designation purely for marketing purposes to foster the illusion for the client of dealing with a 'local' business, allaying fears somewhat of using credit card transactions on the Web.
2. In light of the case study outlined in the discussion of Question Six (6), and with particular reference to the cited case study, the author suggests a study of the 'critical mass' that a website must reach in terms of volume levels before local

hosting becomes uneconomical, and as a corollary an exploration of any techniques available to *maximize* the traffic level at which offshore hosting becomes necessary.

3. The success of the adult content industry in manipulating search engines is impressive. A thorough study of their techniques could prove very useful to mainstream website designers and operators.

5.9 Conclusion: Censorship Rules and Better Public Policy

This study used simple Information Technology methods to conduct grounded research in an area of public policy relevance. The findings suggest that the present regime is largely ineffective and that given the scope and scale of the content control problem as outlined, it may have negligible impacts on the inflow of adult content via the Internet. This fact should be cold comfort for both the pro-censorship and cyber rights factions, and may in time continue to fuel the debate possibly leading to more draconian control measures. A further issue concerns the cost of the current regime recently estimated to be over $2 million annually (Dearne, 2001).

Ramping up content blocking will likely arise in the future as a possible response to the failure of the current token regime. As discussed, the most obvious development path for content blocking resides with the mandating of proxy server filtering by ISPs. If the Australian Government embarks upon such a course, this will undoubtedly involve real on-costs to the Australian ISP industry with unknown consequences for the Australian Internet economy, but given the insignificance of the Australian market for adult content suppliers, the impact on the adult Internet Content Provider (ICP) industry would be minimal, merely an inconvenience.

Similar moves by the US Government could prompt the adaptation of the adult content industry to the new technology environment. Such adaptation will likely involve encryption of adult content by providers and the adoption of Virtual Private Networks (VPNs). Counter measures of this kind will significantly diminish the effectiveness of blocking an may even constitute a national security hazard by virtue of the greatly increased volume of encrypted information traveling on the Internet.

Within the policy community of regulators, lobby groups, Internet Service Providers and Internet Content Hosts, the question therefore needs to be addressed whether some alternative exists to content blocking as a public policy prescription. It is not the purpose of this research to explore alternatives. However, fieldwork conducted with Internet Content Providers (ICPs) impressed upon the author the potential for including ICPs in the policy community and the undesirability of excluding them.

During the debate preceding the introduction of the present regime all of the focus was placed on the ISP industry to control the perceived problem. A better strategy might arise from involving the adult ICP industry. After all, the aim of the present Act is ostensibly the protection of children from online pornography (BSA, Section 3, (1)) and the people best placed to implement this protection are the content providers. The attitude of the adult website operators was revealed by Mark Tiarra, president of the US industry peak body, the United Adult Sites (UAS);

> "'None of us want children on our sites, for basic moral reasons'. Besides (and perhaps more to the commercial point), Tiarra said, 'minors can't be held responsible for any debts the incur when viewing online porn.'"
>
> (Munro, 1999)

This point is often missed in the public policy debate, ICPs do not want children accessing their sites for purely commercial reasons. This presents a possible framework for cooperation in content blocking efforts concerning children.

In conclusion this research has shown that most Australian online adult content is in fact hosted in the US. The reasons for offshore hosting are almost totally financial and pre-date the introduction of the Broadcasting Services Act (Online Services) Amendment Act. The removal of adult sites from Australian servers should not contribute much to the so called 'data deficit'. The topology of sites suggests that it may be extremely technically problematic, and financially very expensive to implement any effective content control, including the URL filtering endorsed by the CSIRO. As suggested, the present content control arrangements are probably ineffective, and the impact of ABA operations on Australian adult websites inconsequential. Any effective solution may necessitate the inclusion of the adult Internet Content Providers in the public policy debate.

The extreme topology of the online adult content industry is a virtual latter day 'Gordian Knot' intricately woven into the fabric of the World Wide Web. It may be that the only way to control adult content on the Web would be to 'cut the knot' by introducing the packet level blocking as outlined by McCrea et al (1998, p.28) or unreliable keyword blocking, but this could result in severe damage to the Web itself. Given the opportunities presented by the advent of the Web for life-enhancing access to education and communication for children globally, in this case the remedy may prove more damaging than the problem itself.

REFERENCES

Aldred, J. (2000, May 29) APEC Moves on Data Deficit *InternetNews.com*, [online] Available WWW: http://www.internetnews.com/bus-news/article/0,,3_381721,00.html [2001, November 3]

American Library Association (ALA) (2001). *The Children's Internet Protection Act.* [online] Available WWW: http://www.ala.org/cipa/ [2001, November 3]

American Civil Liberties Union (ACLU) (2001) *ACLU Responds to Confusion Over Library Blocking Software Law; Seeks December Trial Date in Legal Challenge.* [online] Available WWW: http://www.aclu.org/news/2001/n051701a.html [2001, November 3]

Argy, P. (1996) *Investigation into the Content of Online Service.* Australian Computer Society (ACS) [online]. Available WWW: http://www.anu.edu.au/people/Roger.Clarke/II/ABAACSSubmn2.0 [2001, November 3]

Australian Broadcasting Authority (ABA) (1999a). *News Release: ABA registers codes of practice for Internet service providers and content hosts* [on-line], Australian Broadcasting Authority, Available WWW: http://www.aba.gov.au/abanews/news_releases/1999/134nr99.htm [2000, January 12]

Australian Broadcasting Authority (ABA) (1999b). *Internet Service Provider (ISP) responsibility* [on-line], Australian Broadcasting Authority, Available WWW: http://www.aba.gov.au/internet/industry/isp/index.htm [2000, January 5]

Australian Broadcasting Authority (ABA) (2001) *News Release: Government releases second report on co-regulatory scheme for Internet content* [online], Australian Broadcasting Authority, Available WWW: http://www.aba.gov.au/abanews/news_releases/2001/17nr01.htm [2001, November 2]

Australian Bureau of Statistics (ABS) (2000) *8147.0 Australian children log on to information technology* [online]. Available WWW: http://www.abs.gov.au/ausstats/abs@.nsf/0/6D8F3C2071273D8DCA25699E0000F590?Open&Highlight=0,internet#Links [2001, November 2]

Australian Bureau of Statistics (ABS) (2001a) *1367.5 Western Australians out front in information technology stakes* [online] Available WWW: http://www.abs.gov.au/ausstats/abs@.nsf/0/992D5FAD0BFC1887CA256A8D0017FB23?Open&Highlight=0,internet#Links [2001, November 3]

Australian Bureau of Statistics (ABS) (2001b) *8153.0 Internet Activity, Australia* [online] Available WWW: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/NT00018FDE#Links [2001, November 2]

Broadcasting Services Amendment (Online Services) Act (Cwlth) (1999), [online]. Available WWW: http://scaleplus.law.gov.au/html/comact/10/6034/rtf/122of99.rtf [2000, April 20]

Budde, P. (1999, August 24) Regional ISPs Under Threat from $150m Censorship Compliance. *The Australian.* p. 24.

Buskin, J. (2000, April 17) *E-Commerce (A Special Report): Industry by Industry --- The Web's Dirty Little Secret: What porn sites lack in respect, they make up for in profits.* Wall Street Journal. [online] Available WWW: http://proquest.umi.com/pqdweb?Did=000000052666098&Fmt=1&Deli=1&Mtd=1&Idx=7&Sid=2&RQT=309 [2000, August 8]

Classifications (Publications, Films and Computer Games) Act 1995 (Cwlth) [online] Available WWW: http://www.austlii.edu.au/au/legis/cth/consol_act/cfacga1995489/ [2001, November 2]

CaveCreek (2000) CaveCreek Wholesale Internet Exchange [on-line] Available WWW: http://www.cavecreek.com/ cavecreek wholesale internet exchange.htm [2000, August 20]

Chapman, G. (1995) Not so naughty. *The New Republic 213* (5) p. 11

Clarke, R. (1998) Prosecution for online child pornography in the ACT. *Internet Law Bulletin 1,* (5) pp. 76-77

Communications Decency Act (U.S. Congress) 1996. [online]. Available WWW: http://www.epic.org/free_speech/censorship/copa.html [2000, February 10]

Connolly, C. (1999) Content Regulation Rejected in Canada. *Internet Law Bulletin 2*, (3) p. 43.

Connolly, C. (2001) An Introduction to Internet Content Regulation in Asia and the Pacific Region. *Internet Law Bulletin. 3*, (1) pp. 129-131.

Coopee, T. (2000, June 12) How to climb the search engine rankings. *InfoWorld.* [online]. Available WWW: http://www.infoworld.com/articles/mt/xml/00/06/12/000612mtsearch.xml [2001, November 3]

Dearne, K. (2001, May 15) Net censorship a $2.5m “waste”. *The Australian IT* [online] Available WWW: http://australianit.news.com.au/articles/0,7204,1998795%5E15306%5E%5Enbv%5E,00.html [2001, November 15]

Department of Communications and the Arts (DCA) (1994) *Report: Regulation of Computer Bulletin Board Systems.* [online] Available WWW: http://www.dcita.gov.au/nsapi-text/?MIval=dca_dispdoc&pathid=%2fpubs%2fbulletin%5fboard%2freport%2ehtm [2001, November 3]

Department of Communications, Information Technology and the Arts (DCITA) (1999). *Media Release: Internet Content Advisory Board Announced* [on-line]. Available WWW: http://www.dcita.gov.au/nsapi-text/?MIval=dca_dispdoc&ID=4642&template=Newsroom [2001, November 3]

Dietal, H.M & Dietal, P.J. *Java: how to program* (3rd Ed). Upper Saddle River: Prentice Hall.

Dionne, Pierre. (1999*) Legal and judicial aspects: extraterritorial law and extradition* Paper presented at the conference: Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: An international challenge - Expert Meeting, UNESCO, Paris, 18-19 January [online] Available WWW: http://www.unesco.org/webworld/child_screen/documents/dionne.rtf [19 October, 2001]

Dyson, P. & Kelly-Bootle, S. & Heilborn, J. (1999) *Unix Complete.* Alameda: Sybex.

Electronic Frontiers Foundation (EFA) (2001a*) FOI Request on ABA* [online] Available WWW: http://www.efa.org.au/FOI/foi_aba2000.htm [2001, November 3]

Electronic Frontiers Foundation (EFA) (2001b*) South Australia Net Censorship Bill 2000* [online] Available WWW: http://www.efa.org.au/Campaigns/sabill.html [2001, November 3]

Electronic Privacy Information Center (EPIC) (1997). Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet [online] Available WWW: http://www.epic.org/reports/filter_report.html [2001, November, 11]

Elmer-Dewitt (1995, July 3) On a screen near you: Cyberporn. *Time 146* (1) pp. 38-45

Endeshaw, A. (2001) *Internet and E-Commerce Law: With a Focus on Asia-Pacific.* Singapore: Prentice Hall.

Feit, S. (1996*). TCP/IP: architecture, protocols, and implementations with IPv6.* New York, McGraw-Hill.

Garfinkel, S & Spafford, G. (1997) *Web Security and Commerce.* Cambridge: O'Reilly & Associates, Inc.

Gaskin, J. (1997) *The complete guide to Netware® 4.11/IntranetWare™* (2nd Edition) Alameda, Network Press.

Gibson, H. (2000) Shooting the Messenger *Issue Analysis* 10, pp. 1-11 [online]. Available WWW: http://www.cis.org.au/IssueAnalysis/ia10/ia10.pdf [2001, November 2]

Glidewell, R. (2000, April) Business lessons from online porn. *Upside 12* (4). pp. 194-208. [online] Available WWW: http://www.upside.com/texis/mvm/print-it?id=38adbbff0 [2001, November 2]

Goncalves, M. (1997) *Firewalls Complete.* New York: McGraw-Hill.

Greenfeld, K. (1999, April 19) Taking stock in smut. *Time 153* (15) p. 43. [online] Available WWW: http://proquest.umi.com/pqdweb?Did=000000040519573&Fmt=3&Deli=1&Mtd=1&Idx=1&Sid=21&RQT=309 [2001, November 2]

Greenfield, P. (1999*) Technical Aspects of Blocking Internet Content* CSIRO

Greenfield, P& McCrea, P & Ran, S (1999) *Access Prevention Techniques for Internet Content Filtering* CSIRO

Hansell, S. (2000, July 27) *Amazon Reports Losses of $317 Million in the Second Quarter.* New York Times. [online] Available WWW http://proquest.umi.com/pqdweb?Did=000000056996982&Fmt=3&Deli=1&Mtd=1&Idx=28&Sid=19&RQT=309. [2000, August 8]

Hawkins, G & Zimring, F.E. (1998) *Pornography in a free society.* Cambridge: Cambridge University Press.

Heaton, G. (2000) Nazis on the Net: free speech versus the world police. *Internet Law Bulletin. 3,* (8) pp. 109-110

Hellwege, J. (1996) Internet regulation: law makers try to tame cyberspace. *Trial. 32,* (1) pp. 11-14.

Inktomi Corporation (2001) *Inktomi Web Map* [online] Available WWW: http://www.inktomi.com/webmap/ [2001, November 3].

Internet Industry Association. (1999) *Internet Industry Code of Practice.* [online] Available WWW: http://www.iia.net.au/code6.doc [2001, November 2]

Judge, P. & Green, H. (1998, November 23) Sex: One Savvy Web Industry. *Business Week.* [online] Available WWW: http://proquest.umi.com/pqdweb?Did=000000036129512&Fmt=3&Deli=1&Mtd=1&Idx=1&Sid=11&RQT=309

Kahaner, L (2000, June 12) Content matters most in search-engine placement. *Informationweek.* (790) pp. 172-178. [online] Available WWW: http://www.informationweek.com/790/search.htm [2001, November 3]

Kendrick, W. (1996) *The Secret Museum: Pornography in Modern Culture*. Berkely: University of California Press.

Kennedy, J. (1995) *The Internet & World Wide Web: The Rough Guide*. London: Rough Guides.

Koener, B (2000, March 27) *A Lust for Profits Pornography is a huge a growing cyberspace draw. But will salacious Web sites be a hit on Wall Street?* U.S. News & World Report 128 (12) pp. 36-44. [online] Available WWW: http://proquest.umi.com/pqdweb?Did=000000051397642&Fmt=3&Deli=1&Mtd=1&Idx=1&Sid=1&RQT=309 [2001, August 8]

Kuo, P. (1997) *NetWare Web Development.* Indianapolis: Sams.net Publishing.

Lin, J. (1996) *The Net Persona* [online] Available WWW: http://www.law.ucla.edu/students/academicInfo/coursepages/archive/S96/340/persona.htm [2001, November 2]

Lumby, C. & Cross, R. & Mountford, C. (1997) Manufacturing Dissent. In A. Crawford & R. Edgar (Eds.), *Transit Lounge* (pp. 67-70). North Ryde: Craftsman House.

Martin, L. (1999). Cyberporn: Slipping Through the Net. [online] *Sydney Morning Herald Online.* Available WWW: http://www.smh.com.au/news/9903/20/features/features3.html [2000, April 12]

McComb, G. (1998) *Web Commerce Cookbook.* New York: John Wiley & Sons.

McCrea, P & Smart, B & Andrew, M. (1998) *Blocking Content on the Internet: a Technical Perspective.* CSIRO.

Microsoft (2001) *Streaming Methods: Web Server vs. Streaming Media Server* [online] Available WWW: http://www.microsoft.com/Windows/windowsmedia/compare/webservvstreamserv.asp [2001, November 3]

Nachbar, T. (2000) Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character. *Minnesota Law Review 85* pp. 215-318. [online] Available WWW: http://papers.ssrn.com/sol3/delivery.cfm/SSRN_ID259951_code010214130.pdf?abstractid=259951 [2001, November 3]

The National Office for the Information Economy (NOIE) (2001)(*The Current State of Play: Australia and the Information Economy* [online], NOIE, Available WWW: http://www.noie.gov.au/projects/information_economy/research&analysis/ie_stats/CSOP_June2001/exec.htm [2001, November 2]

Nielsen-NetRatings (2001) *INTERNET USAGE STATISTICS FOR THE MONTH OF SEPTEMBER 2001* [online]. Available WWW:

http://epm.netratings.com/au/web/NRpublicreports.usagemonthly [2001, November 2]

Office of Film and Literature Classification (OFLC) (2001) *Communique: Launch of combined review of guidelines for the classification of films and computer games.* [online] Available WWW: http://www.oflc.gov.au/PDFs/AG_Glines_Rev_Communique.pdf [2001, November 3]

Pastore, M. (2000) *The Web: More Than 2 Billion Pages Strong.* [online] Available WWW: http://cyberatlas.internet.com/big_picture/traffic_patterns/article/0,,5931_413691,00.html [2001, November 3]

Pearl Software (2001*) Internet Monitoring Solutions for the Way You Work, Study and Play* [online] Available WWW: http://www.pearlsoftware.com [2001, November 2]

Pfleeger, C. P. (1996*). Security in computing.* Upper Saddle River, Prentice-Hall.

Reno v ACLU (US Supreme Court No. 96-511, 26 June 1997) [online]. Available WWW: http://www.aclu.org/court/renovaclu.html [2001, April 15]

Resnick, P & Miller, J. (1996) PICS: Internet Access Controls Without Censorship. *Communications of the ACM. 39*, (10), pp. 87-93.

Rimm, M. (1995) *Marketing Pornography on the Information Superhighway.* [Electronic version] Available WWW: http://rhodes.www.media.mit.edu/people/rhodes/Cyberporn/mrtext.html [2001, November 3]

Sarantakos, S. (1994) *Social Research.* Melbourne: McMillan.

Scott, B. (1999a). *The Dawn Of A New Dark Age - Censorship and Amendments to the Broadcasting Services Act* [online]. Available WWW: http://www.gtlaw.com.au/flash/index.jsp?c=/t/ca/lpubs.jsp?&s=1&p=82&e=t&t=GILBERT+and+TOBIN&a=false [2000, April 12]

Scott, B. (1999b) *An Essential Guide to Internet Censorship in Australia* [online]. Available WWW: http://www.gtlaw.com.au/flash/index.jsp?c=/t/ca/lpubs.jsp?&s=1&p=82&e=t&t=GILBERT+and+TOBIN&a=false [2001, November 2]

Senate (1995) *Report on Regulation of Computer On-Line Services Part 2* [online] Available WWW: http://www.aph.gov.au/senate/committee/comstand_ctte/online2 [2001, November 3]

Senate (1997) *Report on Regulation of Computer On-Line Services Part 3* [online] Available WWW: http://www.aph.gov.au/senate/committee/comstand_ctte/online3 [2001, November 3]

Senate Hansard (1999a, April 27) Official Committee Hansard: Select Committee on Information Technologies. [online] Available WWW: http://www.aph.gov.au/hansard/senate/commttee/s2259.pdf [2001, November 3]

Senate Hansard (1999b, April 28) Official Committee Hansard: Select Committee on Information Technologies. [online] Available WWW: http://www.aph.gov.au/hansard/senate/commttee/s2279.pdf [2001, November 3]

Senate Hansard (1999c, April 29) Official Committee Hansard: Select Committee on Information Technologies. [online] Available WWW: http://www.aph.gov.au/hansard/senate/commttee/s2280.pdf [2001, November 3]

Senate Hansard (1999d, May 3) Official Committee Hansard: Select Committee on Information Technologies. [online] Available WWW: http://www.aph.gov.au/hansard/senate/commttee/s2281.pdf [2001, November 3]

Simms, M. (1998) *Why Censorware Can't Work.* [online] Available WWW: http://www.censorware.net/essays/whycant_2_ms.html [2001, November 11]

SurfControl (2001) *Web and Email Filtering Products* [online] Available WWW: http://www.surfcontrol.com/resources/business/index.html [2001, November 2]

Sullivan, D. (2000a) How search engines work. *SearchEngineWatch.* [online] Available WWW: http://www.searchenginewatch.com/webmasters/work.html [2000, September 2]

Sullivan, D. (2000b) How search engines rank web pages. *SearchEngineWatch.* [online] Available WWW: http://www.searchenginewatch.com/webmasters/rank.html [2000, September 2]

Sullivan, D. (2000c) What is a Bridge or Doorway Page. *SearchEngineWatch.* [online] Available WWW: http://www.searchenginewatch.com/webmasters/bridge.html [2000, September 2]

Tate, T. (1990) *Child Pornography: An investigation.* London: Methuen.

Viewpoint: X-Rated Wisdom; What online porn can teach Asia about Web profits. (2001, March 23) p. 1. *Asiaweek*

W3C. (1999) *Platform for Internet Content Selection (PICS).*_W3C [online]. Available WWW: http://www.w3.org/PICS/ [2001, November 2]

Walker, D. (1999) Photographers cash in on Web Porn. *Photo District News* 19 (3) pp. 65-71 [online] Available WWW:

http://proquest.umi.com/pqdweb?Did=000000039600307&Fmt=4&Deli=1&Mtd=1&Idx=1&Sid=1&RQT=309 [2001, November 2]

Wallace, J. (1997) *CyberPatrol: The Friendly Censor.* [online] Available WWW: http://www.censorware.net/essays/cypa_jw.html [2001, November 11]

Weckert, J. & Adeney, D. (1997) *Computer and Information Ethics.* Westport: Greenwood Press.

Westphal, H & Towell, E. (1998) Investigating the future of Internet regulation. *Internet Research: Electronic Networking Applications and Policy. 8* (1), 26-31

Yee, F.L. (1999) Singapore: internet regulation or censorship? *Internet Law Bulletin 2*, (3) pp. 44-46

Zakon, R.H. (2000*). Hobbes Internet Timeline v5.0* [online]. Available WWW: http://info.isoc.org/guest/zakon/Internet/History/HIT.html [2000, April 12]

GLOSSARY

- Application Level

  The application layer is the topmost layer in the International Organisation for Standardisation (ISO) reference model for Open Systems Interconnection (OSI). This layer communicates directly with user applications running on a computer, providing an interface to the distributed data processing services below this level.

- Collocation

  Placed together, situated in close proximity. In the context of an ISP, the placing of many Internet servers at the same location, sharing a common Internet access point.

- Content

  Any data that may be downloaded or uploaded via the Internet e.g. text, graphics, sound, movies, etc.

- Error of misattribution

  To attribute incorrectly a cause and effect. In the context of this study, it was vital to ensure data gathering on websites was completed before January 2000 so that any effects of the introduction of the BSA could be correctly attributed to events occurring after January 2000 and not misattributed to events before this time.

- Internet Protocol (IP) Address

  A 32-bit number which uniquely identifies a computer's interface on the Internet.

- Packet

  On the Internet, communication is accomplished by the exchange of Internet Protocol (IP) packets. Each packet includes a source IP address and a destination IP address as well as the data to be transmitted over the network.

- Packet Level

  Usually refers to the Network Layer of the OSI architecture. Data at this layer is packaged into discrete packets of information for transmission between computers.

- Proxy Server

A computer that makes a single Internet connection and services Internet content requests on behalf of many users.

- Router

  A computer that is used to interconnect two or more Local Area Networks (LANs) together. It is configured to forward packets. It may also be called a gateway or intermediate system.

- Server

  A computer providing services on a network. The client computers make requests to the server. The server responds to the request by providing some service to the client computer.

- **URL**

  Universal Resource Locator. A symbolic name that relates to a particular resource at a precise location on the Internet e.g. http://www.cowan.edu.au/library. This URL is the location of the file relating to the library home page on the Edith Cowan University site.

- Website

  A program stored on a host computer on the Internet. When the website is accessed, a part of this program is downloaded and run on the browser of the accessing computer.

APPENDIX A

Internet Content Provider Survey

Participant Profile

How many individuals do you employ in Australia?

Can you estimate your average subscriber base?

What do you know of the new Commonwealth co-regulatory regime?

Do you think it will adversely impact your business? (Yes, how?; No, why?)

Have you noticed any change in subscriber download behaviour since January 2000? (No change; Drop; Increase)

Technology

Do you provide streaming video at present?

Do you anticipate the provision of streaming video in the future?

Are there any future technology marketing strategies you can identify in this area?

Hosting Arrangements

What percentage of your content is hosted in Australia?

What percentage of your content is hosted offshore?

What is the approximate cost to you of hosting in Australia?

What is the approximate cost to you of hosting offshore?

What is your hosting configuration (Disk Space?, Server Farm?, Own Web access?)

What are your volume costs in Australia ($/Meg)?

What are your volume costs offshore ($/Meg)?

APPENDIX B

INTERNET CONTENT PROVIDER INTERVIEW SCRIPT

Industry Structure

- Hosting Arrangements

- Web site structure

- Use of .au domain designations

- Ghetto domains

- Traffic volumes

Attitudes to Censorship

- Censorship issues

- Paedophile activity on the Web

- ABA operations

- Filtering technology

- Counter measures

- Content labeling

Future Directions

- New technology (streaming media, interactive broadband technology)

- Industry growth

- New markets

- Marketing techniques

APPENDIX C

Statement of Disclosure

This project entitled *Internet Content Control in the Australian Context* is attempting to measure the compliance effects of the Commonwealth Government's *Broadcasting Services Amendment (Online Services) Act 1999*, and the effectiveness of the Act in controlling access to erotic content on the Internet.

It is intended to gather data from Australian Internet Service Providers (ISPs) and Australian Internet Adult Content Providers (ICPs). The ISPs will be asked to provide information on the compliance costs to the ISP industry, and the extent of takedown notice requests. The ICP industry will be asked for information on user download behaviour. This information will be used to measure the effectiveness of the content control regime. In addition the members of the ICP industry will be questioned on future technology or marketing strategies, which may impact on the compliance requirements of the ISP industry.

The interview or survey will take only a few minutes to complete and participants are advised that they are under no obligation to answer any or all questions. The information provided will be treated with the utmost care to guarantee confidentiality. No individual or organisation will be identified in the dissertation, or in any subsequent publication unless authorised in writing by the subject or organisation concerned.

The use of content control on the Internet has implications for the entire Australian Information Economy. This project may provide data, which will prove useful in public policy formulation in this area. The Government's content control regime costs over $2 million per year, it is vital to measure if it is effective or not.

An effect of the Act may be to force Australian ICPs offshore. This may have implications for both the ISP industry and the general economy. Data gained in this project may be of use to the ISP and ICP industries, providing information on possible public policy, marketing, and technology changes that may be of interest.

Any questions concerning the project *Content Control Issues in the Australian Context* can be directed to David Harte, School of Computer and Information Science, Edith Cowan University, on 0416209674.

If you have any concerns about this project and would like to talk to an independent person, you may contact Mr. Mark Brogan (Project Supervisor) on (08) 93706300.