2009

Untangling the net: the scope of content caught by mandatory internet filtering

John Hartley

Catharine Lumby

Lelia Green

Untangling the Net: The Scope of Content Caught By Mandatory Internet Filtering

Professor Catharine Lumby,
Journalism and Media Research Centre,
University of New South Wales

Professor Lelia Green,
Edith Cowan University

Professor John Hartley, ARC Centre for
Creative Industries and Innovation,
Queensland University of Technology

Table of Contents

Executive Summary

Background

The following report considers a number of key challenges the Australian Federal Government faces in designing the regulatory framework and the reach of its planned mandatory internet filter. Previous reports on the mandatory filtering scheme have concentrated on the filtering technologies, their efficacy, their cost and their likely impact on the broadband environment. This report focuses on the scope and the nature of content that is likely to be caught by the proposed filter and on identifying associated public policy implications.

We recognise that the Federal Government faces real challenges in balancing the risks posed by the online media environment with the opportunities that environment presents. In preparing this report, the authors acknowledge that the Federal Government is still considering the detail of how mandatory filtering will be implemented and how classification will work under the scheme. Our research is not intended to pre-empt those decisions but to offer constructive input, to highlight key public policy challenges and to inform public dialogue.

This report was prepared by three senior academics in the media studies field, Professor Catharine Lumby, Professor Lelia Green and Professor John Hartley. We have all published extensively on the issues of online media, media content regulation, young people and media consumption, and public policy. As members of the ARC Centre of Excellence for Creative Industries and Innovation, we are currently collaborating on a large research project that considers the risks and opportunities for children in the online and mobile media era. The research on which this report is based was supported by the Internet Industry Association and we acknowledge their assistance. We would also like acknowledge the input of Professor Stuart Cunningham, Director of the ARC Centre of Excellence for Creative Industries and Innovation at QUT, and the research assistance of Paul Taylor.

The Federal Government faces unprecedented challenges in media content regulation. The online environment is one in which media consumers are increasingly becoming media producers, with enormously varying levels of skill and distribution. The means of distribution and consumption range across content developed and distributed by established media organizations, through emerging online sites, to amateur and peer-to-peer content.

A neglected aspect of public policy that needs to be considered in the internet filtering debate is the question of how we sensibly balance the risks posed by online material, particularly to children, and the opportunities provided to the broader community to participate in sometimes controversial debates, to access and debate material pertaining to political and social issues, and to allow reasonable adults to make decisions about what they consume or produce online.

Australia's current system for regulating media content has evolved erratically, reactively and inconsistently. The Federal Government has inherited not only the challenges of the new media era but equally the deficiencies of the regulatory regime developed for past media eras. It is clear that Australia needs to avoid simply applying an inadequate and inconsistent media content regulation regime to a very different and emergent media landscape. There is a clear need to rethink media content regulation in the online era –a need supported by the research detailed in the body of this report.

The challenge of regulating media content in the online era is also an opportunity to examine the rationale of media content regulation from first principles and to engage the public and all stakeholders in a dialogue about the purpose and scope of classification.

Key Findings

On the basis of our survey of international research, we argue that Australia should not apply a system of media content classification that already treats different media inconsistently to the online environment without any consideration of the existing flaws in regulation and the complex particularities of the online world. *The internet is not a medium*: it is a whole new media environment which requires us to rethink how we regulate content, protect vulnerable groups and define the relationship between media consumers and media producers.

One of the clear risks of focusing disproportionate public policy attention and public resources on content regulation is that many parents and teachers may gain a false sense of security when it comes to the material their children encounter online. This risk is particularly high in a regulatory system that relies on a blacklist which, by its very nature, will only capture and represent a small sample of the online material of concern.

1. Scope of Content

One of the often stated aims of the Federal Government's internet filter is to prevent access to child pornography[12]. No serious commentator could question the importance of shutting down the production and distribution of child abuse materials or of blocking access to other categories of the content the great majority of Australians find abhorrent, including bestiality and active incitement to violence. Yet if the mandatory internet filtering proceeds on the basis of the current approach to opt-in voluntary filtering of material hosted overseas- via a blacklist maintained by the Australian Communication and Media Authority – a far broader variety of material than that represented at the extreme end of the spectrum may be caught.

In December 2009, Minister Conroy announced that the RC category would be used as a basis for mandatory filtering of the internet at ISP level in Australia. This submission addresses some public law and policy concerns about the efficacy of using that category as a basis for filtering.
The current proposal indicates that the list of mandatorily filtered sites will be based on the RC category. The key issue that arises here is that the RC category – developed primarily as a classification code for film and video – is a broad category which invites broad legal and quasi-legal interpretation.

In Australia, much material which falls outside the R 18+ category moves into the RC category because the X 18+ category excludes any material that depicts violence. The broad range of material that is produced for and distributed on the internet, including news, current affairs and other material of public interest, may well be caught on the basis that a classification regime intended for film and video is applied to an online environment where multiple producers and consumers intersect.

The interpretation of the RC category on its own also opens an array of potential issues given the breadth of the purpose and audience for online material. The Classification Act does not offer detailed criteria for determining whether content is RC. Rather, it states that material be classified in accordance with the principles in the National Classification Code. These guidelines are extremely broad.

The cases referred to in this report strongly suggest that interpretations of what is deemed part of the RC category is one the courts are inclined to leave to the discretion of the Classification Board and Review Board. This is of real concern for an online environment in which the range, scope and purpose of material is far wider than that encountered in films produced for entertainment purposes. Adding weight to this concern is that one of the factors that the Classification Act states must be taken into account when classifying material is "the persons or class of persons to or amongst whom it is published or intended or likely to be published". This provision reflects a set of assumptions about the way material is generated and consumed which map onto the traditional media environment but which become almost meaningless in an era where material migrates rapidly across many contexts and where an enormous amount of content is generated by consumers themselves.

In the report we consider some hypothetical examples of material that could well be deemed RC and mandatorily filtered out of the Australian internet. Potential material that could feasibly be deemed RC on the basis of the current Classification Code includes:

- A site devoted to debating the merits of euthanasia in which some participants exchanged information about actual euthanasia practices.
- A site set up by a community organisation to promote harm minimisation in recreational drug use.
- A site designed to give a safe space for young gay and lesbians to meet and discuss their sexuality in which some members of the community narrated explicit sexual experiences.
- A site that included dialogue and excerpts from literary classic such as Nabokov's *Lolita* or sociological studies into sexual experiences, such as Dr Alfred Kinsey's famous *Adult Sexual Behaviour in the Human Male*.
- A site devoted to discussing the geo-political causes of terrorism that published material outlining the views of terrorist organisations as reference material.

2. Transparency

Another critical question raised by the prospect of a mandatory filtering system is whether the public will have the right to know what is on the blacklist, the right to appeal decisions to place material on the blacklist and a consequent right to judicial review. There are clear public policy reasons for denying access to some categories of material on this kind of list – for example, information that might facilitate access to child pornography or compromise national security. However, if the range and nature of material potentially blacklisted extends well beyond these categories then there are some clear public law principles that require attention. We need to consider what material on the blacklist will not be released and for what reason. We also need a clear policy and regulatory framework that spells out who is able to access the list and who will have legal standing to appeal content caught by the list.

A related concern here is that if parents and other who care for or educate children are unaware of the size and content of the blacklist they may have a false sense of security and fail to properly supervise young people's online activities. It is critical, in this regard, that the public is informed about how extensive the blacklist is and what kind of material it catches.

3. International Context

The proposed public model of mandatory internet filtering would separate Australia from the great bulk of western liberal democracies who have opted for industry self or co regulatory approaches. It is clear that liberal democracies tend to adopt voluntary regulatory approaches that focus on narrowly defined segments of undesirable content – usually child pornography. In the European Union, for example, the filtering regime requires interaction between governments, police, advocacy groups and the general public who identify instances of undesirable content, and the ISPs who voluntarily filter such content on the understanding that any failure to do so is likely to result in greater regulation of the sector. There is general consensus on the material that is considered illegal or harmful and this includes: child pornography, human trafficking, racist material, material promoting terrorism and all forms of internet fraud.

While it is clearly important that Australians make our own decisions about managing the risks and opportunities posed by the online media environment, we submit that it is equally important that we take into account how those decisions place us in relation to comparable democracies and to explore the evidenced-based options that have informed policy-making in other jurisdictions.

4. Balancing Rights and Managing Risk

If the government were to implement a mandatory filter, the extent to which this would conflict with the right to freedom of speech and access to information is uncertain although it is clear that the scope of the content caught would certainly increase the level of the conflict. Our governments have a clear obligation to protect national security, the public order and to uphold public morals. They also have an obligation to consider how to balance and protect freedom of speech and association. In the online and mobile media era balancing these obligations becomes increasingly difficult: both in terms of policy orientation and detail. The Federal Government in Australia faces an unprecedented scenario in which media consumers have become media producers and distributors online and in which the means of hosting and producing material proliferate hourly.

The clear issue at this juncture is whether mandatory internet filtering, via a blacklist, is the most appropriate method to go forward in terms of balancing rights and blocking the worst category of content. There is evidence to suggest that all systems can be evaded by some internet users and that no technical means of filtering can be implemented that prevents such evasion. The question as to whether overfiltering or underfiltering is preferable remains a matter that individual states must decide. While it seems that many states have delegated responsibility to individual ISPs, this question raises two important public policy questions:

- **In the case of overfiltering**: is the potential of unwittingly restricting the lawful expression of a citizen and their access to information so offensive to fundamental human rights that it conceivably constitutes a breach of Australia's international obligations?

- **In the case of underfiltering**: is the inexact implementation of internet filtering satisfactory given that much content which may be deemed grossly offensive to public morals will not be successfully blocked and may also leave parents and teachers with a false sense of security when it comes to children accessing the internet?

The growth of peer-to-peer online networks generate some additional regulatory challenges for the Federal Government. A mandatory filter will not catch illegal material disseminated through these channels. Indeed, one of the key challenges in identifying those who disseminate and consume child pornography is that much of it is not openly displayed on websites but is exchanged in a covert and encrypted manner via bulletin boards. More recently, evidence is emerging that child pornography is also increasingly being covertly housed on third party websites through the use of malware bots. The international evidence clearly suggests that the majority of child abuse prevention resources need to be targeted towards coordinated policing of those who manufacture and share child abuse materials, often in contexts where they are involving their own family members or children known to them.

1.0 Introduction

1.1 Background

This report investigates the scope and nature of content likely to be included in the Australian Federal Government's planned introduction of a mandatory internet filter, how this compares to international practice and what public policy issues may flow from this change.

1.2 Research Questions

Our report considers the following key issues:

- What is the Federal Government's current policy on internet filtering, particularly in relation to the scope of material to be caught by proposed filtering?
- What public policy considerations should the Government take into account in seeking to implement its current policy?
- What are the matters of public interest in regard to the potential impact of such filtering on democratic debate, access to information, cultural vitality and freedom of speech?
- Where should the line be drawn in terms of striking a balance between a need to protect Australians from harmful material and the rights of adult citizens to freedom of expression and the right to information and to access material which is not itself illegal?
- What are the different categories/types of content that could be blocked under this filtering proposal?
- What are the options open to the Federal Government when it comes to deciding what categories and types of content should be blocked?
- In relation to these categories (including child abuse material, 'Refused Classification' material, and harmful/inappropriate content) what are the challenges implicit in filtering such material including:
    - How (clearly) are they defined in Australian law;
    - How are they currently handled in terms of regulation and law enforcement;
    - How would the filtering of that scope of material compare with international practice;
    - What issues of freedom of expression, access to information, public acceptance of the usefulness/legitimacy of filtering, and government control (or even censorship) of content would arise?
    - Other similar factors thought to be relevant by the research team will also be considered here.
- What challenges and concerns arise in relation to applying existing regulatory frameworks for traditional media (e.g. the RC category) in an online context?
- What is international practice around the scope of material filtered in other jurisdictions?

1.3 Methodology

This report is based on an international literature review on approaches to internet filtering, the scope of content filtered and the public policy issues that arise from different approaches. It also includes a comprehensive review of published Australian documents on the proposed mandatory internet filter. Primary documents such as policy factsheets, ministerial press releases and departmental reports were reviewed. This activity was complemented by an exhaustive search of relevant media reportage of the issue in addition to current scholarly research. Relevant Hansard, legislation and case law was also consulted to establish the framework in which online censorship currently operates.

1.4 Internet Filtering Terminology

Although a discussion on the specifics of filtering technology is beyond the scope of this report, it is necessary to provide a working knowledge of the circumstances under which filtering technology can be applied. Internet filtering can be implemented at three levels:

- On the centralised backbone of a nation's internet infrastructure,
- At the decentralised Internet Service Provider (ISP) level; or
- At the individual PC level

Filtering can also be mandatory or voluntary. That is, governments can apply a mandatory filter on the nation's internet infrastructure. Otherwise they can regulate that ISPs apply a mandatory filter that filters content. Alternatively, governments have the option to allow ISPs to voluntary implement filtering software on their products or provide individual PCs users with appropriate filtering software that they freely apply to their own PCs.

Filtering technology is a complicated process with a number of different options available. For a brief overview of the options available to governments or ISPs see Appendix One.

1.5 Structure of the Report

This report is structured into the following five sections:

Section 1 introduces the report and provides a brief overview of the evolution of media content regulation in Australia and considers some of the broad public policy principles that need to be balanced in designing a regime for future media content regulation.

Section 2 provides an overview of the current Federal Government's stated policy concerning internet filtering. It also discusses the type of content that is likely to be filtered, how this content is determined in law and the potential legal challenges to this law.

Section 3 discusses the international practices of internet filtering. It considers how other western liberal democracies have approached internet censorship and compares how Australia's proposed filtering policy compares with these, and with countries not currently aligned with western liberal democracies.

Section 4 explore the key public policy issues raised by mandatory internet filtering in relation to the potential scope and nature of the content filtered.

1.6 Media Content Regulation in Australia

In this first section, we introduce and background the key public policy issues identified in this report: the question of whether the Australian federal government should apply a classification regime built on the foundation of a very different media landscape to the current online environment. We see this as a threshold issue for any debate about the scope and form of content that will or should be caught in a mandatory filtering system.

Media Content Regulation: Background

The current Federal Government has inherited a complex and inconsistent system for regulating media content. Over many decades, content regulation in Australia has evolved in an ad hoc manner and on the basis of political expediency, across the political spectrum. Our research into the history of this regulation strongly suggests that Australian media classification systems have not, to date, been built on sufficient empirical evidence about actual public attitudes or on evidence about actual media consumer behaviour. In saying this, we acknowledge the valuable and expert work done by government agencies such as the Australian Media and Communication Authority (ACMA) and the Office of Film and Literature Classification (OFLC). ACMA, in particular, has been exemplary in producing research to inform public policy. However, the historical record gives little room for public confidence in the level of resourcing for the role either agency is potentially being asked to play in the next iteration of public policy and regulation around online media content.

The anomalies in the regulation of media in Australia are perhaps best illustrated by the current treatment of computer games which, while classifiable under the Classification (Publications, Films and Computer Games) Act 1995 remain unavailable for classification under the R 18+ or X18+ categories. This distinction is based, according to the Classification Guidelines, on the premise that the interactivity of games changes their impact on media audiences. This distinction is, from the point of view of a wide body of media studies research into gaming and other media consumption practices, unsustainably broad and certainly not supported by the empirical evidence in our field. As a research paper examining a major national study of computer gamers clearly demonstrates, the typical gamer is 30 years of age, often a parent and actively engaged in making decisions about what media is appropriate for themselves and their children (Brand et al, 2009). The question necessarily arises: why is such a consumer trusted to have access to R 18+ material in a cinema but be denied access to an R18+ video game they play on their computer?

Much of the regulation of media content in Australia has evolved in a distinctly jerry built manner that has often taken little account of empirical evidence about public attitudes or of expert studies of how consumers actually interact with media. The treatment of X-rated material in Australia is another case in point. This category of sexually explicit and non-violent material was first proposed in 1983 at a meeting of Australian commonwealth and state ministers responsible for censorship. They agreed that a new X-rated classification was warranted to accommodate the new video market which allowed adults to view sexually explicit material in their own homes. The original classification clearly excluded sexually violent material, child pornography and bestiality. Under the new scheme, all excluded material was to be refused classification (RC) and deemed illegal to sell or rent. The agreed plan was for all the state Attorneys- General to pass mirror legislation, also passed in the ACT and NT, that brought this classification into law. The reality was very different. Following political pressure applied by interest groups, no states followed through on the agreement. The result is that this material is available in the ACT and in parts of the Northern Territory but still not legally available for sale or rental in any Australian state. The more insidious result is that there is now a substantial unregulated black market in not only X rated, but also RC material in all states. The ban on this material has been in place since the mid-1980s, despite a wealth of research showing that up to 90 % of Australians, in common with international studies, have no concern about adults accessing non-violent sexually explicit material (McKee, Albury, Lumby, 2009)

The history of public policy and regulation around other media is not incidental to our focus in this report. The examples provided above demonstrate an issue germane to public policy issue: that the current system of classification and media content regulation has not been developed in an evidenced-based manner. It has historically treated various new media in a piecemeal fashion, been shaped by interest groups with scant reference to empirical evidence about what the majority of Australians think and want and by untested (though understandable) public fears about new media and new genres. From the consumer's point of view, the current system of media content regulation

now resembles a bowl of spaghetti. There is a raft of different systems that work simultaneously, and with little coherence, in relation to consumer concerns. These systems range across self-regulation (advertising and much of news and current affairs reporting), variable and inconsistent levels of regulation (popular magazines, videos, computer games) and strict criminal regulation (child pornography, incitement to terrorist activities). How the content of different media is regulated and understood depends largely on what original medium the content arrived in, on what political pressures were extant at the time of regulation and on what political and public debates have subsequently arisen.

In the relatively new but rapidly evolving online environment the disjuncture between these different and often contradictory regulatory systems are fracturing along numerous fault lines. As material from a wide variety of media- produced by professionals and amateurs – is increasingly published online, the issue of which original classification lens it should be seen through becomes increasingly vexed.

A compelling example of this is the public debate that erupted over a photograph of a 12 year old female taken by internationally known artist Bill Henson. Henson has been exhibiting his photographs for three decades and a substantial portion include nude subjects who are in their early adolescence. 65,000 people attended his retrospective exhibition hung in the Art Gallery of NSW in 2006. There was no attendant public outcry when his works were exhibited in a major gallery. In 2008, however, when the Roslyn Oxley gallery put the work in question on an invitation and it went up on the gallery's website a small group of media commentators ignited a public furore. Bill Henson's work was subsequently seized by police from the Oxley gallery and from public institutions, including the National Gallery of Australia. Many public commentators, including key politicians, denounced the work as a form of child pornography. ACMA was asked to classify Henson's images, on the basis that they had been posted online. They then referred them to the OFLC. After two weeks of heated public debate, a panel of five classifiers determined that the images should be given the lowest classification rating: G.

Despite the regulatory outcome, what the Henson affair alerts us to is the potential for the broad language of the current classification code and guidelines to be used to ignite public and political controversy. This is particularly the case under a mandatory rather than a voluntary filtering system. The diversity, intent and audience of online material multiplies this potential exponentially. The Henson affair was a case that clearly demonstrated how weeks of public furore, media attention and regulatory resources can be easily consumed by concerns about a small group of images or a body of text, understood as legal or innocuous elsewhere, if posted online. A much more pointed question that flows from this controversy is how well ACMA and the OFLC are prepared and resourced to deal with the innumerable controversies and challenges to online material that will potentially arise once filtering is mandatory and proceeds on the basis of a blacklist of content that, on the basis of the existing ACMA blacklist, will range across a broad variety of material.

The online environment brings together an unprecedented range of media formats, platforms and technologies. It does so in a way that allows consumers, of all ages, to both produce and consume media. It allows them to access content via their computers and phones. It also confronts them, as citizens, parents and public policy advocates, with an unprecedented array of content to negotiate. Understanding the risks and opportunities of this new media environment, as we argue on the basis of research outlined below, involves understanding how this environment changes the way in which people produce and consume media. Just as video technology fundamentally changed the context and the autonomy with which people consume documentary and entertainment media, so the rise of the internet, and particularly the Web 2.0 environment, have had a radical impact on the agency of media consumers and on how they consume and understand the media content they live with on a daily basis.

Online Media Content Regulation: Future Directions

A neglected aspect of public policy that needs to be considered in the internet filtering debate is the question of how we sensibly balance the risks posed by online material, particularly to children, and the opportunities provided to the broader community to participate in sometimes controversial debates, to access and debate material pertaining to political and social issues, and to allow reasonable adults to make decisions about what they consume or produce online.

The potential risks of an unregulated online environment to the public, and to children in particular, are real. In an Australian context, however, these debates have frequently run parallel to utopian

discussions of the educational and socially transformative potential of digital, online and mobile media without any recognition of how the two might relate. In thinking about how we frame online content regulation and public policy it is critical that we bring these two frames of reference into dialogue. Our understanding of risk must be balanced with an appreciation of the opportunities that this new media environment provides.

There is now a substantial body of work available on the risks and opportunities that the internet poses and provides to young people, particularly that gathered by the extensive and expert EU Kids Online research network. This project examined key European research on cultural, contextual and risk issues in children's safe use of the internet and new media across 21 countries. This work, cited in the influential and recent UK Byron Review [3] clearly suggests that public policy and regulation which is genuinely and empirically grounded in an ethic of care for children and young people will fail if it relies too heavily on a simplistic block and control strategy. It also strongly suggests that getting the balance right between regulation and the education of parents and young people about safe internet use is critical when it comes to the overall effectiveness of a broader protection strategy[4].

Both the EU Kids Online research and the Byron Review found that many parents are simply unaware of the risks to their children and/or feel unable to supervise their internet use. One of the clear risks of focusing disproportionate public policy attention and public resources on content regulation is that many parents will gain a false sense of security when it comes to the material their children encounter online. This risk is particularly high in a regulatory system that relies on a blacklist that, by its very nature, will only capture and represent a small sample of the wealth of online material of concern. As Dr Tanya Byron argued when launching her report: “A useful way for us all to think about this is to look at how we protect children in places of benefit and risk in the real (offline) world: public swimming pools. Here there are safety signs and information; shallow as well as deep ends; swimming aids and lifeguards; doors, locks and alarms. However children will sometimes take risks and jump into waters too deep for them or want to climb walls and get through locked doors – therefore we also teach them how to swim. We must adopt the same combination of approaches in order to enable our children and young people to navigate these exciting digital waters while supporting and empowering them to do so safely”[5].

In broader terms, focusing too much public attention and government policy on filtering material detracts from the need to promote and propagate the use of the internet much more widely, for many new purposes, including education, science, journalism, imaginative work, health and community-building. With the progressive roll-out of the National Broadband Network, public education is required on the use of the internet, not only on its dangers. The internet offers new opportunities for innovation, entrepreneurship and the growth of knowledge, and it extends these opportunities to the whole population.

Public policy, arguably, needs to promote a clear element of personal responsibility for navigating the online environment, just as people have to take responsibility for walking down the street and driving a car. The priority should be to balance maximum access to information with necessary regulation. The ‘opportunity cost’ incurred by mandatory ISP filtering of content is that this move potentially puts in jeopardy the economic, cultural and social benefits of population-wide internet use (which is a government priority via NBN and the Education Revolution), by focusing public attention on control, prohibition, and danger.

Young people, particularly those under 18, are accustomed to being told that their parents know best. To some extent the journey of adolescence is a conversation between parents and their maturing offspring about learning trust and respect for the other’s perspective, to the point where the children are themselves prepared to take on the responsibilities of adulthood and parenting. ABS research has repeatedly communicated the existence of this family-level negotiation around trust, autonomy and consequences when it comes to online access and activity, with negotiated changes in family rules as children mature. In the 2007 Australian study of 751 households, involving telephone interviews with parents and 1003 children of the households aged between 8-17 completing diaries, researchers found that: “Most parents trust their child’s judgement about the internet and, at least some of the time, leave it up to him/her to choose what is done on the internet (83%). This includes two-thirds who trust their child’s judgement all/most of the time (66%).”[6]

The Rudd government is committed to rolling out a national broadband network with world class speeds and capacity, with the aim of enhancing education, commerce and innovation. Applying a filter to an already slow system, prior to the NBN roll-out, will cripple it further. To apply the filter to the enhanced services available once the NBN is in place will reduce the benefit and increase the costs

of access necessarily excluding some from participation: arguably those who stand to benefit most. Coupled with the other reasons to rethink such a strategy, the NBN is an encouragement to regulators to see their role as an enabling one, and not as one which restricts and limits.

2.0 The Scope of Filtered Content

2.1 Introduction

As part of their pre-election platform, and since their election in 2007, the Rudd government has sought to address public concerns over internet content by signalling an intention to expand the regulatory approach to internet censorship by implementing a mandatory internet filtering program. This program would compel Internet Service Providers (ISPs) to block users from accessing websites deemed prohibited.

The proposed internet filter was promised as part of the government's election pledge regarding their *Plan for Cyber Safety Policy*, which also called for greater education, international cooperation, more research and additional law enforcement[7]. Concerning the planned internet filter, the Labor party's pre-election factsheet specified that, if elected, the government would:

> "Provide a mandatory 'clean feed' internet service for all homes, schools and public computers that are used by Australian children. Internet Service Providers (ISPs) will filter out content that is identified as prohibited by the Australian Communications and Media Authority (ACMA). The ACMA 'blacklist' will be made more comprehensive to ensure that children are protected from harmful and inappropriate online material.[8]

More specifically, in regards to the type of content that will be filtered, the factsheet states:

> "Labor's ISP policy will prevent Australian children from accessing any content that has been identified as prohibited by ACMA, including sites such as those containing child pornography and X-rated material.[9]"

In May 2008, the Government made good on its election promise and committed $125.8 million over four years to implement their proposed range of cyber safety measures[10]. According to the minister's website, "The policy reflects the view that ISPs should take some responsibility for enabling the blocking of 'prohibited' material on the internet, as they do in a number of western, developed countries.[11]" Similarly, in regards to the type of content that the government intends to blacklist, the Minister for Broadband, Communications and the Digital Economy has stated that ACMA will maintain a list of internet web sites, predominantly comprising images of the sexual abuse of children, which are defined as 'prohibited' under Australian legislation.

2.2 Current Government Policy

Understood broadly, the current federal government policy on cyber-safety acknowledges the importance of taking a comprehensive approach to the issue. The Minster responsible for Broadband, Communications and the Digital Economy, Senator Stephen Conroy, has been clear that "ISP filtering is no silver bullet" and stated that the government's $125.8 million cyber-safety policy includes an emphasis on education and information measures along with law enforcement, consultation with industry and community stakeholders and conducting further research. The critical issue, and one that is yet to emerge in the detail of the policy roll out, is where the balance will ultimately lie in terms of resourcing and policy focus.

Australia lags well behind its US, and particularly its European counterparts, when it comes to any detailed and original research into how children, families and adult consumers interact with and experience online material. Despite recent Federal funding of research on these matters, there is, in relative terms, still a paucity of broad and rich research on which our Federal Government can draw in responding to the increasingly pressing issue of what kind of material Australians, including children, produce and share online and how to protect them from genuinely inappropriate and illegal material. As technology and platforms rapidly evolve, the list of questions about how to understand and regulate new kinds of material grows. In such an environment, it is to be expected that government policy on cybersafety needs to be flexible enough to reflect this uncertain and evolving landscape.

In December 2009, Minister Conroy announced that the RC category would be used as a basis for mandatory filtering of the internet at ISP level in Australia. This submission addresses some public law and policy concerns about the efficacy of using that category as a basis for filtering.
The current proposal indicates that the list of mandatorily filtered sites will be based on the RC category. The key issue that arises here is that the RC category – developed primarily as a classification code for film and video – is a broad category which invites broad legal and quasi-legal interpretation.

2.3 The ACMA Blacklist

In 2007, the Broadcasting Services Act 1992 (BSA) was amended by the Communications Legislation Amendment (Content Services) Act. These changes, which came into effect in January 2008, significantly changed the face of online media content regulation in Australia. Working together, Schedule 5 of the BSA and a new Schedule 7 established a scheme to regulate internet content which is overseen by the Australian Communication and Media Authority.

Under the current co-regulatory scheme, internet content in Australia is regulated by a complaints based schemed managed by ACMA. Their response to a complaint depends on two factors: how the content is classified and where it is hosted. If it is hosted in Australia and deemed to be "prohibited content" it is subject to a takedown notice issued to the content host or ISP hosting the content. If it is hosted offshore, however, ACMA notifies IIA's Family Friendly filter providers accredited under its co-regulatory industry codes. They must update their filters upon such notification. Under the IIA codes, ISPs do not have to block access to URLs. Instead they must make an accredited filter or filtered services available to users. It is up to the users if they wish to use such filters or adopt other means to supervise their children online.

The mandatory filtering scheme proposed would remove this voluntary aspect of filtering in relation to content hosted offshore (the bulk of online material) and potentially result in a system where an extremely wide range of sites from MA 15+ material to RC material will be blocked.

Schedule 5 of the Broadcasting Services Act establishes the mechanism for ACMA to deal with prohibited content of the internet that is hosted offshore:

> This Schedule sets up a system for regulating certain aspects of the Internet industry.
>
> If the ACMA is satisfied that Internet content hosted outside Australia is prohibited content or potential prohibited content, the ACMA must:
>
> (a) if the ACMA considers that the content is of a sufficiently serious nature to warrant referral to a law enforcement agency--notify the content to an Australian police force;
>
> (b) notify the content to Internet service providers so that the providers can deal with the content in accordance with procedures specified in an industry code or industry standard (for

example, procedures for the filtering, by technical means, of such content).

Bodies and associations that represent the Internet service provider section of the Internet industry may develop industry codes.

The ACMA has a reserve power to make an industry standard if there are no industry codes or if an industry code is deficient.

The ACMA may make online provider determinations regulating Internet service providers.

If they believe that the content would be considered prohibited content if reviewed by the Classifications Board then ACMA would add it to the blacklist which is given to the filtering software providers.

Schedule 7 relates to content hosted in Australia. It provides:

A person may make a complaint to the ACMA about prohibited content, or potential prohibited content, in relation to certain services.

The ACMA may take the following action to deal with prohibited content or potential prohibited content:

(a) in the case of a hosting service--issue a take-down notice;

(b) in the case of a live content service--issue a service-cessation notice;

(c) in the case of a links service--issue a link-deletion notice.

Content (other than an eligible electronic publication) is ***prohibited content*** if:

(a) the content has been classified RC or X 18+ by the Classification Board; or

(b) the content has been classified R 18+ by the Classification Board and access to the content is not subject to a restricted access system; or

(c) the content has been classified MA 15+ by the Classification Board, access to the content is not subject to a restricted access system, the content does not consist of text and/or one or more still visual images, and the content is provided by a commercial service (other than a news service or a current affairs service); or

(d) the content has been classified MA 15+ by the Classification Board, access to the content is not subject to a restricted access system, and the content is provided by a mobile premium service.

Content that consists of an eligible electronic publication is ***prohibited content*** if the content has been classified RC, category 2 restricted or category 1 restricted by the Classification Board.

Generally, content is ***potential prohibited content*** if the content has not been classified by the Classification Board, but if it were to be classified, there is a substantial likelihood that the content would be prohibited content.

Bodies and associations that represent sections of the content industry may develop industry

codes.

The ACMA has a reserve power to make an industry standard if there are no industry codes or if an industry code is deficient.

The ACMA may make determinations regulating certain content service providers and hosting service providers.

Under existing legislation[12], prohibited online content is any content that would be rated "RC" and "X18+" or rated R18+ or MA15+ (for commercial services) and not subject to a restricted access warning system.

Refused Classification ("RC") content is any content which depicts:

- paedophilic activity
- child abuse
- instruction on drug use
- instruction on how to commit a crime
- bestiality
- sexual nudity involved minors
- excessive and frequent violence
- sexual activity involving minors or descriptions of it
- violence during sex
- fetish activity
- incest fantasies
- exceeds lower classification categories
- video games that exceed MA15+

X18+ Content is any content which depicts:

- Actual sexual intercourse between consenting adults
- The following is also strictly not permitted in this category:
    - No violence, sexual violence or coercion
    - Fisting
    - Candle wax
    - Bondage
    - Spanking
    - Golden showers
    - Depiction of people over 18 as minors

R18+ permits simulated sex but not visual material that shows people having actual intercourse, including penetration and oral sex.
In terms of the ACMA reviewers reaching a decision about the likelihood of material being prohibited content, Senator Conroy stated:

> ACMA content assessors have been members of the Classification Board and/or undergo formal training provided by the Classification Board. ACMA employs a number of former National Classification Board members within the Codes, Content and Education Branch who have a combined experience of close to 20 years at the Classification Board. This experience in conjunction with the formal training and regular referrals of content to the Classification Board help ensure consistency of classification decisions[13].

At the 30th of April 2009 there were 977 URLs on the ACMA blacklist[14]. Although the specific sites on the blacklist remain undisclosed, approximately 49% (479 URLs) of these websites were blocked on

the basis of an X18+, R18+ or MA15+ classification. Approximately 51% of the blocked sites were refused classification: 32% being for child depiction with the other 19% for unspecified other reasons.

This figure of 977 URLs has decreased from "around 1,110 URLs" which was the figure quoted on January 31st 2009[15]. Two of the blacklisted URLs contained images of dismembered foetuses. In the period 1 January 2008 to 31 December 2008, ACMA notified 1206 URLs relating to prohibited content and potential prohibited content hosted outside Australia to the makers of filtering software. Over the same period, ACMA removed 1048 items that no longer provided access to prohibited content or potential prohibited content. In the period 1 January 2007 to 31 December 2007, 1812 were notified. The figures stated above include any duplicate notifications resulting from multiple complaints about a specific URL during the period.

According to Senator Stephen Conroy[16], as at 30 November 2008, of the URLs on the blacklist:

(i) 0 relate to Internet content which is or would be classified MA15+;
(ii) 65 relate to Internet content which is or would be classified R18+;
(iii) 441 relate to Internet content which is or would be classified X18+;
(iv) 864 relate to Internet content which is or would be refused classification (RC);
(v) 674 relate to Internet content which is or would be refused classification in accordance with paragraph 1(b) of the Films Table of the National Classification Code because it depicts in a way likely to cause offence to a reasonable adult a person who is (or appears to be) a child under 18.

ACMA assessed and took action in relation to a further 778 items of overseas-hosted content, which were assessed as follows for the year ended 30 June 2008[17]:

Classification and description of online content	Number of items
MA 15+ – Violence	0
MA 15+ – Sex	0
MA 15+ – Themes	0
MA 15+ – Drug Use	0
MA 15+ – Nudity	0
MA 15+ – Language	0
R 18+ – Violence	0
R 18+ – Sex	6
R 18+ – Themes	0
R 18+ – Drug Use	0
R 18+ – Nudity	3
R 18+ – Language	0
X 18+ – Actual sexual activity	249
RC – Crime – promotion/instruction	2
RC – Violence – depiction	1
RC – Paedophilia – promotion/instruction	3
RC – Child – depiction	409
RC – Bestiality – depiction	10
RC – Sexual violence – depiction	13
RC – Sexual fetish – depiction	42
RC – Sexual fantasy – depiction	40
RC – Drug use – promotion/instruction	0
RC – Terrorist related material	0

RC – Publication	0
Cat 1 – Publication	0
Cat 2 – Publication	0

2.4 Online content regulation: the treatment of X and RC material

In order to determine whether content is permissible, ACMA relies on their interpretation of the censorship regulations as contained in the *Classification (Publications, Films and Computer Games) Act 1995 (Cth).* Internet content is regulated through the same classification system used for films (not the more relaxed publications classification system). Section 9 of the Act states that "subject to section 9A, publications, films and computer games are to be classified in accordance with the Code and the classification guidelines." The Code refers to the National Classification Code[18] (see appendix three and four). The legislative scheme also includes Guidelines for the Classification of Films and Computer Games 2005. The Guidelines were made under s 12 of the Act which empowers the Minister, (that is, the Attorney-General of the Commonwealth), with the agreement of participating State and Territory Ministers, to determine guidelines to assist the decision-maker in applying the criteria set out in the Code.[19]

The recent broadening of what may be considered prohibited content under the current voluntary filtering system raises more questions than it answers about what kind and scope of material may disappear from our computer screens in the near future and how the Classification Act will work in relation to Schedules 5 and 7. There is certainly a very real risk that reasonable adults will be prohibited from viewing a very wide range of content and that some content, which is legal offline, may become illegal to access online. For example, X18+ material can be legally purchased in the ACT or bought by mail order and viewed on a home DVD player. Under the new prohibited content scheme and mandatory filtering it appears very likely that all Australia adults would be denied the right to watch legally classifiable material on the internet, regardless of whether such sites were restricted to viewers over the age of 18.

The interpretation of the RC category, in particular, opens an array of potential issues given the breadth of the purpose and audience for online material. While the category is designed to refuse classification to material that the vast majority of Australians find abhorrent, including child pornography, bestiality and active incitement to acts of violence, there is also room to include material that sits in a much greyer area. The Classification Act does not detail criteria for determining what criteria should be applied in determining whether content is RC. Rather, it states that material be classified in accordance with the principles in the National Classification Code. These guidelines are extremely broad For example, in relation to publications, films and computer games one sections states that content will be RC if it deals with: sex, drug misuse, addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified". The term 'reasonable adult' could be understood as a means of limiting the range of material caught under the RC provision. A common sense reading would suggest that the views of the majority of Australians should be taken into account when determining whether a 'reasonable adult' would expect material to be refused classification. In practice, however, this has not been the case.

In Adultshop.Com Ltd v Members of the Classification Review Board [2007] FCA 1871 the court considered the test of "likely to cause offence to a reasonable adult" provision in the Code. The case was brought by Adultshop.com Pty Ltd. who applied to have the court review the Classification Review Board's decision to classify the sexually explicit film, *Viva Erotica*, as X18+. Although R18+ and X18+ are both restricted to persons above the age of 18, the effect of an X18+ rating means that the film cannot be legally sold or rented in Australia, other than in the Australian Capital Territory or the Northern Territory. In their original appeal to the Classification Review Board, Adultshop.Com had provided extensive expert witness material demonstrating that the great majority of Australians were not opposed to people over the age of 18 accessing non-violent sexually explicit films.

In bringing their suit against the Classification Review Board, the applicants contended that (1) the Guidelines are beyond the power of the Minister under s 12 of the Act because they dictate an X18+ classification without regard to "the standards of morality, decency and propriety generally accepted by reasonable adults" or the provisions of the Code; (2) if the Guidelines are valid, the Review Board applied them without regard to the merits of the case; (3) that the Review Board failed to give effect to a proper construction of the phrase "likely to cause offence to a reasonable adult"; (4) the Review Board's approach to the task led it to wrongly reject or discount certain survey and expert evidence called by Adultshop in support of its claim for an R18+ classification; and (5) Adultshop pointed to a finding made by the Review Board that there was extensive community consultation in the process of updating the Guidelines in 2005. Adultshop contended that the 2005 review of the Guidelines did not consider the X18+ classification and there was no community consultation on that issue.

In rendering their verdict, the court ruled that a reasonable adult was not a mechanistic test, nor was it to be applied in a majoritarian sense but rather as a collective interpretation of what society considered inappropriate or likely to cause offense. Because relevant legislation specifies that the Classification Board and the Classification Review Board are to be composed of a cross section of Australian society, the court ruled that the board's judgement as to the likelihood of certain content to cause offense is sufficient. In short, evidence about the views of what a large majority of adults think other adults should be allowed to see, read or watch is not taken directly into account in the current classification system. The OFLC, unlike its UK counterpart, has not conducted broad empirical research into community attitudes and the interpretation of the guidelines is de facto left to a small group of people who are said to represent and understand who the 'reasonable man'.

Another area, which deserves scrutiny in relation to material that is potentially caught under RC guidelines online, is the clause in the Code referring to materials that "promote, incite or instruct in matters of crime and violence". The classification guidelines were challenged in this regard in the NSW Council for Civil Liberties Inc v Classification Review Board (No. 2) [2007] FCA 896[20]. In this case, two publications, *Join the Caravan* and *Defence of the Muslim Lands* were assessed as 'RC' (Refused Classification) by the Classification Review Board. The grounds upon which the applicant claimed relief depended upon what it contended was the Review Board's erroneous application of the provisions of the *Classification (Publications, Films and Computer Games) Act 1995 (Cth)*. In particular, the applicant took issue with the Review Board's decision to classify the publications 'RC' on the basis of its finding that both publications 'promoted, incited or instructed in matters of crime or violence'.

The NSW Council for Civil Liberties Inc challenged the Classification Review Board's decision on four key points: (1) the meaning of the clause "promote, incite or instruct in matters of crime or violence" (2) that violence only refers to violence in Australia (3) that the review board failed to consider the elements of Section 101 of the Criminal Code and (4) the failure of the review board to consider the educational merits of the books.

The court found that in order to be refused classification under the Act, it is not necessary for a publication to solely stimulate or increase the likelihood for the recipient to commit violence, but that it should also be considered against the other provisions of the section of the Act which include "in such a way that the contents of the publication offend against the standards of morality, decency" and "... in a way that it is likely to cause offence to a reasonable adult." The judge also reasoned that "the publications 'may appeal to some disenfranchised segments of the community' and that 'the book was designed to encourage such people to take up arms and commit specific crimes against non-believers'" and that this was in fact "addressed to the audience, in Australia, to which the instructions and exhortations in the publications might appeal."

The Rabelais case[21] (Michael Brown & Ors v Members of the Classification Review Board of the Office of Film and Literature [1998] FCA 319) tested the "instruct in matters of crime" of the National Classification Code made under the *Classification (Publications, Films and Computer Games) Act*

1995 (Cth). The facts of the case pertained to the July 1995 edition of "Rabelais", the student newspaper of the La Trobe University Student Representative Council. The edition contained an article called "The Art of Shoplifting". Following complaints from retailers the article was found by the Commonwealth Office of Film and Literature to "*instruct in matters of crime*" and was subsequently refused classification thus prohibiting its distribution. In rendering its decision, the review Board considered what it described as "*the content, theme and tone of the publication*". It found the tone of the article to be instructional and hortatory. While it was claimed that the writing was not without humour, it lacked indicators that it was intended to be satirical. Its tone was considered to border on malicious. A majority of the Board concluded that the publication instructed in matters of crime and should be refused classification. A minority of the Board was of the opinion that “while the article was instructional in shoplifting the context of the publication with the nature of the crime was *such that the publication should not be refused classification*".

In their ruling, the three presiding justices concurred with the review board’s decision arguing that the assessment of whether a publication instructs in matters of crime must be read as whole and in context including the authors, the publication itself and the intended target readership. Only when the writing is of satirical or ironic character such that it negates the instruction by conveying the message that this is not to be taken seriously can it be found to be not in breach of the law. In this instance the court found that the language of the article did not convey such negation and that the review board had diligently followed the provisions of the Act in rendering its decision to refuse classification.

The cases referred to above strongly suggest that interpretations of what is deemed part of the extraordinarily catch-all RC category is one the courts are inclined to leave to the discretion of the Classification Board and Review Board. This is of real concern for an online environment in which the range, scope and purpose of material is far wider than even that encountered in films produced for entertainment purposes. Adding weight to this concern is that one of the factors that the Classification Act states must be taken into account when classifying material is “the persons or class of persons to or amongst whom it is published or intended or likely to be published”. This provision reflects a set of assumptions about material is generated and consumed which map onto the traditional media environment but which become almost meaningless in an era where material migrates rapidly across many contexts and where an enormous amount of content is generated by consumers themselves.

It is useful, at this point, to consider some hypothetical examples of material that could well be deemed RC and mandatorily filtered out of the Australian internet. Potential material that could feasibly be deemed RC on the basis of the current Classification Code includes:

- A site devoted to debating the merits of euthanasia in which some participants exchanged information about actual euthanasia practices.
- A site set up by a community organisation to promote harm minimisation in recreational drug use.
- A site designed to give a safe space for young gay and lesbians to meet and discuss their sexuality in which some members of the community narrated explicit sexual experiences.
- An art gallery website which includes photographs of naked children or adolescents taken by an established artist.
- A site discussing the causes of terrorism that published material exemplifying the beliefs of a terrorist organisation in order to ground the discussion of the causes of terrorism.
- A website in which survivors of child sexual abuse shared their experiences in a therapeutic context
- The online publication of a university newspaper which include an article about smoking marijuana

It is important not to be alarmist about the scope of material that will be caught under the RC or X18+ categories should mandatory filtering go ahead. It should certainly be noted that the Classification

Code clearly states classification decisions should give effect to the principle that “adults should be able to read, hear and see what they want”. How this injunction will be interpreted in relation to online material under a mandatory system, however, is open to broad interpretation.

2.5 Transparency and the right of appeal and judicial review

While it is clear that the government’s stated intention is the adoption of a mandatory internet filter to prevent access to prohibited content, it is unclear exactly how the mechanisms for this will be implemented. While preventing access to child pornography is clearly one of the primary reasons for implementing this filter, the current ACMA blacklist suggests that majority of websites (61%) on the blacklist fall outside this category of material.

A further critical concern is that, under the present system, the ACMA blacklist is not released for public comment and, while those hosting content which is put on the list have a right of appeal, content creators or other people who could be deemed to have standing in the matter, have no right of appeal. Without a right of appeal under public administrative law, there is also no avenue of judicial review. While there are well established precedents for exemption from administrative appeal – for instance if matters pertaining to national security or the broad protection of public morality – the offence to established democratic practice arguably increases exponentially in relation to the scope of content being filtered. Given the breadth of material that exists online and is potentially caught by the prohibited content provisions it seems to us, imperative, that at the very least the Federal Government commits to a clear system of appeal and judicial review of decisions and that there is transparency about what is put onto such a blacklist with rare exceptions.

3.0 The International Practice of Internet Filtering

3.1 Europe

The practice of internet filtering does occur in Europe; however, the vast majority of European filtering is voluntary. Internet service providers (ISPs), search engines and content providers engage in voluntary filtering on the understanding that by cooperating with the state, they can prevent further regulation in the future. Overall, ISPs are under no obligation to monitor the acceptability of internet content, but must filter unacceptable content once it is brought to their attention by the government, police, advocacy groups or the general public. In this way, the overwhelming majority of EU nations achieve the aim of blocking access to child pornography sites without resorting to legislation that their parliaments and peoples find coercive and objectionable. For most jurisdictions, it is illegal to possess or circulate child pornography (although the definition of 'child' varies, as does the age of consent).

Over the past few years, however, there has been a discernable move towards greater regulation among EU countries, with a particular focus upon child pornography websites. As discussed below, in June 2009 Germany legislated to filter such websites in the face of considerable opposition and controversy and having given firm guarantees that the filtering regime only applies to child pornography. In the subsequent general election, the ruling Christian Democrat Party lost power and the laws have not yet been implemented. This leaves Italy as the only EU country using mandatory filtering. Here, the Italian government filtered some online gambling websites whose operations are illegal, before subsequently mandating the filtering of online child pornography, and an on/off prohibition of *The Pirate Bay* peer-to-peer BitTorrent site. Overall, however, there is no wholesale mandatory filtering of internet content in any EU country as is proposed for Australia, and EU countries have adopted voluntary filtering regimes prior to any consideration of mandated filtering.

In terms of broader EU regulations, there is a general sentiment that voluntary ISP, search engine and content filtering should be preferred on the implicit understanding that it is through such voluntary cooperation with state authorities that further legislation will be unnecessary. The type of content filtered voluntarily relates to child pornography, racism, terrorism and sometimes gambling, as well as defamation. There is no obligation which requires ISPs to monitor internet traffic and they are largely protected from prosecution.

The regional policy is specified in the Electronic Commerce Directive 2000/31/EC[22]. In Article 12, the "mere conduct" exception prevents ISPs from being prosecuted for information 'merely' transmitted over their networks with the proviso that they (1) did not initiate the message (2) they did not select or modify the information and or (3) they did not select the intended recipient. Article 14 addresses liability of ISPs for hosting content – "ISPs will not be liable for hosting information, provided they do not have actual knowledge that the activity is illegal and, upon obtaining such knowledge, act quickly to remove it." Article 15 precludes ISPs from any general obligation to monitor content or data transmission on their servers[23].

In 1996, the European Council requested that the European Commission produce a "summary of the problems posed by the rapid development of the internet." The commission produced a report entitled "Illegal and Harmful Content on the Internet.[24]" This was followed by the drafting of a common framework for self regulation resulting in an Action Plan on Promoting Safe Use of the Internet[25]. The plan endorsed five major strategies to combat illegal and harmful content on the Internet:

- Promoting voluntary industry self-regulation and content monitoring schemes, including the use of hotlines for the public to report illegal or harmful content.

- Providing filtering tools and rating systems that enable parents or teachers to regulate the access of Internet content by children in their care, while allowing adults to access legal content.
- Raising awareness among consumers about services offered by industry to allow users to leverage the internet more fully.
- Exploring the legal implications of promoting the safer use of the internet
- Encouraging international cooperation in the area of regulation.

Overall, in the EU, the filtering regime requires interaction between governments, police, advocacy groups and the general public who identify instances of undesirable content, and the ISPs who voluntarily filter such content on the understanding that any failure to do so is likely to result in greater regulation of the sector. The definition of undesirable content tends to vary between countries but is broadly classified as content which is either illegal or harmful. There is general consensus on what is considered illegal or harmful and this includes: child pornography, human trafficking, racist material, material promoting terrorism and all forms of internet fraud. Harmful material is material that might offend the values and sentiments of others and could pertain to politics, religion or racial matters. In the countries that have moved to legislate some mandatory filtering, Germany and Italy, assurances were given that the mandated filtering is narrowly defined (see below).

3.1.1 Great Britain

Large scale voluntary internet filtering was spearheaded by the United Kingdom whose Cleanfeed program was launched in June 2004 through a commitment by BT, Britain's largest ISP. The program revolves around the filtering of content deemed inappropriate by its inclusion on a list of websites compiled by the Internet Watch Foundation (IWF). The IWF is a not-for-profit organisation that runs in collaboration with government, industry, the police and the public. The program is largely orientated towards the filtering of images of child abuse as established in the UK's *Protection of Children Act 1978*. ISPs, mobile network operators, content providers and search engines such as Google and Yahoo are provided with a copy of the list and are encouraged to remove access to websites listed on it. Those who attempt to access illegal content hosted overseas encounter an error message. For content hosted in the UK, the offending material is required to be taken down. Additional internet surveillance is conducted by the UK's Child Exploitation and Online Protection Centre. The law also enables police to forward the personal details of people who have accessed illegal content to banks, who will cancel their credit cards as a breach of service.

3.1.2 Germany

In June 2009, ignoring widespread opposition, the German parliament passed legislation to require ISPs to filter websites that contain child pornography. The secret filtering list was to be compiled by the German Federal Police and transmitted to ISPs daily, with a committee to monitor and check the list of banned sites[26]. In response to concerns that the filtering infrastructure could be used to block content such as online gambling, copyright violations and so on, Martina Krogmann, a government spokesperson and supporter of the legislation stated that "she is clearly opposed to a broadening of the scope, adding that the new law had been defined narrowly[27]". In September 2009, before the legislation could be implemented, the Christian Democrats lost power in a General Election and were required to enter into coalition with the Free Liberals to remain in government. As part of the negotiations it was agreed not to implement the legislation but instead to embark upon a year's trial of deleting websites hosting child abuse material, rather than blocking them[28].

3.1.3 Italy

During 2006 Italian ISPs were forced to block access to Web sites that offer online gambling by virtue of Financial Law (Law 266/2005). This gave the Amministrazione Autonoma dei Monopoli di Stato (AAMS or Autonomous Administration of State Monopolies, a part of the Ministry of Economy and Finances) the power to bring to the attention of ISPs instances in which gambling sites are operating without authorization from the AAMS itself. When brought to their attention by the AAMS, ISPs have the legal obligation to inhibit access to these sites by adopting appropriate technical measures to this end. The AAMS has compiled a list of websites that should not be accessed from Italian networks. This was list was implemented by ISPs through "hijacking" DNS communication and redirecting it to the DNS server of the AAMS. Users trying to access blocked websites were provided with a notice saying "pursuant to the decree of the AAMS of 7 February 2006 the requested website is not accessible because it does not have the necessary authorizations for collecting bets in Italy". The system, however, is easily circumvented by using a proxy server. Nevertheless, although technically avoidable, the blacklist is apparently still applied by Italian ISPs[29]. In January 2007 the Italian government passed a decree requiring ISPs to block access to child pornography websites after being notified of such websites by the National Centre against Child Pornography[30]. In 2008, using commercial law, an Italian court ordered ISPs to block access to Swedish BitTorrent site *The Pirate Bay* which facilitates the illegal exchange of copyright material. Successfully overturned on appeal, the original ruling was upheld by the Italian Supreme Court and the situation is still in flux.

3.1.4 Sweden and Norway

The Norwegian government has considered blocking access to “foreign gambling, websites that desecrate the flag or coat of arms of a foreign nation, that promote hatred towards public authorities, contain hate speech or promote racism, offensive pornography sites, and peer-to-peer sites that offer illegal downloads of music, movies or television shows.[31]” However, this proposal was not adopted by the government.

A filtering system was announced in 2004 as collaboration between Telenor, the leading Scandinavian telecom company and KRIPOS, the Norwegian National Criminal Investigation Service. This system was designed to prevent access to child pornography at ISP level. The blacklisted URLs were based on a list compiled by KRIPOS. In May 2005, Telenor and the Swedish National Criminal Investigation Department announced that a similar filtering system had been introduced for all Telenor’s customers in Sweden[32].

Overall, however, in both Sweden and Norway, filtering occurs on a voluntary basis with no sanction for noncompliance. Each ISP determines the scope of blocking access[33].

3.1.5 Ireland

Irish ISPs generally self-regulate in regards to child protection. When illegal content is identified, ISPs must take reasonable measures to remove that content from public access. ISPs are only required to respond to illegal content by removing illegal content hosted on their systems[34].

3.1.6 Denmark and Finland

Since 2005, Finland has maintained a voluntary program to restrict access to child pornography websites. The Finnish police maintain a list of sites; however, there is no obligation for ISPs to block these sites. The same voluntary ISP-end filtering program is implemented by Denmark[35].

3.2 United States and Canada[36]

The application of internet filtering regulations differs in both Canada and the United States. Neither Canada nor the United States adopts a mandatory internet filtering system; nevertheless, regulation exists in both countries that revolves around four key issues: child-protection and morality, national security and computer security.

In the US, the government has tried several times to legislate child protection; however, government mandated attempts have been struck down by the courts on the grounds of the First Amendment, regarding freedom of speech and freedom of the press. The first piece of legislation was the United States Communication Decency Act (CDA). The provisions of this Act were to "criminalise the transmission of indecent material to persons under eighteen and the display to minors of patently offensive content and communications." Civil libertarians challenged this law with the court finding that the bill's uses of "indecent" and "patently offensive" were so vague that enforcement would have violated the First Amendment. This was later affirmed by the Supreme Court. Following this defeat, a second piece of legislation was introduced - which became known as the Child Online Protection Act (COPA). This legislation was directed at material considered "harmful to minors." Again, however, the courts enjoined this legislation on first amendment grounds for the reason that to accurate identify "indecent" material and pre-emptively block it, would have required ISPs to filter arbitrarily and extensively in order to avoid criminal liability. In 2000, The Children's Internet Protection Act (CIPA) was passed requiring public schools and libraries to implement Internet filtering technology in order to receive federal E-Rate funding. The law required that in order for a school or library to receive federal funds for internet access they must demonstrate to the FCC that it has installed or will install filtering technology. The technology must filter content that is deemed to be obscene, child pornography, or material harmful to minors. The choice as to which content fulfils this criteria is at the discretion of filtering technology developers who make such choices during the development phases of the technology. The law has been upheld by the Supreme Court following challenges on first amendment grounds.

Overall, internet filtering in the United States is largely left to private manufacturers that compete for market share in internet filtering technologies. Those required to block content, such as schools and libraries, can select from a range of different filters each with different approaches. Some include whitelists of pre-approved sites whereas the majority use blacklists which are generated through automated screenings of the web. The decision as to what to filter rests in the purview of the filter manufacturers in the first instance, and then the individual PC users who implement that filtering software.

Canadian practice in relation to internet filtering is orientated towards government facilitated industry self-regulation. Private parties are required to self-regulate with the encouragement of the government under the threat of future legislation or potential legal action. The Criminal Law Amendment Act of 2001 made it a crime to access and distribute child pornography online. However, the law includes a proviso that ISPs are not required to assess the legality of content or to take action unless there is a judicial determination as to the legality of the content. Even so, the law does require that ISPs must provide all information required regardless of its content in return for immunity over the nature of its content. Therefore, ISPs cannot choose which information to pass on to law enforcement officers and which information to restrict access to. Section 36 of the Canadian Telecommunications Act indicates that without the approval of the Canadian Radio-Television and Telecommunications Commission (CRTC), a Canadian carrier "shall not control the content or influence the meaning or purpose of telecommunications carried by it to the public[37]."

In November 2006, Canada launched Project Cleanfeed, a voluntary collaboration between Bell, Bell Aliant, MTS Allstream, Rogers, Shaw, SaskTel, Telus, and Vidéotron Canada[38]. Although the government was not directly involved, they did indicate their approval. The processes involved in

Project Cleanfeed are as follows: A member of the public or an authority notifies assessors when questionable images or content are found online. Two analysts assess that content and decide either to reject or approve it. If the site is to become listed, the URL is added to the Cleanfeed distribution list which is sent out to all ISPs who have agreed to voluntarily block sites on the list. This also prevents the ISPs from having to evaluate the URLs themselves, which would be considered illegal. ISPs will only block specific URLs and not a generic IP address to prevent overblocking, since overblocking could be illegal under the Telecommunications Act. Additionally, given that accessing child pornography is illegal in Canada it does not infringe on the right of access or free speech under the Canadian Charter of Rights and Freedoms. Similarly, however, it is also illegal to publish the list of blocked sites because it is considered illegal to provide access to child pornography. These different considerations raise a number of controversial issues for project Cleanfeed such as: (1) it has not received authorisation from CRTC (2) the list needs to be keep undisclosed (3) the procedure for appealing the blocking of a site may have implications for anonymity.

3.3 New Zealand

Overall, New Zealand's implementation of internet filtering is much less onerous than that proposed for Australia. New Zealand law does define offensive content, which includes hate speech, and such content can be investigated by the Department of Internal Affairs. Upon investigation, the Department of Internal Affairs submits non-classified material to the Office of Film and Literature Classification for a ruling. However, unlike in Australia, there is no explicated mechanism under which the government can issue a takedown notice. The New Zealand system relies instead on a classification system and while there is no direct online regulation of content, officials agree that the Films, Videos and Publications Act (1993) applies equally to objectionable online material. New Zealand law defines objectionable material as any material that "describes, depicts, expresses or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good." More specifically, any material that promotes "the exploitation of children, or young persons or both, for sexual purposes; or the use of violence or coercion to compel any person to participate in, or submit to, sexual conduct, or sexual conduct with or upon the body of a dead person; or the use of urine or excrement in association with degrading or dehumanising conduct or sexual conduct, or bestiality, or acts of torture or the infliction of extreme violence or extreme cruelty" is considered to be objectionable.

In July 2009, the New Zealand government's Department of Internal Affairs (DIA) announced that they would be introducing software for voluntary use by ISPs which would form the basis of 'The Digital Child Exploitation Filtering System.' The software is explicitly restricted to blocking sites which provide access to child sexual abuse images. An independent committee is to oversee the operation of the filter and anyone who believes a site may be wrongly blocked can request a review of the filter. Keith Manch, Deputy Secretary of the Department, commented that "Joining the filtering programme is voluntary and if any ISP subsequently is unhappy it will be able to withdraw. This is another way of ensuring that the Department gets the filter right."[39] There is some indication that ISPs servicing over 90% of NZ's internet market are willing to adopt the system.[40] A period of public consultation closed in September and the New Zealand government's intentions regarding the system are spelled out in terms of services provided by the DIA.[41] It is anticipated that the System will be operational early in 2010.

3.4 Reporters Without Borders

Reporters Without Borders (RWB) provides a list of countries that they consider to be enemies of the internet[42]. Enemies of the internet are those countries which "prevent[ed] Internet users from obtaining news seen as 'undesirable'. All of these countries mark themselves out not just for their

capacity to censor news and information online but also for their almost systematic repression of Internet users.[43]" This list comprises twelve countries[44]:

- Burma
- China
- Cuba
- Egypt
- Iran
- North Korea
- Saudi Arabia
- Syria
- Tunisia
- Turkmenistan
- Uzbekistan; and
- Vietnam

The report on enemies of the internet also includes a further eleven countries which RWB considers to be "under surveillance." Countries under surveillance are considered by RWB to "alternate between censorship and harassment of Internet users." Australia is the only western nation included in this list of countries, on the grounds of its intention to "force all service providers to filter private Internet connections in each home to remove all 'inappropriate' content". The list comprises:

- Australia
- Bahrain
- Belarus
- Eritrea
- Malaysia
- South Korea
- Sri Lanka
- Thailand
- United Arab Emirates
- Yemen
- Zimbabwe

3.5 Open Net Initiative (ONI) Study of Countries with Pervasive or Substantial Filtering

ONI is a global collaboration of four leading universities to monitor freedom on the Net. It is supported by Harvard, Toronto, Cambridge and Oxford Universities and researches and reports on a country by country and regional basis. While some western countries engage in selective filtering of certain types of content, usually within a cooperative and voluntary framework, a number of countries worldwide enforce more widespread forms of internet filtering. The following table[45] indicates how countries engaged in pervasive or substantial censorship implement such internet censorship, for example through centralised control of the internet backbone, or decentralised ISP level filtering. The level of consistency of the filtering efforts is also noted, as is whether the government conceals that it is filtering content, and the level of government transparency and accountability. If the proposed Australian ISP-level filter were to be implemented then it would be appropriate for Australia to occupy a place on this table as indicated. (In the absence of a mandatory filter, Australia is not currently included in this table). Regarding a possible Australian entry, a 'D' in the first column indicates that the filtering occurs at the level of the ISP. The second column indicates that there will be consistency

across users since all ISPs will be required to filter up to 10,000 named sites. Australians do not yet know whether users attempting to access a blocked site will be told that the site is blocked but it is clear that the introduction of a filtering regime will be acknowledged publicly. Also evident, from the regulations regarding the ACMA blacklist, is that the specific details of prohibited sites will be kept secret and thus beyond public scrutiny and debate.

	Locus	Consistency	Concealed Filtering	Transparency and Accountability
Australia*	D	High	No	High
Azerbaijan	D	Low	No	Medium
Bahrain	C	High	Yes	Low
China	C and D	Medium	Yes	Low
Ethiopia	C	High	Yes	Low
India	D	Medium	No	High
Iran	D	Medium	No	Medium
Jordan	D	High	No	Low
Libya	C	High	Yes	Low
Morocco	C	High	Yes	Low
Myanmar	D	Low	No	Medium
Oman	C	High	No	High
Pakistan	C and D	Medium	Yes	High
Saudi Arabia	C	High	No	High
Singapore	D	High	No	High
South Korea	D	High	No	High
Sudan	C	High	No	High
Syria	D	High	No	Medium
Tajikistan	D	Low	No	Medium
Thailand	D	Medium	No	Medium
Tunisia	C	High	Yes	Low
United Arab Emirates	D	Low	No	Medium
Uzbekistan	C and D	High	Yes	Low
Vietnam	D	Low	Yes	Low
Yemen	D	High	No	Medium

***Australia** is not currently included in this list. This inclusion here indicates how Australia's filtering regime is likely to be categorised were the proposed mandatory filter to be introduced.

Locus: C = centralised (internet backbone), D = decentralised (implemented by ISPs)

Consistency = the variation in filtering across different ISPs where applicable

Concealed Filtering = efforts to conceal the fact that filtering is occurring or the failure to clearly indicate when it occurs

Transparency and accountability = overall level of openness in regards to the practice of filtering.

Similarly, the table below[46] breaks into categories the type of internet censorship that countries actively pursue in terms of whether the material affected constitutes political censorship, social censorship, conflict and security censorship or the censorship of internet tools. According to the ONI, political censorship includes content that expresses views in opposition to those of the current government, or is related to human rights, freedom of expression, minority rights, and religious

movements[47]. Social content is content related to sexuality, gambling, and illegal drugs and alcohol, as well as other topics that may be socially sensitive or perceived as offensive[48]. Conflict and security content refers to armed conflicts, border disputes, separatist movements, and militant groups[49]. Internet tools refers to web sites that provide e-mail, Internet hosting, search, translation, Voice over Internet Protocol (VoIP) telephone service, and circumvention methods[50].

	Political	Social	Conflict and Security	Internet Tools
Australia*	•	•	-	-
Azerbaijan	•	-	-	-
Bahrain	••	•	-	•
Belarus	O	o	-	-
China	•••	••	•••	••
Ethiopia	••	•	•	•
India	-	-	•	•
Iran	•••	•••	••	•••
Jordan	•	-	-	-
Kazakhstan	O	-	-	-
Libya	••	-	-	-
Morocco	-	-	•	•
Myanmar	•••	••	••	••
Oman	-	•••	-	••
Pakistan	•	••	•••	•
Saudi Arabia	••	•••	•	••
Singapore	-	•	-	-
South Korea	-	•	•••	-
Sudan	-	•••	-	••
Syria	•••	•	•	••
Tajikistan	•	-	-	-
Thailand	•	••	-	•
Tunisia	•••	•••	•	••
United Arab Emirates	••*	•••	•	••
Uzbekistan	••	•	-	•
Vietnam	•••	•	-	••
Yemen	••*	•••	•	••

***Australia** is not currently included in this list. This inclusion here indicates how Australia's filtering regime is likely to be categorised were the proposed mandatory filter to be introduced

- ••• Pervasive Filtering
- •• Substantial Filtering
- • Selective Filtering
- o Suspected Filtering
- - No evidence of Filtering
- * According to website: http://opennet.net/research/profiles/

Given the way in which Australia treats radical Muslim materials it might earn • 'selective filtering' for Political material. Similarly, the way Australia proposes to filter legal but restricted content and materials such as those provided by Exit Australia, the voluntary euthanasia and assisted suicide society, indicates that the Social category might also become • 'selective filtering'. According to the definitions above, there is little evidence of 'conflict and security' filtering other than that already identified in the 'political' category, while there is also little evidence currently of the blocking of internet tools. Such practices may emerge, however, when patches are created to circumnavigate the ISP-level filters.

Even at the level of 'selective filtering', such a practice could place Australia in the uncomfortable company of some comparatively restrictive regimes. The list created comes from a table in the ONI book 'Denied Access' (2008), with ratings checked against the current website[51]. This indicates that UAE[52] and Yemen[53] may have moved from being classified as selective filterers of political content of the internet to nations that use substantial filtering. According to the combination of the book and the website, countries that operate selective filtering of political content comprise: Azerbaijan, Jordan, Pakistan, Tajikistan and Thailand. Those that practice selective filtering of social content are: Bahrain, Ethiopia, Singapore, South Korea, Syria, Uzbekistan and Vietnam.

With regards to the specific countries that operative selective filtering of political content, the Open Net Initiative comments:

Azerbijan: "Azeri law does not require mandatory filtering or monitoring of Internet content … Anecdotal accounts claim that filtering of specific Web sites occurs, which is seemingly the result of informal requests to ISP managers by state officials from the Ministry of National Security, Ministry of Communications and Information Technologies, or the Presidency. These instances have been infrequent, and the resulting public outcry has led to a swift unblocking of the affected sites."[54]

Jordan: "ONI conducted in-country tests in Jordan on four ISPs: Jordan Telecom, Batelco, Orange, and Linkdotnet. Only arabtimes.com, a U.S.-based online newspaper often critical of Arab leaders, was found to be blocked."[55]

Pakistan: "Currently Pakistanis have unimpeded access to most sexual, political, social, and religious content. However, the Pakistani government continues to use repressive measures against antimilitary, Balochi, and Sindhi political dissidents, and it blocks Web sites highlighting this repression. The government also filters high-risk antistate materials and blasphemous content."[56]

Tajikistan: "Tajikistan does not have an official policy on Internet filtering. However, state authorities have been known to restrict access to some Web sites at politically sensitive times by communicating their "recommendations" to all top-level ISPs."[57]

Thailand: "ONI conducted testing after the [Thai] coup on three major ISPs: KSC, LoxInfo, and True. Of the sites tested, only a small percentage was actually blocked. The Thai government does implement filtering and primarily blocks access to pornography, online gambling sites, and circumvention tools. Outside these categories, only a few sites were blocked by all three ISPs." [58]

If a country such as Australia were to operate a mandatory filter at the level of the ISP, with a capacity to block up to 10,000 sites, with a secret blacklist less than 1/3 of which is child pornography (30 April 2009)[59], but which includes political/extremist publications such as *Join the Caravan* and *Defence of the Muslim Lands* among the materials refused classification, it might quite possibly find itself classified alongside the countries listed, judged as engaged in selective filtering of political content.

A similar picture emerges when considering countries that engage in selective filtering of social content. It should be noted here that while Bahrain was categorised in print as a selective filterer of social content, it is deemed on the ONI website to use 'pervasive filtering'[60]. Countries classified in both print and on the web as selective filterers of social content are: Ethiopia, Singapore, South Korea, Syria, Uzbekistan and Vietnam. The ONI website offers specific country comments:

Ethiopia: "Ethiopia's current approach to filtering can be somewhat spotty, with the exception of the blanket block on two major blog hosts … ONI conducted testing on Ethiopia's sole ISP, the ETC, in 2008 and 2009. The ETC's blocking efforts appear to focus on independent media, blogs, and political reform and human rights sites, though the filtering is not very thorough."[61]

Singapore: "The government of the Republic of Singapore engages in minimal Internet filtering, blocking only a small set of pornographic Web sites as a symbol of disapproval of their contents."[62]

South Korea: "ISPs have become increasingly responsible for policing content on their networks. In 2001, the state promulgated the 'Internet Content Filtering Ordinance', reportedly requiring ISPs to block as many as 120,000 Web sites on a state-compiled list, and requiring Internet access facilities that are accessible to minors, such as public libraries and schools, to install filtering software."[63]

Syria: "ONI testing results indicate that Syria's Internet filtering regime has increased the scope and depth of targeted content. Censorship has been extended to include high profile sites such as the video sharing Web site YouTube, the social networking Web site Facebook, and the online shop Amazon.com."[64]

Uzbekistan: "The 2002 Law on Principles and Guarantees on Access to Information reserves the government's right to restrict access to information when necessary to protect the individual 'from negative informational psychological influence' … ONI detected a consistent and substantial filtering system that employs blockpages as well as re-directs to other Web sites … Selective filtering of Web sites displaying social topics was also detected, including sites with religious, extremist, porn, gay, and lesbian content."[65]

Vietnam: "Surprisingly, Vietnam does not block any pornographic content (though it does filter one site ONI tested with links to adult material), despite the state's putative focus on preventing access to sexually explicit material. The state's filtering practices are thus in obvious tension with the purported justification for these actions."[66]

Although other countries do not seem to target pressure groups such as EXIT, Australia's filtering of such sites along with its stated intention to block, for example, MA15+ content which seems to fail restricted access tests, would likely see it categorised as at least a selective filterer of social content.

3.6 Conclusion

Although there are indications of a growing preparedness to filter content in some European nations, mandatory filtering at present is very restricted and very targeted. Germany and Italy have both legislated to block access to child pornography, while Italy also prevents access to some online gambling sites. It is clear that liberal democracies tend to adopt voluntary regulatory approaches that focus on narrowly defined segments of undesirable content – usually child pornography. The United States, New Zealand, Canada and Great Britain have implemented voluntary programs that delegate

the choice of what to filter and how to filter it to end-users, individual ISPs and/or filtering software vendors. The identification of undesirable internet content is usually retained under the purview of a not-for-profit organisation who maintains a blacklist through collaboration with the police, advocacy groups, the government and the general public. The majority of European ISPs filter content "voluntarily" under the implicit understanding that failure to do so will force the government to implement strict regulatory frameworks.

Given this general European and north American approach to the regulation of the internet, Australia is the only western country identified by the international NGO Reporters Without Borders (RWB) as being 'under surveillance' as a potential 'enemy of the internet'. Australia's proposed filtering regime, operating at the level of the ISP to "force all service providers to filter private Internet connections in each home to remove all 'inappropriate' content" is offered as the main justification for RWB setting it apart in this way from all other liberal democracies. Since Australia has been singled out in this way by RWB for discussing the possible introduction of an ISP-level filter, its implementation would be likely to have significant ramifications for Australia's place in lists which monitor internet freedoms, such as those compiled by the Harvard, Toronto, Cambridge and Oxford University-sponsored Open Net Initiative. An examination of ONI's evaluation of countries which engage in filtering of social and political content, which do not currently include any western liberal democracies, indicates that an Australian mandatory filter would probably qualify the country for inclusion as engaging in 'selective filtering' of social and political content. This is on the basis of material already judged by Australian courts to be legitimately repressed, although it is clear that there is no intention that the public should be allowed to scrutinise the up to 10,000 sites to be blocked by Australia's mandatory ISP filter, should it be enacted.

As a parting observation, using the printed charts from the Feb 2008 ONI-based publication, *Access Denied*, and comparing these with the online materials current in Nov 2009, of the 14 countries which were judged as using selective filtering of political or social content in the book, two had since been re-classified as using 'substantial filtering' while a third had become labelled as a 'pervasive' filterer of online material. All changes over this comparatively short time frame had been in the direction of greater repression of material: none of the regimes indicated had become more liberal.

4.0 Public Interest Matters: A Summary

A range of public policy issues and matters of public interest arise from the matters we have considered above.

Scope of Content

What types of content will be filtered under a centralised mandatory internet filtering program? Will it just focus on child pornography or will broader categories also be included?

A pressing issue that needs to be resolved concerns the scope of content that is likely to be filtered under a mandatory internet filtering regime. As discussed above, according to the current Federal Government's statements the proposed policy has been framed as an approach to prevent the dissemination of child pornography. The question then arises of whether the Federal Government should not simply define and circumscribe in law the actual categories of material to be filtered, with child pornography being the highest priority category.

While this may be considered acceptable where filtering is opt-in by an end user (or parent for family computers), under a mandatory filtering regime this would result in capturing material that is clearly legal but restricted in availability (off the internet) through classification restrictions. Therefore, the following questions need to be resolved:

- Will the types of content that are to be blocked under the mandatory internet filter be defined in new legislation or will this remain under the purview of existing classification legislation?

- How will content which is considered legal content but potentially offensive to minors be dealt with?

Balancing rights to free speech

Unlike all other liberal democratic nations, Australia has no explicit protection of the rights to free speech or access to information. Whereas in the United States, the first amendment has been used to strike down mandatory internet filtering laws; no such protections are afforded to Australians either through the constitution or through subsequent Acts of Parliament. The Labor party upon election in 2007 indicated that they would provide a comprehensive review of human rights issues in Australia, and that report was delivered in September 2009[67]. The *National Human Rights Consultation Report* 2009[68] references findings from a Colmar Brunton survey of Australians and their beliefs about human rights issues in Australia. This focuses on which rights Australians believed should be protected. One of the findings of this research was that those surveyed believed that freedom of speech was one of the most important rights, and that people considered it to be one of the "absolutes."[69] The committee recommended that amongst other things:

> ...the Federal Government immediately compile an interim list of rights for protection and promotion, regardless of whether a Human Rights Act is introduced. The list should include rights from the International Covenant on Civil and Political Rights as well as the following rights from the International Covenant on Economic, Social and Cultural Rights that were most often raised during the Consultation: the right to an adequate standard of living (including food, clothing and housing); the right to the highest attainable standard of health; and the right to education.[70]

If the government were to implement a mandatory filter, the extent to which this would conflict with the right to freedom of speech and access to information is uncertain although it is clear that the scope of the content caught would certainly increase the level of the conflict. Australia is a signatory to the UN Declaration of Human Rights which explicitly upholds the right to freedom of opinion and expression, as well as access to information (see below). Similarly the International Covenant on Civil and Political Rights (ICCPR), in which Australia is also a participant, states that "everyone shall have the right to hold opinions without interference and everyone shall have the right to freedom of expression[71]." These rights are often used by courts as constituting basic human rights. However, the statements are broad in meaning and also carry with them certain "special duties and responsibilities." Article 20 of the ICCPR states that restrictions need to be placed on communications intended to promote or incite war or "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence."

Article 17(2) states that "(1) no one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation; and (2) Everyone has the right to the protection of the law against such interference or attacks.[72]" Article 19 (2) states that:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.[73]

However, this is followed by article 19(3) which qualifies this right:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order, or of public health or morals.

In this sense, while the state has the obligation to protect the inalienable human right of freedom of speech and freedom of association, there is also an obligation to protect people from defamation and also protect national security, the public order and uphold public morals. It is on such grounds that most states which engage in internet filtering have sought to justify its use. The question is not so much whether states have a right to protect citizens from a degradation of public morals in the form of preventing access to child pornography or offensive material, but whether mandatory internet filtering is the most appropriate method with which to pursue this aim. Likewise, in the case of defamation and hate speech, the state is in fact obligated under international treaties such as UNDHR and ICCPR to uphold the rights of citizens to be protected from communication that undermines the rights of others. As stated by Zittrain and Palfrey (2008)[74]:

> The strongest argument for [an] internet filter is that it is a legitimate expression of the sovereign authority of states to prevent its citizens from unfettered access to the internet when doing so would adversely affect local morals and norms…A state has the right to protect the morality of its citizens, the arguments goes, and unfettered access to and use of the internet undercuts public morality in myriad ways. Many regimes, including those in Western states, have justified online surveillance of various sorts on the grounds of ordinary law enforcement activities, such as the prevention and enforcement of domestic criminal activity. Most recently, states have begun to justify online censorship and surveillance as a measure to counteract international terrorism. More simply, internet filtering and surveillance is an expression of the unalienable right of a state to ensure its national security.

In regards to internet filtering there is a fundamental conflict between protecting the rights to freedom of expression and access to information and upholding the state's obligations of maintaining national security and protecting public morals. The conflict stems from the nature of the technology and the potentially capricious and arbitrary manner in which regulations could be applied. There is no evidence to suggest that any state has ever managed to regulate a foolproof system in which underblocking or overblocking does not occur[75].

Similarly, there is evidence to suggest that all systems can be evaded by some internet users and that no technical means of filtering can be implemented that prevents such evasion. The question as to whether overfiltering or underfiltering is preferable remains a matter that individual states must decide. While it seems that many states have delegated responsibility to individual ISPs, this question raises two important public policy questions:

- **In the case of overfiltering**: is the potential of unwittingly restricting the lawful expression of a citizen and their access to information so offensive to fundamental human rights that it conceivably constitutes a breach of Australia's international obligations?

- **In the case of underfiltering**: is the inexact implementation of internet filtering satisfactory given that much content which may be deemed grossly offensive to public morals will not be

successfully blocked and may also leave parents and teachers with a false sense of security when it comes to children accessing the internet.

Transparency

How transparent will the regulatory approach be? Will citizens be made aware if certain websites have been prohibited?

While it is clear that the government's stated intention is the adoption of a mandatory internet filter to prevent access to prohibited content, it is unclear exactly how the mechanisms for this will be implemented. While preventing access to child pornography is clearly one of the primary reasons for implementing this filter, the current ACMA blacklist suggests that majority of websites (61%) on the blacklist fall outside this category of material.

A further critical concern is that, under the present system, the ACMA blacklist is not released for public comment and, while those hosting content which is put on the list have a right of appeal, content creators or other people who could be deemed to have standing in the matter, have no right of appeal. Without a right of appeal under public administrative law, there is also no avenue of judicial review. While there are well established precedents for exemption from administrative appeal – for instance if matters pertaining to national security or the broad protection of public morality – the offence to established democratic practice arguably increases exponentially in relation to the scope of content being filtered. Given the breadth of material that exists online and is potentially caught by the prohibited content provisions it seems to us, imperative, that at the very least the Federal Government commits to a clear system of appeal and judicial review of decisions and that there is transparency about what is put onto such a blacklist with rare exceptions.

As of the time of writing, the following questions about how internet filtering will proceed need to be resolved:

- Will the blacklist be made publicly available? If not, is there a potential cause of action for discovery or redress?
- Will content providers or other citizens be able to appeal the blocking of individual websites? How will such an appeals process be facilitated?
- Will there be a system of judicial review?

Peer-to-Peer Content

The growth of peer-to-peer and user generated content with the advent of Web 2.0 generates some additional regulatory challenges for the Federal Government. A mandatory filter will not catch illegal material disseminated through these channels. Indeed, one of the key challenges in identifying those who disseminate and consume child pornography is that much of it is not openly displayed on websites but is exchanged in a covert and encrypted manner via bulletin boards. More recently, evidence is emerging that child pornography is also increasingly being covertly housed on third party websites through the use of malware bots. The international evidence clearly suggests that the majority of child abuse prevention resources need to be targeted towards coordinated policing of those who manufacture and share child abuse materials, often in contexts where they are involving their own family members or children known to them[76]**.** A key issue that needs consideration is that even if abhorrent and inappropriate content is identified and notified to ACMA, or another appropriate authority, there is strong evidence that the creators of such material will simply upload or download the same material in a different online context once detected.

International Implications

The proposed filtering regime has a number of implications for Australia in an international context. Firstly, the proposal would set Australia apart from other western liberal democracies that have opted for a transparent, voluntary filtering regime that involves interactions between governments, the police, advocacy groups, ISPs, not-for-profit organisations and the general public in determining how to counteract access to undesirable content. This approach has been successfully applied in the United States, Canada, the United Kingdom and New Zealand. While it is clear that in Europe there is a trend towards greater regulation of internet content, especially in Italy, most European countries still maintain a voluntary regulatory approach.

Australia's treaty obligations under the United Nations Declaration for Human Rights and the International Covenant on Civil and Political Rights (ICCPR) clearly establish Australia's commitment to freedom of speech and expression. While it is clear that if the mandatory internet filter were to focus narrowly upon instances of child pornography it could hardly be consider a breach of Australia's international treaty obligations, the implementation of a non-transparent, a widely scoped filtering system that captures not only child pornography but legal content could constitute a fundamental departure from Australia's commitments.

Balancing Risks with Responsibility

A mandatory policy also raises the issue of how we balance the need for the government to protect children and teenagers from harmful material with the importance of involving parents and teachers in helping children negotiate the online environment and make decisions about what is age appropriate. International research has repeatedly shown the importance of involving parents, educators and children in a dialogue about both their media consumption and the risks and opportunities of the online environment. If parents and educators believe that the government has made the internet safe for children they may no longer feel obligated to engage in these discussions. It is critical that we continue to focus resources on educating and supporting children and young people to become media literate and responsible consumers and producers of online material. Getting the policy balance between protection, education and family- based negotiation is critical if we are to produce future citizens who are prepared for a digital, online and mobile future.

Appendix One - The Practice of Filtering

Any discussion of public policy related to internet filtering is linked to the technology which facilitates it. More specifically, the degree to which the technology underblocks or overblocks the content which is seeks to filter. The following table provides an overview of the types of different filtering options available and their concomitant advantages and disadvantages:

Technique	Description	Advantages	Disadvantages
IP Blocking	**TCP/IP Header filtering** is where routers inspect the IP packet header with the destination IP being located. Routers can be configured to put packets destined for an IP on a list. They only block communication on the basis of where packets are going to or coming from, not what they contain.	• Effective in blocking a requested target. • No new equipment needs to be purchased. • Instantaneous implementation • Required technology and expertise is readily available. • Potential to block at or near international gateways so that blocking is uniform across ISPs.	• Can result in significant overblocking as all other (unrelated) websites hosted on that server will also be blocked.
	TCP/IP Content Filtering is where the contents of a certain packed are examined for banned keywords.	• Greater specify with regards to the type of content which can be filtered – based on keyword. • By filtering based on keywords, the whole IP is not blocked, only those packets with the banned keywords. This reduces the potential for over filtering.	• Extra equipment may be needed. • Typical hardware may be unable to react fast enough to block the infringing packets, • As packets have a maximum size, the full content of the communication will likely be split over multiple packets. • Keywords might be split over a number of packets which means devices may fail to identify banned keywords. • For packet inspection to be fully effective, the stream must be reassembled, which adds additional complexity. • Sites can be aware of this technique and simply not use the offending keyword and select an equivalent term.

DNS (domain name server) Tampering	Most websites use domain names not IP addresses. If the domain name resolution stage can be filtered, access to infringing sites can be effectively blocked. A list of banned domain names can be configured which will display an error message if a user tries to access a listed site.	• Purposefully disrupting DNS servers which resolve domain names into IP addresses. • Can target a particular website by configuring the DNS server to return the wrong IP address.	• Comparatively easy to bypass by the user selecting an alternative recursive resolver. This type of circumvention might be made more difficult by blocking access to external DNS servers, but doing so would be disruptive to normal activities and could also be bypassed.
Proxy-based filtering strategies	Prevents users from directly connecting to a website but requires users to go through a proxy server. The proxy server may temporarily store information in a cache. The proxy decides whether request for webpages should be permitted, and if so, sends the request to the web server hosting the requested content. Since the full contents of the request are available, individual web pages can be filtered, not just entire websites or domains. Also, a transparent HTTP proxy may intercept outgoing web requests and send them to a proxy server.	• Permits the greatest flexibility, allowing blocking both by full Web page URL and by Web page content. • Internet traffic passing through the filtering system is reassembled and the specific HTTP addressing being accessed is checked against a list of blocked websites (can be individual domains, subdomains, specific long URL paths, or keywords in the domain or URL path). This permits greater specificity. • Can also be programmed so that internet traffic passing through the filtering system is reassembled and the specific HTTP address requested is checked against a list of blocked keywords.	• More complex to establish. • This can be fooled by redirecting traffic through an open proxy server. Such servers may be set up accidentally by computer users who misconfigure their own computers. Alternatively, a proxy could be specifically designed for circumventing Internet filtering. Here, the main challenge is to discover an open proxy as many are shut down rapidly due to spammers abusing them, or blocked by organisations that realise they are being used for circumvention. • Encrypted proxy servers may be used to hide what is being accessed through them
Hybrid TCP/IP and HTTP Proxy	Requests are intercepted by an HTTP proxy and are then reassembled from the original packets, decoded and then retransmitted. The system operates by	• Allows the greatest flexibility. • Reduces overblocking	• Hardware required to keep up with a fast Internet connection is very expensive.

	building a list of the IP addresses of sites hosting prohibited content, but rather than blocking data flowing to these servers, the traffic is redirected to a transparent HTTP proxy. There, the full Web address is inspected and if it refers to banned content, it is blocked; otherwise the request is passed on as normal.		

The degree to which an internet filter either over blocks or under blocks websites has important ramifications for public policy. Many countries internationally have declared internet filtering illegal because of the chance that overblocking content might constitute an infringement of the rights of access to information and free speech. The Received Operating Characteristic (ROC) is a hypothetical curve which models the trade-off between overblocking and underblocking. For example, it is possible to obtain fewer instances of underblocking but this is at the cost of more overblocking. In general, the way to improve this trade-off is to devise more precise ways of discriminating between desired and undesired results such as results from a greater investment in internet filtering hardware and software.

There is also the issue of transparency of internet filtering. In some cases a blocked site will simply return an error message giving no indication that the site has been intentionally blocked. Alternatively, a warning label can be applied to sites which have been intentionally blocked and also provide users with information to allow them to write to authorities to register a complaint that a given website has been wrongly blocked.

Another issue comes in the form of under blocking. If filtering is conducted at a centralised location, perhaps on the internet backbone at the county's international gateway, then all internet traffic will encounter the same filters. This means that all users in a country will experience the same access to the internet. Alternatively, if filtering is decentralised amongst ISPs, then this could result in a different level of access to users based on who their ISP is. Therefore, access could be subject to the marketing policies of the ISP provider.

Appendix Two – National Classification Code for Films

Item	Description of Publication	Classification
1	Films that: (a) depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or (b) describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or (c) promote, incite or instruct in matters of crime or violence	RC
2	Films (except RC films) that: (a) contain real depictions of actual sexual activity between consenting adults in which there is no violence, sexual violence, sexualised violence, coercion, sexually assaultive language, or fetishes or depictions which purposefully demean anyone involved in that activity for the enjoyment of viewers, in a way that is likely to cause offence to a reasonable adult; and (b) are unsuitable for a minor to see	X 18+
3	Films (except RC films and X 18+ films) that are unsuitable for a minor to see	R 18+
4	Films (except RC films, X 18+ films and R 18+ films) that depict, express or otherwise deal with sex, violence or coarse language in such a manner as to be unsuitable for viewing by persons under 15	MA 15+
5	Films (except RC films, X 18+ films, R 18+ films and MA 15+ films) that cannot be recommended for viewing by persons who are under 15	M

6	Films (except RC films, X 18+ films, R 18+ films, MA 15+ films and M films) that cannot be recommended for viewing by persons who are under 15 without the guidance of their parents or guardians	PG
7	All other films	G

Appendix Three – National Classification Guidelines (Extract)

RC – REFUSED CLASSIFICATION

Note: Films that exceed the R 18+ and X 18+ classification categories will be Refused Classification.

Computer games that exceed the MA 15+ classification category will be Refused Classification.

Films and computer games will be refused classification if they include or contain any of the following:

CRIME OR VIOLENCE
Detailed instruction or promotion in matters of crime or violence.

The promotion or provision of instruction in paedophile activity.

Descriptions or depictions of child sexual abuse or any other exploitative or offensive descriptions or depictions involving a person who is, or appears to be, a child under 18 years.

Gratuitous, exploitative or offensive depictions of:

(i) violence with a very high degree of impact or which are excessively frequent, prolonged or detailed;
(ii) cruelty or real violence which are very detailed or which have a high impact;
(iii) sexual violence.

SEX
Depictions of practices such as bestiality.

Gratuitous, exploitative or offensive depictions of:

(i) activity accompanied by fetishes or practices which are offensive or abhorrent;
(ii) incest fantasies or other fantasies which are offensive or abhorrent.

DRUG USE
Detailed instruction in the use of proscribed drugs.

Material promoting or encouraging proscribed drug use.

Note: Some of the terms used in this category are defined in the List of Terms at the end of these

Guidelines.

List of References

[1] Conroy, S 2007, *Labor's Plan for Cyber Safety*, Australian Labor Party, Canberra, accessed 1 November 2009, from http://www.alp.org.au/download/now/labors_plan_for_cyber_safety.pdf.

[2] Conroy, S 2008, *Internet Filtering Technology*, Australian Labor Party, Canberra, accessed 1 November 2009, from http://www.alp.org.au/media/0708/mscoit290.php

[3] http://www.dcsf.gov.uk/byronreview/

[4] http://www.lse.ac.uk/collections/EUKidsOnline/

[5] http://www.dcsf.gov.uk/byronreview/pdfs/Byron%20Review%20Press%20Notice.pdf

[6] ACMA 2007, p. 21

[7] Conroy, S 2007, *Labor's Plan for Cyber Safety*, Australian Labor Party, Canberra, accessed 1 November 2009, from http://www.alp.org.au/download/now/labors_plan_for_cyber_safety.pdf.

[8] ibid, page 2.

[9] Department of Broadband, Communications and the Digital Economy 2009, *Cyber-safety plan*, DBCDE, viewed 1 November 2009, from http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan

[10] Department of Broadband, Communications and the Digital Economy 2009, *Internet Service Provider (ISP) Filtering*, DBCDE, viewed 1 November 2009, from http://www.dbcde.gov.au /funding_and_programs/ cybersafety_plan.

[11] Department of Broadband, Communications and the Digital Economy 2009, *Internet Service Provider (ISP) Filtering*, DBCDE, viewed 1 November 2009, from http://www.dbcde.gov.au /funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering

[12] Guidelines for the Classification of Films and Computer Games as amended under section 12 of the Classification (Publications, Films and Computer Games) Act 1995, viewed 1 November 2009, from http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrumentCompilation1.nsf/0/F0EC030A108C93DDCA 2574120004F6B8/$file/FCGGuidelines2005.pdf.

[13] Australia, Senate 2009, Parliamentary Debates, 3 February 2009, 210 (Stephen Conroy, Minister for Broadband, Communications and the Digital Economy), viewed 1 November 2009, from http://www.aph.gov.au/hansard/senate/dailys/ds030209.pdf, page 210.

[14] Australia, Senate 2009, Environment, Communications and the Arts Legislation Committee Budget Estimates, 25 May 2009, 145 (Ms. O'Loughlin, ACMA), viewed 1 November 2009, from http://www.aph.gov.au/hansard/senate/commttee/S12031.pdf, page 156.

[15] Australia, Senate 2009, Senate Standing Committee on Environment, Communications and the Arts Legislation Committee Additional Senate Estimates Hearing, February 2009, ECA73, viewed 1 November 2009, from http://www.aph.gov.au/senate/committee/eca_ctte/estimates /add_0809/bcde/acma.pdf.

[16] Australia, Senate 2009, Parliamentary Debates, 3 February 2009, 210 (Stephen Conroy, Minister for Broadband, Communications and the Digital Economy), viewed 1 November 2009, from http://www.aph.gov.au/hansard/senate/dailys/ds030209.pdf, page 210.

[17] Australia, Senate 2009, Parliamentary Debates, 3 February 2009, 221 (Stephen Conroy, Minister for Broadband, Communications and the Digital Economy), viewed 1 November 2009, from http://www.aph.gov.au/hansard/senate/dailys/ds030209.pdf, page 221.

[18] National Classification Code, viewed 1 November 2009, from http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrument1.nsf/0/A9975715C45E4DE8CA25700D002EF639/$file/Code+26+May_to+attach.pdf

[19] Adultshop.Com Ltd v Members of the Classification Review Board [2007] FCA 1871, viewed 1 November 2009, from http://www.austlii.edu.au/au/cases/cth/federal_ct/2007/1871.html

[20] NSW Council for Civil Liberties Inc v Classification Review Board (No. 2) [2007] FCA 896, viewed 1 November 2009, from http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/FCA/2007/896.html

[21] Michael Brown & Ors v Members of the Classification Review Board of the Office of Film and Literature [1998] FCA 319, viewed 1 November 2009, from http://www.austlii.edu.au/au/cases/cth/federal_ct/1998/319.html

[22] Directive 2000/31/EC of the European Parliament 2000, viewed 1 November 2009, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.

[23] Deibert, R, Palfrey, J, Rohozinski, R, & Zittrain, J 2008. *Access Denied: The Practice and Policy of Global Internet Filtering,* The MIT Press, Cambridge, MA.

[24] European Opinion Research Group 2004, *Illegal and harmful content on the Internet,* viewed 1 November 2009, http://ec.europa.eu/public_opinion/archives/ebs/ebs_203_en.pdf

[25] European Union Official Journal of European Communities 1999, *Action plan on promoting safe use of the Internet,* viewed 1 November 2009, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= OJ:C:1999:092:0012:0012:EN:PDF.

[26] Ermert, M 2009, *Germany Builds Infrastructure to Block the Internet, Intellectual Property Watch*, viewed 1 November 2009, from http://www.ip-watch.org/weblog/2009/06/19/germany-builds-infrastructure-to-block-the-internet/

[27] ibid

[28] DW-WORLD.DE 2009, New German government reaches key internet security agreements, *Deutsche Welle*, October 15, http://www.dw-world.de/dw/article/0,,4794080,00.html

[29] EDRI-gram 2006, *Betting websites are blocked in Italy*, viewed 1 November 2009, from http://www.edri.org/edrigram/number4.12/italybetting.

[30] Edwards, T, Griffith, G 2008. *Internet Censorship and Mandatory Filtering,* NSW Parliamentary Library Research Service, viewed 1 November 2009, from http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/7F8B9A55E2FC8932CA2575030083844A/$File/E%20Brief%20Internet%20Censorship.pdf

[31] Deibert, R, Palfrey, J, Rohozinski, R, & Zittrain, J 2008. *Access Denied: The Practice and Policy of Global Internet Filtering,* The MIT Press, Cambridge, MA.

[32] Edwards, T, Griffith, G 2008. *Internet Censorship and Mandatory Filtering,* NSW Parliamentary Library Research Service, viewed 1 November 2009, from http://www.parliament.nsw.gov.au /prod/parlment/publications.nsf/0/7F8B9A55E2FC8932CA2575030083844A/$File/E%20Brief%20Internet%20Censorship.pdf

[33] Collins, L, Love, P, Landfeldt, B & Coroneos, P 2008, *Feasibility Study ISP Level Content Filtering*, prepared on behalf of the Internet Industry Association, viewed 1 November, from http://www.dbcde.gov.au/__data/assets/pdf_file/0006/95307/Main_Report_-_Final.pdf

[34] ibid

[35] ibid

[36] Deibert, R, Palfrey, J, Rohozinski, R, & Zittrain, J 2008. *Access Denied: The Practice and Policy of Global Internet Filtering,* The MIT Press, Cambridge, MA.

[37] Canadian Government 1993, *Telecommunications Act,* Statutes of Canada, Ottawa, viewed 1 November 2009, from http://www.efc.ca/pages/law/canada/telecom.html.

[38] CTV News 2006, *New initiative will see ISPs block child porn sites*, 23 November, viewed 1 November 2009, http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20061123/isps_childporn_061123/20061123?hub=Canada

[39] DIANZ 2009a, Web filter will focus solely on child sex abuse images, *Resources*, Department of Internal Affairs, Government of New Zealand, 16 July, viewed 8 December 2009, from http://www.dia.govt.nz/press.nsf/d77da9b523f12931cc256ac5000d19b6/26bc0621775bbe47cc2575f50010a894!OpenDocument

[40] NZPA 2009, Internet users take issue with child-porn filter, *nzherald.co.nz*, 17 July, viewed 8 Decmber 2009, from http://www.nzherald.co.nz/internet/news/article.cfm?c_id=137&objectid=10584982&pnum=1

[41] DIANZ 2009b, Digital Child Exploitation Filtering System, *Services*, Department of Internal Affairs, Government of New Zealand, viewed 8 December 2009, from http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Digital-Child-Exploitation-Filtering-System?OpenDocument

[42] Reporters Without Boarders 2009, *Internet Enemies,* viewed 1 November 2009, from http://www.rsf.org/IMG/pdf/Internet_enemies_2009_2_-3.pdf.

[43] ibid, page 2

[44] RWB, 2009, *Reporters without borders* [English version], viewed 18 November 2009, from http://www.rsf.org/en-pays225-Internet.html

[45] Deibert, R, Palfrey, J, Rohozinski, R, & Zittrain, J 2008. *Access Denied: The Practice and Policy of Global Internet Filtering,* The MIT Press, Cambridge, MA.

[46] ibid

[47] Open Net Initiative 2009, Internet Filtering (Political), viewed 1 November 2009, from http://map.opennet.net/filtering-pol.html.

[48] Open Net Initiative 2009, Internet Filtering (Social), viewed 1 November 2009, from http://map.opennet.net/filtering-soc.html

[49] Open Net Initiative 2009, Internet Filtering (Conflict and Security), viewed 1 November 2009, from http://map.opennet.net/filtering-consec.html

[50] Open Net Initiative 2009, Internet Filtering (Internet Tools), viewed 1 November 2009, from http://map.opennet.net/filtering-IT.html

[51] ONI, 2009, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/

[52] ONI, 2009, United Arab Emirates, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/uae

[53] ONI, 2009, Yemen, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/yemen

[54] ONI, 2009, Azerbijan, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/azerbaijan

[55] ONI, 2009, Jordan, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/jordan

[56] ONI, 2009, Pakistan, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/pakistan

[57] ONI, 2009, Tajikistan, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/tajikistan

[58] ONI, 2009, Thailand, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/thailand

[59] Australia, Senate 2009, Environment, Communications and the Arts Legislation Committee Budget Estimates, 25 May 2009, 145 (Ms. O'Loughlin, ACMA), viewed 1 November 2009, from http://www.aph.gov.au/hansard/senate/commttee/S12031.pdf, page 156

[60] ONI, 2009, Bahrain, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/bahrain

[61] ONI, 2009, Ethiopia, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/ethiopia

[62] ONI, 2009, Singapore, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/singapore

[63] ONI, 2009, South Korea, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/south-korea

[64] ONI, 2009, Syria, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/syria

[65] ONI, 2009, Uzbekistan, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/uzbekistan

[66] ONI, 2009, Vietnam, *Open Net Initiative*, viewed 18 November 2009, from http://opennet.net/research/profiles/vietnam

[67] McClelland, R (Attorney General) 2009, *National Human Rights Consultation Report,* Canberra, 8 October, viewed 1 November 2009, http://www.alp.org.au/media/1009/msag080.php

[68] National Human Rights Consultation 2009, *National Human Rights Consultation Report,* Attorney General's Department, Canberra, viewed 1 November 2009,

http://www.humanrightsconsultation.gov.au/www/nhrcc/RWPAttach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~NHRC+Report+(Prelims).pdf/$file/NHRC+Report+(Prelims).pdf

[69] Colmar Brunton 2009, *National Human Rights Consultation - Community Research Phase,* Summary Report, for the Attorney General, Colmar Brunton, Canberra, viewed 1 November 2009, http://www.humanrightsconsultation.gov.au/www/nhrcc/RWPAttach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~NHRC+Report+(Appendix+B).pdf/$file/NHRC+Report+(Appendix+B).pdf

[70] National Human Rights Consultation 2009, *National Human Rights Consultation Report,* Attorney General's Department, Canberra, viewed 1 November 2009, http://www.humanrightsconsultation.gov.au/www/nhrcc/RWPAttach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~NHRC+Report+(Chapter+15).pdf/$file/NHRC+Report+(Chapter+15).pdf.

[71] Office of the United Nations High Commissioner for Human Rights 1976, *International Covenant on Civil and Political Rights,* viewed 1 November 2009, http://www2.ohchr.org/english/law/ccpr.htm

[72] ibid

[73] ibid

[74] Deibert, R, Palfrey, J, Rohozinski, R, & Zittrain, J 2008. *Access Denied: The Practice and Policy of Global Internet Filtering,* The MIT Press, Cambridge, MA.

[75] Deibert, R, Palfrey, J, Rohozinski, R, & Zittrain, J 2008. *Access Denied: The Practice and Policy of Global Internet Filtering,* The MIT Press, Cambridge, MA.

[76] Mckee, Albury and Lumby 2008