THE AUSTRALIAN NATIONAL UNIVERSITY

Dr GREGOR URBAS
ANU College of Law
Australian National University
Canberra ACT 0200
AUSTRALIA

Telephone: +61 2 6125 4262
Facsimile: +61 2 6125 3971

Email: Gregor.Urbas@anu.edu.au
http://www.anu.edu.au

Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001
(02) 8238 6333

National Classification Scheme Review

Dear ALRC Secretariat

We are pleased to offer the following submission to Issues Paper (IP40) regarding the National Classification Scheme Review.

Mr Tristan Kelly
Technology Consultant

Ph. 0418 708 040
Email: TKelly@tristankelly.tk

Dr Gregor Urbas
Senior Lecturer in Law
ANU College of Law
Australian National University
Ph. (02) 6125 4262
Email: Gregor.Urbas@anu.edu.au

15 July 2011

Table of Contents

Glossary 4

Introduction 5

Question 3. Should the technology or platform used to access content affect whether content should be classified, and, if so, why? 7

Questions 4 & 5: Should some content only be required to be classified if the content has been the subject of a complaint? Should the potential impact of content affect whether it should be classified? 9

Questions 12 & 13. What are the most effective methods of controlling access to online content, access to which would be restricted under the National Classification Scheme? How can children's access to potentially inappropriate content be better controlled online? 12

- Restricted Access Systems 12
- Filtering Technology 14
  - Static and Dynamic Filters 15
  - ISP level and PC level Filters 16

Questions 24 & 25: Access to what content, if any, should be entirely prohibited online? Does the current scope of the Refused Classification (RC) category reflect the content that should be prohibited online? 19

- Freedom of Speech 19
- Social Responsibility 21
- Moral Standards 21
- Indirect Harm 23
- Pornography 23
- Child Pornography 24
- The Harm Principle 25
- A New Definition for Prohibited Content 26

Question 29: In what other ways might the framework for the classification of media content in Australia be improved? 29

- Category 1 Restricted Content 29
- Public Confidence 30
  - Integrity Requirements for Internet Censorship 30
  - Analysis and Improvements 30

Bibliography 33

Glossary

Term	Definition
ACMA	Australian Communications and Media Authority
ACT	Australian Capital Territory
ACTCA	*Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (ACT)
Board	Classification Board
BSA	*Broadcasting Services Act 1992* (Cth)
CCA	*Classification (Publications, Films and Computer Games) Act 1995* (Cth)
Code	*National Classification Code 2005* (Cth)
DBCDE	Department of Broadband, Communications and the Digital Economy
EFA	Electronic Frontiers Australia
ICCPR	*International Covenant on Civil and Political Rights*
ISP	Internet Service Provider
MA	Mature Accompanied (classification)
NSW	New South Wales
NSWCA	*Classification (Publications, Films and Computer Games) Enforcement Act 1995 (NSW)*
NT	Northern Territory
PC	Personal Computer
PIN	Personal Identification Number
R	Restricted (classification)
RAS	Restricted Access System
RASD	*Restricted Access Systems Declaration 2007* (Cth)
RC	Refused Classification
UDHR	*Universal Declaration of Human Rights*
UN	United Nations
US	United States of America
VPN	Virtual Private Network
WA	Western Australia
X	Restricted – sexual activity (classification)

Introduction

In a world of rapidly evolving Internet technology that allows for the instant promulgation of ideas and images across the globe, Australia does not have an effective policy or legislation to control potentially harmful electronic material and thereby protect its citizens.

Australia currently maintains a form of Internet censorship through the classification scheme, which allows the Australian Communications and Media Authority ('AMCA') to require Australian web hosts to remove content.

This submission will address a subset of the questions posed in the Issues Paper. The focus of the submission will be on the application of the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) (the '*CCA*') and the *National Classification Code 2005* (Cth) (the '*Code*') in classifying and censoring Internet content, through Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth) (the '*BSA*'). A number of reforms will be proposed to increase public confidence in, and increase the effectiveness of, the existing regime.

In particular, this submission proposes that the Commission adopt a number of recommendations:

1. That the definition of 'prohibited content' in the *BSA* be amended such that content equivalent to Category 1 Restricted or Category 2 Restricted content should not be prohibited online for adults;
2. That an offence be introduced prohibiting the publication of unclassified content on the Internet, where there is a significant likelihood that the content would be prohibited content;
3. That the RAS system be improved by collecting both credit card and identity information, and using the credit card system to assist in verifying this identity;
4. That the Government should consider reinstating its previous policy supporting voluntary PC based dynamic filters;
5. That the definition of 'prohibited content' in the *BSA* be amended to only prohibit RC content to adults;
6. That the RC classification category be amended to include a harm test;
7. That the definitions of 'prohibited content' and 'potential prohibited content' in the *BSA* include the same classification categories;

8. That content publishers be given the right to be notified of classification decisions;
9. That content publishers be given the right to appeal classification decisions;
10. That after confirming a take down notice (relating to Australian hosted content) has been complied with, ACMA publish details identifying the material censored.

Question 3. Should the technology or platform used to access content affect whether content should be classified, and, if so, why?

A common argument raised in support of Internet regulation and filtering is that content which is illegal to access offline should also be illegal to access online.[1] This argument is premised on the desirability of 'medium neutrality' with respect to the regulation of content. However, under the current *BSA*, more content is prohibited online than offline. Existing publications which have already been classified Category 1 or Category 2 Restricted are available for sale in shops across Australia.[2] However, electronic versions of these same publications would be prohibited on the Internet, as Category 1 and Category 2 Restricted content is 'prohibited content' under the *BSA*.[3] With the introduction of iPads and the rise in popularity of digital books, more existing publications are likely to become available over the Internet, and this inconsistent standard will become more problematic.[4]

Similarly, material which has not been previously published offline, but which is equivalent to content that would be classified as Category 1 Restricted or Category 2 Restricted and legally available offline, would be prohibited on the Internet. For example, text or still images on the Internet concerning explicit sex would likely be classified X 18+,[5] and would therefore be prohibited under the *BSA*.[6] However, this same material would be classified as Category 2 Restricted offline[7] and could be sold legally to adults.[8]

Additionally, video content which is, or would be, classified as X 18+ is prohibited on the Internet, despite being available for sale in some Australian jurisdictions.[9]

---

[1] See, eg, Fran Foo and Andrew Colley, *ISP filtering legislation on the way* (2010) Australian IT <http://www.theaustralian.com.au/australian-it/filtering-legislation-on-the-way/story-e6frgakx-1225889109550> at 13 July 2010.
[2] See, eg, *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (ACT) (the '*ACTCA*') ss 35(4), 29-30.
[3] *BSA* sch 7 cl 20(2).
[4] Caitlin Fankhauser and Veronica Scott, 'It's different on the internet: regulating online content' (2010) 13(1) *Internet Law Bulletin* 200, 201.
[5] Internet content which is not a computer game or an electronic version of an existing publication is classified in the same way as a film: *BSA* sch 7 cl 25; *Code* r 3.
[6] *BSA* sch 7 cl 20(1)(a).
[7] *Code* r 3.
[8] See, eg, *ACTCA* ss 35(4), 29-30.
[9] X18+ movies are available for sale to adults in the ACT and NT, see, *ACTCA* ss 54C, 9(2); *Classification of Publications, Films and Computer Games Act* (NT) ss 49, 57(2); Cf, eg, *Classification (Publications, Films and Computer Games) Enforcement Act 1995* (NSW) (the '*NSWCA*') s 6(a).

In this way, the *BSA* creates an inconsistency between online and offline classification, with Internet content being more severely restricted. As technologies converge and the Internet continues to increase in popularity as a method for accessing material traditionally published offline, this inconsistency may be out of step with community standards.

> **Recommendation 1**:
>
> That the definition of 'prohibited content' in the *BSA* be amended such that content equivalent to Category 1 Restricted or Category 2 Restricted content should not be prohibited online for adults.

Adoption of this recommendation would achieve greater medium neutrality. In a world where the same media can be readily consumed by the same people, but over a multitude of different mediums, this is a worthy policy aim.[10]

Note: Recommendation 5 below proposes amending the definition of prohibited content further, on different grounds, to also not prohibit X18+ content for adults.

[10] Catharine Lumby and Kate Crawford, *The Adaptive Moment: A Fresh Approach to Convergent Media in Australia* (2011) 10-18.

Questions 4 & 5: Should some content only be required to be classified if the content has been the subject of a complaint? Should the potential impact of content affect whether it should be classified?

The complaints-based nature of the existing classification scheme limits its effectiveness. ACMA will generally only investigate content after a complaint is made, as opposed to before distribution as is the case with films and computer games.[11] This limits the reach of the scheme and ACMA's ability to prevent unsolicited exposure to prohibited material.

However, requiring content hosts to submit all material for classification prior to publication would be an impractical administrative burden.[12] The quantity of content on the Internet would make it impossible to review all content. Nonetheless, the complaints-based system at least provides a means of identifying a subset of prohibited content, which supports the policy aim of restricting access to such content.

Unlike films and computer games, the existing classification system for offline publications does not require every publication to be submitted for classification prior to publication. Instead, publications only need to be submitted if they are likely to be classified as RC, cause offence to a reasonable person, are unsuitable for minors, or at the request of the Board.[13] It is an offence, punishable by 50 penalty units, to sell or deliver a publication which meets this definition but has not been classified.[14]

An improvement to the classification system for online content would be to introduce a similar obligation on those uploading or publishing content to the Internet ('content publishers'). That is, to create an offence of publishing unclassified content online where there is a significant likelihood that the content would be prohibited content, and to create a mechanism for submitting such content for classification prior to publication. The aim of this improvement would be to increase the amount of content assessed by the Board, within manageable limits, by targeting the Board's efforts at that material which is most likely to be prohibited.

---

[11] Fankhauser and Scott, above n 4, 202.
[12] David Vaile and Renée Watt, 'Inspecting the despicable, assessing the unacceptable: Prohibited packets and the Great Firewall of Canberra' (2009) 59(2) *Telecommunications Journal of Australia* 27.1, 27.1.
[13] *CCA* ss 5, 23(1); see also, eg, *ACTCA* s 28(1).
[14] *NSWCA* s 19(1)(a); *ACTCA* s 28(1); see also *CCA* s 5.

An essential element of this improvement is changing the focus of the *BSA* from only regulating hosting service providers, to also targeting individual content publishers. In many cases, while content hosts are unlikely to be able to review all of the content on their systems, content publishers are in a good position to know about and assess their own content. This is the case for traditional websites, where the web host is likely to host a significant number of sites for different clients, who upload content independently and directly. For social media sites such as Facebook, YouTube or blog sites, users publish their own content, often without review by the site owner.[15] As the Internet allows individuals to publish information more easily than ever before, laws seeking to regulate Internet content should recognise this new reality, and place obligations on these publishers.

This proposal would impose an administrative burden on content publishers. However, it would be no more burdensome than the system which currently exists for offline publications. While it may seem extreme in the case of social media to require individuals to submit their content to the Board before publishing, the content which is likely to be (legally) prohibited would likely already be prohibited under the site's terms of service and thus should not be published anyway.[16] In this case, the offence would merely complement the existing contractual restriction on publishing such content.

A drawback is that this proposal relies on honest content publishers to voluntarily submit their content for classification. A content publisher may be unlikely to take this step if they suspected that the Board would prohibit their content. Nonetheless, assuming the submission process was straightforward, content publishers may wish to submit material for assessment to prove that it should not be restricted, especially for content on the border between prohibited and unrestricted. Further, assuming appropriate knowledge of the offence, the offence would provide an incentive to content publishers to protect themselves and avoid prosecution, by ensuring that they applied for classification when necessary. Increasing the

[15] Google, *Mandatory ISP Level Filtering: Submission to the DBCDE* (2010) 8, 14; Three Google employees received criminal convictions in Italy in 2010 for failure to remove a video uploaded to their site, depicting the mistreatment of a child, despite having no direct knowledge of its content: see Stacy Meichtry, *Italy Says Google Trio Violated Boy's Privacy* (2010) The Wall Street Journal <http://online.wsj.com/article/SB10001424052748704240004575084851798366446.html?ru=yahoo&mod=yahoo_hs> at 30 October 2010.

[16] See, eg, Facebook, *Statement of Rights and Responsibilities* (2010) <http://www.facebook.com/terms.php> at 28 October 2010 [3.7], [5.1].

amount of Internet content assessed by the Board increases the effectiveness of the classification scheme, especially as the additional content assessed would be that content more likely to be prohibited.

An additional advantage of this proposal is that it would apply to all content publishers in Australia, and potentially even to Australians overseas,[17] regardless of where the content is hosted. This would prevent Australians from side-stepping the classification scheme by hosting their content overseas.

Imposing an obligation on content publishers would not completely remove prohibited content published by Australians from the Internet, let alone from the Internet as a whole. The obligation would also create an administrative burden on those wishing to upload material close to the prohibited threshold. However, regulating content publishers in this way would ensure that the law is targeted at those in control of the content, recognising the changed nature of publication in the Internet age. Assuming that users were aware of the obligation, the associated criminal penalties would create a disincentive to uploading likely prohibited content, and would encourage content publishers to submit such content for classification to avoid their exposure to prosecution. Reducing the amount of prohibited content on the Internet and increasing the amount of content assessed by the Board would improve the effectiveness of the classification scheme.

Recommendation 2:

That an offence be introduced prohibiting the publication of unclassified content on the Internet, where there is a significant likelihood that the content would be prohibited content.

[17] Depending on the jurisdictional application of the offence provisions, see *Criminal Code Act 1995* (Cth) pt 2.7.

Questions 12 & 13. What are the most effective methods of controlling access to online content, access to which would be restricted under the National Classification Scheme? How can children's access to potentially inappropriate content be better controlled online?

Restricted Access Systems

The relative difficulty in verifying a person's age on the Internet is one argument for restricting Internet content more severely than offline content. The *BSA* currently specifies (and mandates) a means of achieving access control for content classified MA 15+ or R 18+. This system could potentially be extended to restrict access to X 18+ and Category 1 or Category 2 Restricted content.

The Restricted Access System ('RAS') required for MA 15+ content merely requires access to be limited to users who apply for access, declare that they are over 15 years of age, and are provided with a warning about the nature of the content.[18] While this system may guard against inadvertent access, and provide users with appropriate advice about the content before they receive access, it would not be effective for preventing children from accessing inappropriate material.

The RAS required for R 18+ is more comprehensive. In addition to the above requirements, the applicant must provide evidence that they are at least 18 years of age,[19] and once verified can be issued with a PIN for future access.[20] The type of evidence required must satisfy a 'risk assessment' that the person is who they purport to be, and that the evidence accurately reflects their age.[21] ACMA has previously suggested using credit cards, or copies of driver licences or passports for this purpose.[22] ACMA is entitled to request age verification records in order to ensure compliance.[23]

---

[18] *Restricted Access Systems Declaration 2007* (Cth) ('*RASD*') ss 5-9.
[19] *RASD* s 13(1)(a).
[20] *RASD* s 14(2).
[21] *RASD* s 15(2).
[22] ACMA, *Minimum verification system requirements* (2009) <http://www.acma.gov.au/scripts/nc.dll?WEB/STANDARD/1001/pc=PC_90159> at 5 October 2010.
[23] *RASD*s 17(b).

This scheme has been criticised by the NSW Council for Civil Liberties on the basis that it collects too much personal information when only a date of birth is required.[24] However, it is not possible for a person to prove that they are a certain age without showing documentation which both identifies them and shows their age. On this basis, documentation such as a driver licence or passport is necessary and appropriate for the purpose.

Of greater concern is the ability of any piece of evidence to satisfy the risk assessment test. Without seeing the person attempting to access material through the RAS, it is impossible to know if they are who they purport to be. Children could readily access a parent's or other older family member's driver licence, passport or previously issued PIN, and credit cards do not include a birth date and can be issued to minors. However, a RAS should not be expected to prevent fraud by a child against their parent or family. As advocated by child protection groups, parents have a responsibility to monitor their children's Internet access,[25] which should extend to protecting their own identity documents and monitoring their children's credit cards.

A slight improvement to this system could be to require both a credit card and age verifying identification, in the same name, and to charge an (even nominal) amount to the credit card. This would verify that the name on the credit card is the name of an adult, and the transaction would appear on that adult's credit card statement, potentially alerting them to fraudulent use. The knowledge that the transaction would appear on their parent's credit card statement may deter some children from using the card.

An additional level of security would be for the website owner to include a unique PIN on the credit card transaction, and require this PIN to be entered back into the website prior to granting access to the restricted content. This would ensure that the person accessing the website at least has access to the adult's online banking system or paper statements, increasing the likelihood that they are indeed the adult. This particular technique of using unique PINs is commonly used by organisations to verify that their debtors own bank

[24] NSW Council for Civil Liberties, *Submission to the ACMA on the draft RAS Declaration 2007* (2007), 7.
[25] Ray Cleary, *Protecting children online takes more than a filter* (2010) The Age <http://www.theage.com.au/opinion/society-and-culture/protecting-children-online-takes-more-than-a-filter-20100113-m6g8.html> at 28 October 2010; Annie Pettitt, 'New website takes right approach to internet safety for children' (Press Release, 19 February 2010) <http://www.savethechildren.org.au/images/documents/media/190210_-_Response_to_ThinkuKnow_website.pdf> at 1 October 2010.

accounts corresponding to account numbers their debtors have provided. For example, prior to debiting the account to pay a bill through 'direct debit'. PINs in general are a well accepted means of confirming that a person is the required account holder. When combined with ensuring that the account holder is an adult, this is a practical improvement for verifying age over the Internet.

RASs cannot definitively prevent children from accessing inappropriate content on websites. However, they can assist website owners to control access to this content by children, inadvertently and deliberately. This control can be strengthened by collecting and verifying both credit card and identity information prior to granting access to the restricted content. Combined with parental monitoring, this would be a reasonable attempt at removing inappropriate content from the reach of most children.

Recommendation 3:

That the RAS system be improved by collecting both credit card and identity information, and using the credit card system to assist in verifying this identity.

Filtering Technology

In recognition of the failure of the existing legal regime to control Internet content, especially content hosted outside Australia, governments have proposed technological solutions to remove or restrict access to websites identified as inappropriate. The current Australian Government's policy is to introduce a mandatory ISP level Internet filter, using the list of pages identified by the Board or ACMA as RC. [26] The policy under the previous Australian Government, which has since been abandoned,[27] was to license a number of commercial

[26] DBCDE, *Internet Service Provider (ISP) filtering* (2010) <http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering> at 25 August 2010; Vaile and Watt, above n 12, 27.4.
[27] NetAlert, *Protecting Australian Families Online* (2010) <http://www.netalert.gov.au/> at 30 October 2010.

Internet filters, which users could download for free.[28] These filters used the RC list and optionally dynamic filtering.[29]

Understanding that the Commission does not intend to review the Government's proposed mandatory ISP filter,[30] this submission will only discuss Internet filtering at a general level, and instead focus on how dynamic PC filters are a superior, although not complete, option for protecting children online.

Static and Dynamic Filters

Filters can be categorised as either static or dynamic. A static filter will attempt to block a specific set of pages (for example, those pages identified as RC), while a dynamic filter will attempt to determine if a page should be blocked based on a set of criteria.[31] One criticism of both the existing complaints-based take down system and static filters is that it is impossible to identify all of the prohibited material on the Internet, given the quantity of material. With the number of Internet pages estimated to be growing by over one billion per day,[32] the combined resources of ACMA and other international bodies would never be able to assess even a small fraction of web pages and consider if they should be blocked. As such, while static filters would be effective in blocking some content, they fail to fulfil the task of keeping the Internet free of prohibited material.

An alternative option would be to introduce a dynamic Internet filter. Dynamic filtering analyses the actual data passing through the Internet connection, instead of simply the destination web address. Pages are assessed against an algorithm to determine if they should be blocked.[33] This could include, for example, the text on the website or the file names for embedded pictures or videos.[34] As the filter does not need advanced warning of specific pages, these filters are generally more effective at blocking unwanted content.

---

[28] Helen Coonan, 'NetAlert: Protecting Australian Families Online' (Press Release, 10 August 2007) <http://www.minister.dbcde.gov.au/coonan/media/media_releases/netalert_-_protecting_australian_families_online> at 28 October 2010.
[29] Ibid.
[30] Issues Paper, paragraph 12.
[31] ACMA, *Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety* (2008) 31, 31-5.
[32] Vaile and Watt, above n12, 27.5.
[33] Ibid, 27.14; EFA, *Labor's Mandatory ISP Internet Blocking Plan* (2009) <http://www.efa.org.au/censorship/mandatory-isp-blocking/> at 19 July 2010.
[34] EFA, above n 33.

However, there are issues with introducing a dynamic filter as a mandatory means of censorship. As there is no final list of blocked pages, the system lacks transparency. The blocked content cannot be reviewed easily, and it may not be possible to inform content publishers when their page is blocked.[35] Further, it is impossible to identify a set of tests that would automatically block every offensive web page, and it is currently not possible to effectively assess images or video content.[36] More concerning is that 'false positives' are common as the automated analysis can catch innocent material which uses blocked words in a non-offensive context.[37] Extensive research into nineteen dynamic filters on the market in 2006 identified this problem with every filter.[38] Examples of pages blocked included a gay-interest site and safe sex information sites, but also Shakespeare's complete plays and the US Declaration of Independence.[39]

On this basis, dynamic filters should not be introduced as a mandatory form of censorship. For more information about the importance of maintaining standards of integrity in a censorship system, see this submission's response to question 29. However, as an optional filter, individuals may find some benefit in employing this technology to help prevent inadvertent access to unwanted content, and may be willing to accept the possibility of false positives. In addition, optional dynamic filters could assist parents in preventing their children from accessing inappropriate material.

ISP level and PC level Filters

Filtering of any kind can either occur at the ISP level, or the PC level.

ISP filters can be easily circumvented through proxy servers or virtual private networks. A proxy server acts as an intermediary between the user's ISP and the website the user is trying to access. Instead of requesting access to the website directly, the user requests access to a proxy server, which in turn requests access to the website and then forwards the content back

[35] Vaile and Watt, above n 12, 27.15.
[36] Philip Argy, 'Internet Content Regulation: An Australian Computer Society Perspective' (2000) 23(1) *University of New South Wales Law Journal* 265, 266; ACMA, above n 31, 34.
[37] EFA, above n 33.
[38] Marjorie Heins, Christina Cho and Ariel Feldman, *Internet Filters: A Public Policy Report* (2nd ed, 2006) 73.
[39] Ibid 33.

to the user.[40] Proxy servers are available on the Internet and can be accessed by browsing to the proxy server's web page and entering the requested address.[41] In defiance of Australian laws prohibiting the use of the Internet to access or distribute suicide-related material,[42] Exit International recently began training pensioners to use proxy servers to access euthanasia websites.[43] VPNs operate in a similar way, but can be more complex to setup.[44]

Dynamic filtering in particular can also be circumvented by encrypting traffic between the user and the web host (for example using HTTPS encryption as per most bank and e-commerce websites). In this case, the ISP is unable to read the data being transmitted to the user, and is therefore unable to determine if the page should be blocked.[45] For sites which do not offer encryption directly, the user could use a proxy server which offers encrypted connections, or a VPN, to encrypt the data and evade the filter.[46] As such, ISP level filters could be easily bypassed by children wishing to access inappropriate content. Furthermore, there is likely to be little evidence on the computer that the ISP filter has been bypassed.

PC level filters are not susceptible to the above circumvention by proxy server, VPN or encryption.[47] However, they can be bypassed on the computer itself. A 16 year old boy was reportedly able to bypass two of the Government sponsored Net Alert filters in 40 minutes.[48] Even so, such software generally includes mechanisms indicating when filters have been compromised, protections against deactivation, and would be more challenging to bypass than an ISP filter.[49] While not guaranteeing that the software could not be bypassed by a determined minor, this is a higher technical challenge than bypassing ISP level filters, which merely require browsing to a proxy server's webpage. As such, a PC based filter would

---

[40] Andrew Tanenbaum, *Computer Networks* (4th ed, 2003) 579, 822; ACMA, above n 31, 44.
[41] See, eg, Browzer, *Browse the web anonymously at school and work!* (2010) <http://www.browzer.info/> at 20 October 2010.
[42] *Criminal Code Act 1995* (Cth) ss 474.29A, 474.29B.
[43] ABC Television, 'Access Denied, *Four Corners*, 10 May 2010, <http://www.abc.net.au/4corners/content/2010/s2895350.htm> at 14 July 2010.
[44] Tanenbaum, above n 40, 779-80.
[45] Ibid.
[46] Ibid 779-80, 822.
[47] EFA, above n 33; Nick Higginbottom and Ben Packham, *Porn filters no barrier for net users* (2007) Herald Sun <http://www.heraldsun.com.au/news/national/porn-filters-no-safety-net/story-e6frf7l6-1111114263646> at 20 October 2010; Vaile and Watt, above n 12, 27.10; Liz Tay, *ICT industry all nostalgic for NetAlert* (2010) ITNews <http://www.itnews.com.au/News/219281,ict-industry-all-nostalgic-for-netalert.aspx> at 29 October 2010.
[48] Higginbottom and Packham, above n 47.
[49] Ibid; Vaile and Watt, above n 12, 27.10; Tay, above n 47.

provide parents with a greater ability to restrict their children's Internet access and a better ability to monitor whether their children are bypassing the filter.

Dynamic filters may be of some use to users, including parents, who wish to voluntarily filter material. In particular, PC-based filters provide parents with the best option to control and monitor their children's browsing habits. However, technology should be relied upon alone to protect children from inappropriate content.

Recommendation 4:
The Government should consider reinstating its previous policy supporting voluntary PC-based dynamic filters.

Questions 24 & 25: Access to what content, if any, should be entirely prohibited online? Does the current scope of the Refused Classification (RC) category reflect the content that should be prohibited online?

Debates surrounding free speech and censorship have a long history, dating back to at least 399 BC with the execution of Socrates for corrupting the youth of Athens in the ways of politics and religion.[50] The Internet is the new frontier for global communication, and has brought greater opportunities for political expression, but also expanded the platform for offensive and dangerous material that incites racism, violence, crime and disseminates pornography. This submission will assess the case for censorship on the Internet and will argue that while free expression is particularly important on this medium, a limited degree of censorship is required to protect children and to protect the community from material which incites harm, when accompanied by appropriate safeguards.

Freedom of Speech

In its first session, the General Assembly of the United Nations (the 'UN') declared that the right to access and discuss information freely was a fundamental human right.[51] The UN has subsequently expressed this right through the *Universal Declaration of Human Rights*[52] ('*UDHR*') and the *International Covenant on Civil and Political Rights*[53] ('*ICCPR*').[54] While not directly enforceable in Australia, these treaties set the international benchmark for human rights. Free speech advocates argue that the right to express opinions and influence others is too important to be restricted by other considerations and should be virtually inviolable.[55]

Freedom of speech is particularly important in a democracy. For democracies to function as the voice of the people, those people must be informed and have the ability to discuss and

[50] Frank Caso, *Censorship* (2008) 4.
[51] Walter Dauterman, 'Internet Regulation: Foreign Actors and Local Harms - at the Crossroads of Pornography, Hate Speech, and Freedom of Expression' (2002) 28 *North Carolina Journal of International Law and Commercial Regulation* 177, 208-9.
[52] UNGA Res 217 A (III) (1948).
[53] Opened for signature on 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
[54] Dauterman, above n 51, 178.
[55] Nigel Wilson, 'Regulating the information age – How will we cope with technological change?' (2010) 33 *Australian Bar Review* 119, 37.

debate ideas, and challenge prevailing social and political norms.[56] Equally, free speech helps people gain an appreciation for different perspectives, broadening minds and encouraging empathy.[57] As argued by John Stuart Mill, the strength of an idea can only be assessed after exposing it to a fair hearing of opposing opinions,[58] and thus freedom of speech enables democracies to make not just popular, but well-considered decisions. If governments or others are able to control what information is available, and silence dissent, a democracy cannot function effectively.

This link between democracy and free expression was recognised by the High Court in *Nationwide News v Wills*[59] where Deane and Toohey JJ held that the system of representative government established by the *Australian Constitution* gives rise to an implied right to communicate about politics, so that voters can make informed electoral decisions.[60] While not as comprehensive as the freedom of speech provided by the *First Amendment* to the *United States Constitution*,[61] this case confirms the importance of free expression, in a political context, to the operation of Australia's democracy.

The Internet provides a unique medium for free expression. In the US case *ACLU v Reno*,[62] Dalzell J stated: "The Internet is a far more speech-enhancing medium than print, the village green, or the mails".[63] Email, blogs, websites, social networking and file sharing technologies allow information to be communicated to large audiences across the world instantaneously. The ease with which an individual can publish or communicate information, with limited expertise or expense, allows a higher quantity and more diverse range of information to be disseminated than has ever been possible through traditional publishing, such as in books or newspapers.[64]

---

[56] Alexander Meiklejohn, 'The First Amendment is an Absolute' (1961) *Supreme Court Review* 245; 028, 8.
[57] Robert Trager and Sue Turner, 'The Internet Down Under: Can free speech be protected in a democracy without a Bill of Rights' (2000-2001) 23 *University of Arkansas at Little Rock Law Review* 123, 140.
[58] Randal Marlin, *Propaganda and the ethics of persuasion* (2003) 212-3.
[59] (1992) 177 CLR 1.
[60] *Nationwide News v Wills* (1992) 177 CLR 1, 71; See also: *ACTV v Cth* (1992) 177 CLR 106, 138-140; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 559-60; *Australian Constitution* ss 7, 24.
[61] *Levy v Victoria* (1997) 189 CLR 579, 594-5.
[62] *ACLU v Reno*, 929 F Supp 824 (ED Pa, 1996); Justice Dalzell's judgement was upheld in *Reno v ACLU*, 521 US 844, 863-4 (1997).
[63] *ACLU v Reno*, 929 F Supp 824, 882 (ED Pa, 1996).
[64] Marlin, above n 58, 283-6.

Accordingly, attempts to limit free expression can have a negative effect on democracy and limit people's ability to hold their governments to account and to achieve change. Given its unique position and power as discussed, the Internet is a particularly important medium for free expression. This is threatened by Internet censorship.

Social Responsibility

However, the Internet is also used by terrorists to recruit supporters and by racists to spread hate and incite violence.[65] Such content endangers the community. For example, books such as *The Turner Diaries* and the *Encyclopaedia of the Afghan Jihad* are widely available over the Internet.[66] The former advocates violent revolution and is believed to have motivated Timothy McVeigh to bomb the Alfred P Murrah Federal Building in Oklahoma City.[67] The latter details how to make explosives, carry out terrorist attacks and suggests popular landmarks such as Big Ben and the Eiffel Tower as targets for attack.[68] The Government has a responsibility to protect the community from violence and other threats, and so even in a democracy, there is a justification for censoring this content. The *UDHR*[69] and the *ICCPR*[70] support this exception and allow for limiting an individual's rights in favour of protecting the rights of others. Indeed, subsequent conventions have specifically held that other rights should limit free expression, such as the *Convention on the Elimination of all Forms of Racial Discrimination*[71] which condemns the dissemination of 'ideas based on racial superiority or hatred'.[72]

Moral Standards

Yet inherent in this exception for racial or other hate speech, is a statement of a particular moral standard. Moral standards are problematic as they are difficult to define – what is

---

[65] Dauterman, above n 51, 177; Hillary Clinton, 'Remarks on Internet Freedom' (Speech delivered at the Newseum, Washington DC, 21 January 2010) <http://www.state.gov/secretary/rm/2010/01/135519.htm> at 15 July 2010.
[66] Yaman Akdeniz, *Racism on the Internet* (2009) 12.
[67] Ibid.
[68] Ibid.
[69] *UDHR*, art 29(2).
[70] *ICCPR*, art 19(3).
[71] Opened for signature 21 December 1965, 660 UNTS 195 (entered into force 4 January 1969).
[72] Ibid, art 4.

offensive to one person may be acceptable to another. It could be argued that democracy itself provides a system for determining such community standards, and censorship on this basis therefore represents community consensus. However, democracy can be characterised as simply the voice of the majority. Minorities advocating opinions considered absurd or offensive by the majority stand to benefit most from free speech.[73]

Defining a moral standard for censoring 'offensive' content is particularly challenging on the Internet because so many diverse communities have access to the same material.[74] Unlike books and films where publication and imports can be controlled domestically, content uploaded on the Internet in one country immediately becomes accessible in other countries, including those where it may be banned.

Even within the same country, moral standards can change over time, and free speech can encourage the ongoing development of these standards through open discussion and debate.[75] Today, there may be consensus opposing various forms of discrimination (for example, gender, race, sexual orientation), but previously consensus supported these discriminatory practices. For example, in 1982 the UN Human Rights Commission allowed the Finnish Government to censor television and radio programs which merely discussed discrimination against homosexuals,[76] on the basis that the content was 'offensive' and the government was entitled to protect Finnish moral values under the ICCPR.[77] However, by 1999 the consensus had changed: the government repealed its discriminatory laws and today, Finland recognises same sex civil partnerships.[78]

As such, censorship on the grounds of the perceived current moral standard is difficult to define, especially in an international environment or over time, and has the potential to block important political discussion, silencing emerging and minority opinions.

---

[73] Winfried Brugger, 'The Treatment of Hate Speech in German Constitutional Law (Part I)' (2002) 3(12) German Law Journal 1, 1.
[74] Richard Garnett, 'Regulating Foreign-Based Internet Content: A Jurisdictional Perspective' (2000) 23(1) *University of New South Wales Law Journal* 227, 228.
[75] Google, above n 15, 8.
[76] The material was an interview regarding workplace discrimination and similar television programs: *Hertzberg v Finland* (1985) CCPR/C/OP/1 [2.2]-[2.5].
[77] Ibid [10.2]-[10.4].
[78] Helsingin Sanomat, *Parliament narrowly passes law allowing same-sex registration* (2001) <http://www2.hs.fi/english/archive/news.asp?id=20010928IE9> at 28 October 2010.

Indirect Harm

In addition to content which directly endangers the community, some content can be indirectly harmful to others. Racist speech can affect the self-esteem of the people to whom it is directed, and contribute to the oppression of a community by encouraging prejudice.[79] As demonstrated in *Jones v Toben*,[80] Holocaust denial is an example of speech which is disrespectful to victims and their familles, and which can cause great pain to the Jewish community without actually posing any direct threats.[81] On this broader interpretation of harm, there are clear public benefits in the censorship of Holocaust denial content.

Pornography

Pornography is particularly relevant to the Internet censorship debate. Governments around the world have attempted to restrict access to this material.[82] Responses have ranged from censoring all pornographic material, such as in Pakistan and Syria,[83] to attempting to prevent access to minors, as attempted in the US.[84]

Proponents of censoring pornography argue that this material is immoral and corrupts the viewer. For example, Dworkin, MacKinnon and others argue that pornography sexualises violence, legitimises sexual abuse, and encourages viewers to commit sexual crimes.[85] While there is little statistical evidence supporting these claims, MacKinnon quotes a number of

---

[79] Jeannine Bell, 'Restraining the Heartless: Racist Speech and Minority Rights' (2010) 84 *Indiana Law Journal* 963, 966-7.
[80] 255 ALR 238.
[81] *Jones v Toben* (2009) 255 ALR 238, 242-3.
[82] Steven Gey, 'The Apologetics of Suppression: The Regulation of Pornography as Act and Idea' (1988) 86(7) *Michigan Law Review* 1564, 1564.
[83] Nick, *Top 10 Countries Censoring the Web* (2008) DailyBits <http://www.dailybits.com/top-10-countries-censoring-the-web/> at 28 October 2010.
[84] The *Communications Decency Act*, 47 USCS § 233 (1996) and *Child Online Protection Act*, 47 USC § 231 (1998) were overturned for blocking too much adult speech: *Reno*, 521 US 844, 874-5 (1997); *Ashcroft v ACLU*, 535 US 564 (2002). The *Children's Internet Protection Act*, Pub L 106-554, 114 Stat 2763A-335 (1999) imposes a PC filter on school and library computers and survived a challenge in *United States v American Library Association*, 539 US 194 (2003).
[85] Andrea Dworkin, 'Against the Male Flood: Censorship, Pornography, and Equality' (1985) 8 *Harvard Women's Law Journal* 1, 528; Catharine MacKinnon, 'Pornography, Civil Rights and Speech' in Catherine Itzin (ed), *Pornography: Women, Violence and Civil Liberties* (1992) 456, 461-3, 473-8.

disturbing examples.[86] Pornography which appears to encourage or normalise violence or abuse, should be censored on the same basis as speech which incites violence. Using a harm-based test in censoring pornography obviates any need to rely on a volatile moral standard. Even pornographic material which is not explicitly violent may be offensive to some, but imposing this standard would be imposing the views of one part of the community on the activities of all.

Protecting children from exposure to sexual activity is a separate issue. Children are more vulnerable and may not be in a position to make informed decisions about or understand this material. This is especially true for younger children.[87] As recognised in *Ginsberg v New York*,[88] the freedom of adults to see or read material concerning sex should not extend to children. Further, governments (and parents) have a role in protecting youth from material which could be harmful to them.[89]

Child Pornography

According to the US Government, circulation of child pornography had been almost completely eradicated by the mid-1980s.[90] However, the Internet has provided a new means of distribution,[91] and this is now considered a multi-billion dollar industry.[92] The apparent anonymity of the Internet allows paedophiles to share material easily, while the Internet's international reach allows access to material produced in any country to be accessed globally.[93]

---

[86] MacKinnon, above n 85, 477-80; Deborah Cameron and Elizabeth Frazer, 'On the Question of Pornography and Sexual Violence: Moving Beyond Cause and Effect' in Catherine Itzin (ed), *Pornography: Women, Violence and Civil Liberties* (1992) 359, 361-7.
[87] Tania Voon, 'Online Pornography in Australia: Lessons from the First Amendment' (2001) 24(1) *University of New South Wales Law Journal* 142, 151.
[88] 390 US 629 (1968).
[89] *Ginsberg v New York,* 390 US 629, 636-9 (1968).
[90] US Department of Justice, *Child Pornography* (2007) <http://www.justice.gov/criminal/ceos/childporn.html> at 6 September 2010.
[91] Lesli Esposito, 'Regulating the Internet: The New Battle against Child Pornography' (1998) 30 *Case Western Reserve Journal of International Law* 541, 541.
[92] National Center for Missing & Exploited Children, *Child Porn Among Fastest Growing Internet Businesses* (2005) <http://www.ncmec.org/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2064> at 6 September 2010.
[93] Esposito, above n 91, 541-3.

In contrast to pornography depicting adults, the case for censorship of child pornography attracts almost absolute support.[94] The production of material depicting children engaged in sexual acts is harmful to the children involved and should be censored on this basis alone.

There is some debate surrounding the issue of 'cartoon pornography' and other computer-generated images. This issue was considered in *McEwen v Simmons*[95], where possession of pornographic pictures of the Simpson family children led to the plaintiff being charged with possession of child pornography. This case rested on the definition of 'person', and the Supreme Court of NSW held that this extended to cartoon representations of fictional people.[96] However, while these images did not involve children in their production, Adams J noted that they could still be used for grooming children.[97] Such images can reinforce the behaviour of paedophiles and could be used to lower a child's inhibitions to sexual activity.[98] On this basis, all images depicting children engaged in sexual acts should be censored.

The Harm Principle

This discussion highlights the difficult balancing act between preventing access to certain content and allowing individuals to communicate freely.

If any material is to be censored, this must accord with a clear principle defining the boundaries of acceptable censorship. It will never be possible to pre-judge all possible content which may come before a censor, but the principle should guide decision makers without being so vague as to allow abuse.[99] Failing to define such a standard could result in a chilling effect on speech, as individuals would be unable to reasonably judge how material would be treated.

A common theme identified in the above sections is that content which is sufficiently and specifically harmful to others should be censored. Protecting society from threats of violence

[94] Ibid 545.
[95] (2008) 73 NSWLR 10.
[96] Ibid 12, 20.
[97] Ibid 12.
[98] Esposito, above n 91, 545.
[99] David Hume and George Williams, 'Advocating terrorist acts and Australian censorship law' (2009) 20(1) *Public Law Review* 37, 37.

or encouragement of sexual abuse, protecting children from exploitation and even protecting people from indirect threats such as hurtful speech are examples of censorship which can be justified on this basis. Conversely, a purely moral standard should not be sufficient to justify censorship. Offensive political expression or non-violent pornography should not be restricted, except insofar as harmful consequences may follow from unregulated dissemination of such material. The benefits of free speech, especially on the Internet, are too important to disregard for a moral standard, particularly as such standards are fluid and difficult to define. The 'harm principle' advocated by Mill is built on the premise that legislation should not protect individuals from their own bad decisions, which only affect themselves, but that the law is justified in regulating the conduct between people.[100] The criteria for censorship should be based on this principle, recognising that material which causes either direct or indirect harm to others (including in its production) should be censored.

An exception to this rule should apply in the case of children. As a matter of public policy, governments have a role in protecting children from offensive content as children may not have the ability to assess or make decisions about material.[101] Even Mill argues that children should be protected from offensive content, and that parents have the right to protect their children from the communication of others.[102] On this basis, children should be prevented from accessing material which is offensive, at least without their parents' permission. In particular, restricting access to pornography or violent video games for minors is justifiable, even if this is not the case for adults.

A New Definition for Prohibited Content

The *Code* sets out the principle that adults should be allowed to access what they want, while restricting incitements to violence and protecting children from offensive content.[103] This is consistent with the harm principle. However, the *CCA* and the classification categories deviate from this position and impose moral tests. The Acts require an assessment of

[100] Marlin, above n 58, 210.
[101] EFA, *Submission to the DBCDE 'Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for Refused Classification material' consultation* (2010) 200.
[102] Marlin, above n 58, 215.
[103] *Code* r 1.

'morality, decency and propriety generally accepted by reasonable adults'[104] and the Restricted publication and X 18+ classifications refer to material which is 'likely to cause offence to a reasonable adult'.[105]

For a classification scheme which simply provides advice to consumers, it is reasonable for classification decisions to take account of moral standards, as this allows adults to make informed decisions about viewing or purchasing content. However, under the *BSA*, material classified as X 18+, Category 1 Restricted or Category 2 Restricted (generally nude, sexual or violent content) is censored on the Internet through the take down notice system (if hosted in Australia).[106] Applying this morally charged standard to prohibit content is unacceptable. As such, these classifications should be removed from the prohibited category of Internet content. This would bring Internet censorship into line with offline censorship for text and still images (publications), and with moving images (films) in the ACT and NT.[107]

This proposed standard would also align with the existing criminal offences relating to Internet content: only material which is illegal to distribute over the Internet would be censored.[108]

Removing the prohibition on this content for adults does not mean that it should be freely available. Access should be restricted to adults who seek the content. As previously discussed, a RAS can guard against inadvertent access, and along with parental supervision, can assist in preventing children from accessing this content. As such, MA15+, R18+, X18+, Category 1 Restricted and Category 2 Restricted content should continue to be prohibited if it is not subject to a RAS.

Content classified or likely to be classified as RC is also prohibited under the *BSA*. This category includes topics such as sex, drugs, cruelty or revolting phenomena, and similarly includes a moral test.[109] Google and the EFA have raised concerns that this could extend to

[104] *CCA* s 11(a); *Criminal Code Act 1995* (Cth) s 473.4.
[105] *Code* rr 2(2)-(3), 3(2).
[106] *BSA* sch 7 cls 20(2), 47(1), 62(1).
[107] On the same argument, offline X 18+ films should not be censored in the states.
[108] However, not all material which is illegal to distribute over the Internet would necessarily be censored. For example, *Criminal Code Act 1995* (Cth) s 474.17 would extend to all RC material, but it may extend further, depending on the circumstances of particular cases.
[109] *Code* rr 2(1), 3(1), 4(1).

censoring a broad range of politically controversial material.[110] To bring the level of censorship into line with the principles outlined above, an additional test based on harm should be introduced into this classification. This would achieve the goal already stated in the *Classification Code*: that adults should be able to access the material they want, while restricting that content necessary to protect others in the community. Material which incites violence or terrorism, or is child pornography or violent pornography clearly causes harm and would remain censored under this additional test, while political expression surrounding topics such as sex or drug use could no longer be censored on the basis of the prevailing moral values.

Recommendation 5:
That the definition of 'prohibited content' in the *BSA* be amended to only prohibit RC content to adults.

Recommendation 6:
That the RC classification category be amended to include a harm test.

Note: Recommendation 1 above also proposed amending the definition of 'prohibited content' in the *BSA*. Recommendation 1 proposed not prohibiting content equivalent to Category 1 or Category 2 Restricted content, on grounds of media neutrality. By proposing to only prohibit RC content (to adults), Recommendation 5 would also see Category 1 and Category 2 Restricted material not prohibited, but also X18+ content.

[110] Stephen Collins, *The truth about refused classification* (2010) Australian Broadcasting Commission <http://www.abc.net.au/unleashed/40072.html> at 14 October 2010; Google, above n 15, 8.

Question 29: In what other ways might the framework for the classification of media content in Australia be improved?

Category 1 Restricted Content

A peculiar situation arises under the *BSA* in relation to Category 1 Restricted online versions of existing publications. Content is 'potential prohibited content' if there is a substantial likelihood that the content is RC or Category 2 Restricted, however content is not potential prohibited if it is likely to be classified as Category 1 Restricted.[111] As such, ACMA would not refer this material to the Board or issue an interim take down notice. However, Category 1 Restricted material is included in the definition of 'prohibited content'.[112] If the Board were to classify the same content on application from another party, it would become prohibited. Accordingly, content is allowed to remain on the Internet even though ACMA considers that it would be likely to be prohibited if it were classified.

This situation creates an anomaly in the classification scheme and should be remedied. Using the same classification categories in the definitions of prohibited content and potential prohibited content would be more consistent. Accordingly, the definitions of prohibited content and potential prohibited content should either both include, or both exclude, Category 1 Restricted material.

Recommendations 1 and 5 in this submission advocate removing both Category 1 Restricted and Category 2 Restricted content from the definition of both prohibited content and potential prohibited content, which would also remove this anomaly.

> **Recommendation 7**:
> That the definitions of 'prohibited content' and 'potential prohibited content' in the *BSA* include the same classification categories.

[111] *BSA* sch 7 cl 21(2).
[112] *BSA* sch 7 cl 20(2).

Public Confidence

Integrity Requirements for Internet Censorship

If a system of Internet censorship is to be maintained under the classification system, a set of safeguards is necessary to ensure that the system is not abused. Any restriction on free speech can lead to further restrictions: there is always the opportunity to argue by analogy that other material is sufficiently similar to that censored.[113] For the censorship process to retain public confidence, the system must maintain a high level of integrity which mitigates the risk of abuse.[114]

Censorship decisions should be independent of the political process to avoid real or perceived political abuse. Further, as a matter of natural justice, those parties who have their material censored should be informed and have access to review and appeals processes.

The greatest protection against abuse is to ensure that the process is open and transparent, with publicly available assessment criteria and the publishing of censorship decisions. This would allow citizens to assess the rationale for censorship and gain confidence that the type of material being blocked is appropriate.[115]

Analysis and Improvements

Classification decisions are made by the Board, which is an independent statutory body. While the Government can request that decisions be reviewed,[116] there is no provision for it to overrule decisions. This satisfies the political independence test.

Critics argue that potential prohibited content hosted outside Australia is not subject to assessment by the Board.[117] Instead, ACMA makes a determination based on its opinion of how the Board would classify the content. However, as these pages are only added to an optional filter list, the determination is better characterised as advice than censorship, and is therefore acceptable.

---

[113] Ibid 230.
[114] EFA, above n 101, 9.
[115] Derek Bambauer, 'Filtering in Oz: Australia's Foray into Internet Censorship' (Working Paper No 125, Brooklyn Law School, 2008) 20.
[116] *BSA* sch 7 cls 28(2)(a)(i), 30(1)(a).
[117] Cf *BSA* sch 7 cl 47(1)(b).

Classification decisions can be appealed to the Classification Review Board (a similarly independent body) and appeals can be lodged by anyone aggrieved by the decision.[118] Decisions by ACMA to issue take down notices can be appealed to the Administrative Appeals Tribunal.[119] However, only content hosts have this right.[120] The actual content publisher would need to rely on their content host to lodge a complaint on their behalf. There is also no requirement to notify the content publisher when a take down notice is issued.[121] To improve the accountability and transparency of the classification scheme, content publishers should be given the right to be notified of classification decisions, and the right to appeal these decisions.

Additionally, the process lacks transparency. While the classification criteria are publicly available, classification decisions for websites are not published and are exempt from freedom of information requests[122] (in contrast to classification decisions for films, publications and computer games).[123] Critics have referred to this as 'secret state censorship'.[124] However, even EFA agrees that there is a reasonable justification for keeping some blacklists secret.[125] For material which is hosted overseas, ACMA only has the authority to add the webpage to their optional commercial filtering blacklist, and the content remains on the Internet. Publishing an Australian Government verified list of child pornography and other prohibited sites would only draw this material to the attention of offenders. As material hosted overseas is not censored, secrecy does not undermine the list's integrity as it would for content subject to removal.

However, this reasoning does not apply for Australian web hosts. After confirming that a take down notice has been complied with, ACMA should publish details identifying the material censored, as currently occurs for films, computer games and publications, in order to improve transparency.[126]

---

[118] *BSA* sch 7 cl 30(1)(d).
[119] *BSA* sch 7 cl 113(1)(a)-(b).
[120] *BSA* sch 7 cl 113(2).
[121] EFA, above n 101, 2.
[122] *Freedom of Information Act 1982* (Cth) s 7(2), sch 2 pt II div 1 (d); Vaile and Watt, above n 12, 27.4.
[123] *CCA* s 27(1)(a).
[124] Carolyn Dalton, *Google Submission to ACMA's Draft RAS Declaration* (2007), 15.3.
[125] EFA, above n 101, 2.
[126] See, Classification Board, *Search the Classification Database* (2010) <http://www.classification.gov.au/www/cob/find.nsf/Search?OpenForm> at 22 October 2010.

As such, the existing scheme could be improved by adding appeal and notice rights, and by publishing decisions once Australian content has been removed.

Recommendation 8:
That content publishers be given the right to be notified of classification decisions.

Recommendation 9:
That content publishers be given the right to appeal classification decisions.

Recommendation 10:
That after confirming a take down notice (relating to Australian hosted content) has been complied with, ACMA publish details identifying the material censored.

Bibliography

1. Articles/Books/Reports

Akdeniz, Yaman, *Racism on the Internet* (2009).

Argy, Philip, 'Internet Content Regulation: An Australian Computer Society Perspective' (2000) 23(1) *University of New South Wales Law Journal* 265.

Australian Communications and Media Authority, *Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety* (2008).

Australian Law Reform Commission, *Film and Literature Censorship Procedure*, Report No 55 (1991).

Bambauer, Derek, 'Cybersieves' (Working Paper No 149, Brooklyn Law School, 2009).

Bambauer, Derek, et al, 'Internet Filtering in China in 2004-2005: A Country Study' (2005).

Bambauer, Derek, 'Filtering in Oz: Australia's Foray into Internet Censorship' (Working Paper No 125, Brooklyn Law School, 2008).

Bell, Jeannine, 'Restraining the Heartless: Racist Speech and Minority Rights' (2010) 84 *Indiana Law Journal* 963.

Berg, Terrence, 'The Changing Face of Cybercrime: New Internet Threats Create Challenges to Law Enforcement' (2007) 86(6) *Michigan Bar Journal* 18.

Berkeley Technology Law Journal Editors, 'Additional Developments in Constitutional Law: American Civil Liberties Union v. Reno' (2002) 17(1) *Berkeley Technology Law Journal* 467.

Bernard, Chris, 'The Child Online Protection Act: Can the COPA Cope with Constitutional Scrutiny in Light of Reno v. ACLU ' (1999) 45 *Wayne Law Review* 1665.

Blackshild, Tony and Williams, George, *Australian Constitutional Law and Theory* (2006).

Bronitt, Simon and McSherry, Bernadette, *Principles of Criminal Law* (2005).

Brookshear, J, *Computer Science: An Overview* (8th ed, 2005).

Brugger, Winfried, 'The Treatment of Hate Speech in German Constitutional Law (Part I)' (2002) 3(12) *German Law Journal* 1.

Brugger, Winfried, 'The Treatment of Hate Speech in German Constitutional Law (Part II)' (2003) 4(1) *German Law Journal* 23.

Bryant, Randel and O'Hallaron, David, *Computer Systems: A Programmer's Perspective* (2003).

Butt Peter, *Concise Australian Legal Dictionary* (2004).

Cameron, Deborah and Frazer, Elizabeth, 'On the Question of Pornography and Sexual Violence: Moving Beyond Cause and Effect' in Itzin, Catherine (ed), *Pornography: Women, Violence and Civil Liberties* (1992) 359.

Caso, Frank, *Censorship* (2008).

Chen, Peter, 'Pornography, Protection, Prevarication: The Politics of Internet Censorship' (2000) 23(1) *University of New South Wales Law Journal* 221.

Commonwealth Science and Industrial Research Organisation, *Effectiveness of Internet Filtering Software Products* (2001).

Dalton, Carolyn, *Google Submission to ACMA's Draft RAS Declaration* (2007).

Dauterman, Walter, 'Internet Regulation: Foreign Actors and Local Harms - at the Crossroads of Pornography, Hate Speech, and Freedom of Expression' (2002) 28 *North Carolina Journal of International Law and Commercial Regulation* 177.

Department of Broadband, Communications and the Digital Economy, *Internet Service Provider Content Filtering Pilot: Technical Testing Framework* (2009).

Department of Broadband, Communications and the Digital Economy, *Outcome of public consultation on measures to increase accountability and transparency for refused classification material* (2010).

Depken, Craig, 'The Demand for Censorship: Who Supports Internet Censorship?' (2006) 11(9) *First Monday* 1.

Dines, Gail, Jensen, Robert and Russo, Ann, *Pornography: The Production and Consumption of Inequality* (1998).

Dollimore, *Sex, Literature and Censorship* (2001).

Dworkin, Andrea, 'Against the Male Flood: Censorship, Pornography, and Equality' (1985) 8 *Harvard Women's Law Journal* 1.

Eisenberg, Julie, 'Safely Out of Sight: The Impact of the New Online Content Legislation on Defamation Law' (2000) 23(1) *University of New South Wales Law Journal* 232.

Electronic Frontiers Australia, *Submission to the DBCDE 'Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for Refused Classification material' consultation* (2010).

Enex TestLab, *Internet Service Provider (ISP) Content Filtering Pilot Report* (2009).

Esposito, Lesli, 'Regulating the Internet: The New Battle against Child Pornography' (1998) 30 *Case Western Reserve Journal of International Law* 541.

Fankhauser, Caitlin and Scott, Veronica, 'It's different on the internet: regulating online content' (2010) 13(1) *Internet Law Bulletin* 200.

Feeley, Matthew, 'EU Internet Regulation Policy: The Rise of Self-Regulation' (1999) 22(1) *Boston College International and Comparative Law Review* 159.

Flood, Michael and Hamilton, Clive, *Regulating Youth Access to Pornography* (2003).

Flood, Michael and Hamilton, Clive, *Youth and Pornography in Australia* (2003).

Garnett, Richard, 'Regulating Foreign-Based Internet Content: A Jurisdictional Perspective' (2000) 23(1) *University of New South Wales Law Journal* 227.

Garry, Patrick, 'Defining Speech in an Entertainment Age: The Case of First Amendment Protection for Video Games' (2004) 57(1) *Southern Methodist University Law Review* 101.

Gerrand, Peter, 'Will our National Broadband Network support network neutrality and avoid Internet censorship?' (2009) 59 *Telecommunications Journal of Australia* 15.1.

Gey, Steven, 'The Apologetics of Suppression: The Regulation of Pornography as Act and Idea' (1988) 86(7) *Michigan Law Review* 1564.

Godwin, Mike, *Cyber rights: defending free speech in the digital age* (1st ed, 1998).

Google, *Mandatory ISP Level Filtering: Submission to the Department of Broadband, Communications and the Digital Economy* (2010).

Greenwood, Jeremy and Guner, Nezih, 'Social Change' (Working Paper No DP6125, Universidad Carlos III de Madrid; Centre for Economic Policy Research, 2008).

Grossman, Dave and DeGaetano, Gloria, *Stop teaching our kids to kill: a call to action against TV, movie & video game violence* (1999).

Heins, Marjorie, Cho, Christina and Feldman, Ariel, *Internet Filters: A Public Policy Report* (2nd ed, 2006).

Hull, Gorden, 'Overblocking Autonomy: The Case of Mandatory Library Filtering Software' (2009) 42 *Continental Philosophy Review* 81.

Hume, David and Williams, George, 'Advocating terrorist acts and Australian censorship law' (2009) 20(1) *Public Law Review* 37.

Johnson, Paul, 'Law, Morality and Disgust: The Regulation of "Extreme Pornography" in England and Wales' (2010) 19 *Social & Legal Studies* 147.

Kelly, Liz, 'Pornography and Child Sexual Abuse' in Itzin, Catherine (ed), *Pornography: Women, Violence and Civil Liberties* (1992) 113.

Linsley, William, 'Pornography: Research Advances and Policy Considerations' in Zillmann, Dolf and Bryant, Jennings (ed), *The Case Against Censorship of Pornography* (1989) 343.

Lumby, Catharine and Crawford, Kate, *The Adaptive Moment: A Fresh Approach to Convergent Media in Australia* (2011).

Lumby, Catharine, Lelia Green and John Hartley, *Untangling The Net: The Scope of Content Caught By Mandatory Internet Filtering* (2009).

MacKinnon, Catharine, 'Pornography, Civil Rights and Speech' in Itzin, Catherine (ed), *Pornography: Women, Violence and Civil Liberties* (1992) 456.

Marlin, Randal, *Propaganda and the ethics of persuasion* (2003).

McGlynn, Clare and Rackley, Erika, 'Criminalising Extreme Pornography: A Lost Opportunity' (2009) 4 *Criminal Law Review* 245.

McGlynn, Clare and Rackley, Erika, 'Striking a balance: arguments for the criminal regulation of extreme pornography' (2007) *Criminal Law Review* 677.

Meiklejohn, Alexander, 'The First Amendment is an Absolute' [1961] *Supreme Court Review* 245.

Mill, John Stuart, *On Liberty* (1859).

NetAlert Limited, *A Study on Server Based Internet Filters: Accuracy, Broadband Performance Degradation and some Effects on the User Experience* (2006).

NSW Council for Civil Liberties, *Submission to the ACMA on the draft RAS Declaration 2007* (2007).

Penfold, Carolyn, 'Australian Internet Censorship in International Context' (2001) 14 *Cyberspace Law Resources* <http://www.austlii.edu.au/au/other/CyberLRes/2001/14/> at 4 August 2010.

Preston, Cheryl, 'Internet Porn, ICANN, and Families: A Call to Action' (2008) *Journal of Internet Law* 3.

Przybylski, Paul, 'A Common Tool for Individual Solutions: Why Countries Should Establish an International Organization to Regulate Internet Content', (2007) 9(3) *Vanderbilt Journal of Entertainment and Technology Law* 927.

Raiche, Holly, *Internet Society of Australia Submission: in response to the Australian Communications and Media Authority consultation paper, Restricted Access System Declaration* (2007).

Rozanski, Stella, 'Obscenity: Common Law and the Abuse of Women' (1991) 13 *Adelaide Law Review* 163.

Scott, Brendan, 'Silver Bullets and Golden Egged Geese: A Cold Look at Internet Censorship' (2000) 23(1) *University of New South Wales Law Journal* 215.

Stevens, Richard, *TCP/IP Illustrated, Volume 1: The Protocols* (1994).

Svantesson, Dan, 'Sexting and Australia's regulation of child pornography' (2010) 13(2) *Internet Law Bulletin* 34.

Tanenbaum, Andrew, *Computer Networks* (4th ed, 2003).

Thampapillai, Dilan, 'Facebook or Racebook? Time for a different approach' (2010) 13(2) *Internet Law Bulletin* 30.

Trager, Robert and Turner, Sue, 'The Internet down Under: Can Free Speech Be Protected in a Democracy without a Bill of Rights' (2000-2001) 23 *University of Arkansas at Little Rock Law Review* 123.

Tsesis, Alexander, 'Hate in Cyberspace: Regulating Hate Speech on the Internet.' (2001) 38(3) *San Diego Law Review* 818.

Urbas, Gregor and Fouracre, Kendra, 'Obligations and Liability of ISPs as Guardians of Internet Content: Comparative Perspectives' (2010) 2 *Computer Law Review International* 33.

Vaile, David and Watt, Renée, 'Inspecting the despicable, assessing the unacceptable: Prohibited packets and the Great Firewall of Canberra' (2009) 59(2) *Telecommunications Journal of Australia* 27.1.

Voon, Tania, 'Online Pornography in Australia: Lessons from the First Amendment' (2001) 24(1) *University of New South Wales Law Journal* 142.

Wilson, Nigel, 'Regulating the information age – How will we cope with technological change?' (2010) 33 *Australian Bar Review* 119.

Zwart, Melissa de, 'Freedom of speech in virtual worlds: learning to live together virtually' (2010) 13(1) *Internet Law Bulletin* 192.

2. Case Law

America Civil Liberties Union v Gonzales, 478 F Supp 2d 775 (ED Pa, 2006).

America Civil Liberties Union v Reno, 929 F Supp 824 (ED Pa, 1996).

Australian Capital Television v Commonwealth (1992) 177 CLR 106.

Adultshop.Com Ltd v Members of the Classification Review Board (2007) 243 ALR 752.

Ashcroft v American Civil Liberties Union, 535 US 564 (2002).

Capital Duplicators Pty Ltd v Australian Capital Territory (No 2) (1993) 178 CLR 558.

FCC v Pacifica Foundation, 438 US 726 (1978).

Ginsberg v New York, 390 US 629 (1968).

Hertzberg v Finland (1985) CCPR/C/OP/1.

Jones v Toben (2009) 255 ALR 238.

Lange v Australian Broadcasting Corporation (1997) 189 CLR 520.

Levy v Victoria (1997) 189 CLR 579.

McEwen v Simmons (2008) 73 NSWLR 10.

Nationwide News v Wills (1992) 177 CLR 1.

NSW Council for Civil Liberties Inc v Classification Review Board (No. 2) (2007) 159 FCR 108.

RAV v St. Paul, 505 US 377 (1992).

Reno v American Civil Liberties Union, 521 US 844 (1997).

Sanders v Acclaim Entertainment, 188 F Supp 2d 1264 (D Colo, 2002).

United States v American Library Association, 539 US 194 (2003).

Yahoo! v La Ligue Contre Le Racisme et L'antisemitisme, L'union Des Etudiants Juifs De France, 433 F 3d 1199 (9th Cir, 2006).

3. Legislation

Australian Constitution.

Broadcasting Services Act 1992 (Cth).

Child Online Protection Act, 47 USC § 231 (1998).

Children's Internet Protection Act, Pub L 106-554, 114 Stat 2763A-335 (1999).

Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (ACT).

Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic).

Classification (Publications, Films and Computer Games) Act 1995 (Cth).

Classification (Publications, Films and Computer Games) Act 1995 (SA).

Classification (Publications, Films and Computer Games) Enforcement Act 1995 (NSW).

Classification (Publications, Films and Computer Games) Enforcement Act 1996 (WA).

Classification (Publications, Films and Computer Games) Enforcement Act 1995 (Tas).

Classification of Computer Games and Images Act 1995 (Qld).

Classification of Publications, Films and Computer Games Act (NT).

Communications Decency Act, 47 USCS § 233 (1996).

Crimes Act 1900 (ACT).

Crimes Act 1900 (NSW).

Crimes Prevention Act 1916 (NSW).

Criminal Code 2002 (ACT).

Criminal Code Act 1995 (Cth).

National Classification Code 2005 (Cth).

Restricted Access Systems Declaration 2007 (Cth).

Telecommunications Act 1997 (Cth).

United States Constitution.

4. Treaties

Convention on Cyber Crime, opened for signature 23 November 2001, ETS no 185 (entered into force 1 July 2004).

International Convention on the Elimination of all Forms of Racial Discrimination opened for signature 21 December 1965, 660 UNTS 195 (entered into force 4 January 1969).

International Covenant on Civil and Political Rights opened for signature on 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

Universal Declaration of Human Rights, UNGA Res 217 A (III) (1948).

5. Other Sources

Al Jazeera, *Ahmadinejad 'set for Iran victory'* (2009) <http://english.aljazeera.net/news/middleeast/2009/06/200961219574914973 3.html> at 10 September 2010.

Attorney-General's Department, *An R 18+ Classification for Computer Games - Public Consultation* (2009) <http://www.ag.gov.au/gamesclassification> at 8 October 2010.

Attorney-General's Department, *Classification Policy* (2010) <http://www.ag.gov.au/www/agd/agd.nsf/page/Classification_policy> at 8 October 2010.

Attorney-General's Department, *National classification scheme* (2010) <http://www.ag.gov.au/www/agd/agd.nsf/Page/Classificationpolicy_NationalClassificationScheme#section11> at 8 October 2010.

Australian Associated Press, *Greens reject internet filter* (2010) The Australian <http://www.theaustralian.com.au/national-affairs/greens-reject-internet-filter/story-fn59niix-1225905900898> at 28 October 2010.

Australian Broadcasting Corporation, 'Access Denied', *Four Corners*, 10 May 2010, <http://www.abc.net.au/4corners/content/2010/s2895350.htm> at 14 July 2010.

Australian Broadcasting Corporation, 'Q and A live from Melbourne', *Q&A*, 26 March 2009, <http://www.abc.net.au/tv/qanda/txt/s2521164.htm> at 10 July 2010.

Australian Broadcasting Corporation, *US concern over Australian internet filter* (2010) <http://www.abc.net.au/news/stories/2010/03/29/2858931.htm> at 25 October 2010.

Australian Communications and Media Authority, *Frequently Asked Questions* (2009) <http://www.acma.gov.au/WEB/STANDARD/pc=PC_310147#whatwill> at 2 July 2010.

Australian Communications and Media Authority, *Minimum verification system requirements* (2009) <http://www.acma.gov.au/scripts/nc.dll?WEB/STANDARD/1001/pc=PC_90159> at 5 October 2010.

Australian Communications and Media Authority, *Online content complaint statistics* (2010) <http://www.acma.gov.au/WEB/STANDARD/pc=PC_90105> at 7 October 2010.

Beazley, Kim, *Plan to shield young from net vice: Clean Feed Policy: Q&A* (2006) Internet Archive: Labor eHerald <http://web.archive.org/web/20080719070626/http://eherald.alp.org.au/articles/0306/natp24-01.php> at 10 October 2010.

Berkovic, Nicola and Kelly, Joe, *Conroy shelves net filter as election looms* (2010) The Australian <http://www.theaustralian.com.au/news/conroy-shelves-net-filter-as-election-looms/story-e6frg6n6-1225889985524> at 7 August 2010.

Bray, Hiawatha, *Finding a way around Iranian censorship* (2009) The Boston Globe <http://www.boston.com/business/technology/articles/2009/06/19/activists_utilizing_twitter_web_proxies_to_sidestep_iranian_censorship/> at 10 September 2010.

Brooks, Paul, 'Internet Content Filtering: What it is – and still isn't' (Paper presented at the UNSW Cyberspace Law and Policy Centre Internet Filtering and Censorship conference, Sydney, 4 March 2009) <http://www.bakercyberlawcentre.org/censorship/forum2.htm> at 17 July 2010.

Browzer, *Browse the web anonymously at school and work!* (2010) <http://www.browzer.info/> at 20 October 2010.

Classification Board, *Search the Classification Database* (2010) <http://www.classification.gov.au/www/cob/find.nsf/Search?OpenForm> at 22 October 2010.

Cleary, Ray, *Protecting children online takes more than a filter* (2010) The Age <http://www.theage.com.au/opinion/society-and-culture/protecting-children-online-takes-more-than-a-filter-20100113-m6g8.html> at 28 October 2010.

Clinton, Hillary, 'Remarks on Internet Freedom' (Speech delivered at the Newseum, Washington, 21 January 2010) <http://www.state.gov/secretary/rm/2010/01/135519.htm> at 15 July 2010.

Collerton, Sarah, *Coalition vows to block internet filter* (2010) Australian Broadcasting Corporation <http://www.abc.net.au/news/stories/2010/08/05/2974827.htm> at 6 August 2010.

Colley, Andrew, *Fears web filter will cast net too wide* (2010) The Australian <http://www.theaustralian.com.au/business/media/fears-web-filter-will-cast-net-too-wide/story-e6frg996-1225846626626> at 10 October 2010.

Collins, Stephen, *The truth about refused classification* (2010) Australian Broadcasting Commission <http://www.abc.net.au/unleashed/40072.html> at 14 October 2010.

Conroy, Stephen, 'Federal Labor To Lead On Cyber-Safety' (Press Release, 19 November 2007) <http://web.archive.org/web/20071121143224/www.alp.org.au/media/1107/mscoit190.php> at 10 October 2010.

Conroy, Stephen, *Labor's Plan for Cyber-safety* (2007) Internet Archive: Australian Labor Party <http://web.archive.org/web/20080719180723/www.alp.org.au/download/now/labors_plan_for_cyber_safety.pdf> at 10 October 2010.

Conroy, Stephen, 'Measures to improve safety of the internet for families' (Press Release, 15 December 2009) <http://www.minister.dbcde.gov.au/media/media_releases/2009/115> at 15 September 2010.

Conroy, Stephen, 'Outcome of consultations on Transparency and Accountability for ISP Filtering of RC content' (Press Release, 9 July 2010) <http://www.minister.dbcde.gov.au/media/media_releases/2010/068> at 14 July 2010.

Coonan, Helen, 'NetAlert: Protecting Australian Families Online' (Press Release, 10 August 2007) <http://www.minister.dbcde.gov.au/coonan/media/media_releases/netalert_-_protecting_australian_families_online> at 28 October 2010.

Department of Broadband, Communications and the Digital Economy, *Measures to increase accountability and transparency for Refused Classification material* (2010) <http://www.dbcde.gov.au/all_funding_programs_and_support/cybersafety_plan/transparency_measures> at 14 July 2010.

Department of Broadband, Communications and the Digital Economy, *Internet Service Provider (ISP) filtering* (2010) <http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering> at 25 August 2010.

Electronic Frontiers Australia, *Internet Censorship Laws in Australia* (2008) <http://www.efa.org.au/Issues/Censor/cens1.html> at 3 August 2010.

Electronic Frontiers Australia, *Internet Censorship: Law & policy around the world* (2002) <http://www.efa.org.au/Issues/Censor/cens3.html> at 5 September 2010.

Electronic Frontiers Australia, *Labor's Mandatory ISP Internet Blocking Plan* (2009) <http://www.efa.org.au/censorship/mandatory-isp-blocking/> at 19 July 2010.

Electronic Frontiers Australia, *Restricted Access / Age Verification Systems* (1999) <http://www.efa.org.au/Publish/ABAresp9911.html> at 5 October 2010.

Facebook, *Statement of Rights and Responsibilities* (2010) <http://www.facebook.com/terms.php?ref=pf> at 28 October 2010.

Foo, Fran and Colley, Andrew, *ISP filtering legislation on the way* (2010) Australian IT <http://www.theaustralian.com.au/australian-it/filtering-legislation-on-the-way/story-e6frgakx-1225889109550> at 13 July 2010.

Foo, Fran, *Gillard should halt ISP filtering plan: Greens* (2010) The Australian <http://www.theaustralian.com.au/australian-it/gillard-should-halt-isp-filtering-plan-greens/story-e6frgakx-1225889467829> at 8 July 2010.

Gay Wedding Destinations, *Information on the Legal Status of Same Sex Marriage* (2010) <http://www.gayweddingdestinations.com/legalities.php> at 28 October 2010.

Grubb, Ben, *Coalition to dump 'flawed' internet filter* (2010) The Sydney Morning Herald <http://www.smh.com.au/technology/technology-news/coalition-to-dump-flawed-internet-filter-20100805-11kmv.html> at 7 August 2010.

Hamilton, Clive, *Net porn: Whose rights matter most?* (2008) Australian Broadcasting Corporation <http://www.abc.net.au/news/stories/2008/12/01/2433845.htm> at 30 October 2010.

Higginbottom, Nick and Ben Packham, Porn filters no barrier for net users (2007) Herald Sun <http://www.heraldsun.com.au/news/national/porn-filters-no-safety-net/story-e6frf7l6-1111114263646> at 20 October 2010.

Hirsch, Afua, *How to police popslash* (2009) The Guardian <http://www.guardian.co.uk/world/2009/jul/04/girls-scream-aloud-obscenity-laws> at 5 October 2010.

Horrocks, Peter, *Stop the blocking now* (2009) BBC <http://www.bbc.co.uk/blogs/theeditors/2009/06/stop_the_blocking_now.html> at 9 September 2010.

Jacobs, Colin, *Mandatory ISP Filtering* (2010) Electronic Frontiers Australia <http://www.efa.org.au/category/censorship/mandatory-isp-filtering/> at 12 July 2010.

Kelly, Joe and Foo, Fran, *Conroy delays controversial web filtering plan* (2010) Perth Now <http://www.perthnow.com.au/business/conroy-delays-controversial-web-filtering-plan/story-e6frg2rc-1225889852261> at 7 August 2010.

Kravets, David, *WikiLeaks Exposes Australian Web Blacklist* (2009) Wired <http://www.wired.com/threatlevel/2009/03/wikileaks-expos/> at 19 October 2010.

Lyle, Shelton, *Campaigns* (2010) Australian Christian Lobby <http://australianchristianlobby.org.au/featured-campaigns/> at 30 October 2010.

Maurushat, Alana, 'Evolving Role of ISPS: Political Hot Potato' (Paper presented at the UNSW Cyberspace Law and Policy Centre Internet Filtering and Censorship conference, Sydney, 4 March 2009) <http://www.bakercyberlawcentre.org/censorship/forum2.htm> at 17 July 2010.

Meichtry, Stacy, *Italy Says Google Trio Violated Boy's Privacy* (2010) The Wall Street Journal <http://online.wsj.com/article/SB10001424052748704240004575084851798366446.html?ru=yahoo&mod=yahoo_hs> at 30 October 2010.

Moses, Asher, *Ban naughty countries from the net: former intelligence chief* (2010) The Sydney Morning Herald <http://www.smh.com.au/technology/security/ban-naughty-countries-from-the-net-former-intelligence-chief-20101008-16as5.html> at 9 October 2010.

Moses, Asher, *Conroy backs down on net filters* (2010) The Sydney Morning Herald <http://www.smh.com.au/technology/technology-news/conroy-backs-down-on-net-filters-20100709-10381.html> at 11 July 2010.

Moses, Asher, *Conroy's net filter still alive and kicking* (2010) The Sydney Morning Herald <http://www.smh.com.au/technology/technology-news/conroys-net-filter-still-alive-and-kicking-20100910-1540s.html> at 10 September 2010.

Moses, Asher, *Government goes to war with Google over net censorship* (2010) The Age <http://www.theage.com.au/technology/technology-news/government-goes-to-war-with-google-over-net-censorship-20100330-r9bp.html> at 13 June 2010.

Moses, Asher, *Net filters may block porn and gambling sites* (2008) The Sydney Morning Herald <http://www.smh.com.au/articles/2008/10/27/1224955916155.html> at 10 October 2010.

National Australia Bank, *Customer help* (2010) <http://secure1.ubank.com.au/ub/web/customer-help/help-security#q4> at 28 October 2010.

National Center for Missing & Exploited Children, *Child Porn Among Fastest Growing Internet Businesses* (2005) <http://www.ncmec.org/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2064> at 6 September 2010.

NetAlert, *Protecting Australian Families Online* (2010) <http://www.netalert.gov.au/> at 30 October 2010.

Nick, *Top 10 Countries Censoring the Web* (2008) DailyBits <http://www.dailybits.com/top-10-countries-censoring-the-web/> at 28 October 2010.

O'Connor, Brendan, 'R 18+ Classification for Computer Games Consultation Report Released' (Press Release, 7 May 2010) <http://www.ministerhomeaffairs.gov.au/www/ministers/oconnor.nsf/Page/MediaReleases_2010_SecondQuarter_7May2010-R18+ClassificationforComputerGamesConsultationReportReleased> at 8 October 2010.

Parliament of Australia, *Joint Select Committee on Cyber-Safety – Terms of Reference* (2010) <http://www.aph.gov.au/house/committee/jscc/tor.htm> at 8 July 2010

Pettitt, Annie, 'New website takes right approach to internet safety for children' (Press Release, 19 February 2010) <http://www.savethechildren.org.au/images/documents/media/190210_-_Response_to_ThinkuKnow_website.pdf> at 1 October 2010.

Rural Funds Management, *New Anti-Money Laundering Laws* (2007) <http://www.ruralfunds.com.au/documents/Forms/AML_Notice_-_Direct_Clients.pdf> at 28 October 2010.

Sanomat, Helsingin, *Parliament narrowly passes law allowing same-sex registration* (2001) <http://www2.hs.fi/english/archive/news.asp?id=20010928IE9> at 28 October 2010.

Save the Children, et al, 'Joint Statement on Internet Censorship' (Press Release, July 2009) <http://www.savethechildren.org.au/component/content/article/78-media-listing-blog/190-joint-statement-on-internet-censorship.html> at 25 October 2010.

Selby, John, 'Internet Filtering' (Paper presented at the UNSW Cyberspace Law and Policy Centre Internet Filtering and Censorship conference, Sydney, 4 March 2009) <http://www.bakercyberlawcentre.org/censorship/forum2.htm> at 17 July 2010.

Sharp, Ari, *Child porn filter move hits snag* (2010) The Sydney Morning Herald <http://www.smh.com.au/technology/technology-news/child-porn-filter-move-hits-snag-20100712-107w3.html> at 14 July 2010.

Sharp, Ari, *Gillard to stick with web filter despite disquiet* (2010) Sydney Morning Herald <http://www.smh.com.au/technology/technology-news/gillard-to-stick-with-web-filter-despite-disquiet-20100707-100qe.html> at 8 July 2010.

Sharp, Ari, *Internet filter 'won't protect kids'* (2010) The Sydney Morning Herald <http://www.smh.com.au/technology/technology-news/internet-filter-wont-protect-kids-20100708-102ap.html> at 10 July 2010.

Sivasubramanian, Siva, 'Internet Filtering and Censorship Proposals' (Paper presented at the UNSW Cyberspace Law and Policy Centre Internet Filtering and Censorship conference, Sydney, 4 March 2009) <http://www.bakercyberlawcentre.org/censorship/forum2.htm> at 18 July 2010.

Tay, Liz, *ICT industry all nostalgic for NetAlert* (2010) ITNews <http://www.itnews.com.au/News/219281,ict-industry-all-nostalgic-for-netalert.aspx> at 29 October 2010.

The Associated Press, *Iran targets media after disputed election* (2009) MSNBC <http://www.msnbc.msn.com/id/31357829/ns/world_news-mideastn_africa/> at 28 October 2010.

Totaro, Paola, *Facebook child-porn ringleader jailed over 100,000 indecent images* (2010) The Sydney Morning Herald <http://www.smh.com.au/technology/technology-news/facebook-childporn-ringleader-jailed-over-100000-indecent-images-20100827-13ugq.html?autostart=1> at 28 August 2010.

US Department of Justice, *Child Pornography* (2007) <http://www.justice.gov/criminal/ceos/childporn.html> at 6 September 2010.

Vaile, David, 'Classification and Internet technical filtering' (Paper presented at the UNSW Cyberspace Law and Policy Centre Internet Filtering and Censorship conference, Sydney, 4 March 2009) <http://www.bakercyberlawcentre.org/censorship/forum2.htm> at 18 July.

Welch, Dylan, *Facebook failed to tell police about paedophile porn ring* (2010) The Sydney Morning Herald <http://www.smh.com.au/technology/facebook-failed-to-tell-police-about-paedophile-porn-ring-20100826-13ual.html> at 28 August 2010.