

University of New South Wales
University of New South Wales Faculty of Law Research Series
2009

Year 2009

Paper 7

Clean Feed: Australia's Internet Filtering
Proposal

Alana Maurushat*

Renée Watt†

*University of New South Wales

†University of New South Wales

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps09/art7>

Copyright ©2009 by the authors.

Clean Feed: Australia's Internet Filtering Proposal

Alana Maurushat and Renée Watt

Abstract

This article examines the Australian Federal government's proposal on internet filtering. Technical, policy and legal frameworks are discussed. A comprehensive comparative chart is provided looking at other countries which already have internet filtering in place.

Clean Feed: Australia's Internet Filtering Proposal

Alana Maurushat* and Renée Watt**

Forthcoming Internet Law Bulletin March 2009

The Australian Proposal in the International Context

The Australian Proposal

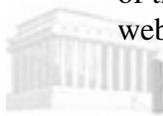
The Australian government is seeking to make the internet a safer place, especially for children. Cyber-safety was an electoral promise of the newly-appointed Labor government.¹ A key aspect of the Rudd government's cyber-safety program, unofficially known as Clean Feed, is a national internet filter.² This means legally mandating Internet Service Providers ('ISPs') such as Optus, Telstra and iiNet to implement technical means to filter out a prescribed list of websites. Sites containing images of child abuse, in particular child pornography, will be the initial focus of the list.

The government has not publicly stated its goals for the Clean Feed proposal; perhaps the project's aims remain unformulated even within the Labor Party. As there is no Australian legislation yet on internet filtering, important details of the scheme remain mysterious, and its configuration and scope may change. Once enacted, Clean Feed legislation will be open to the amendment of future governments. If Parliament defeats the eventual legislation, it is still possible that a number of ISPs will voluntarily implement internet filtering.

The criteria for evaluation of websites to be blocked remains nebulous. As the proposal currently stands, ACMA investigates complaints about 'prohibited content' based on a classification scheme of X18, R18, RC, and MA15+ (though rare). Materials classified as X18 or RC comprise the 1300 plus blacklist maintained by ACMA.³ Classification decisions of such content is secret; the blacklist remains unknown. Senator Fielding, a proponent of Clean Feed, has argued to expand the blacklist to include R18+ (eg. adult pornography) The Clean Feed proposal has two tiers:

- 1) **Blacklist Filtering:** The first tier comprises the mandatory filtration for all Australians (no possibility to opt-out) of sites on an ACMA-issued blacklist of 'child pornography' websites and 'other prohibited' materials, the scope of which remains unknown. ISPs must block such sites at the URL level. Circumvention of the blacklist will be illegal. Operating only on URLs, the filter will *not* block websites with 'child pornography' and 'other prohibited content' found on:

- Peer-to-peer systems (for example: bit torrent, Winny),



berkeley Electronic Press Legal Repository

- Encrypted channels,
- Chatrooms,
- MSN Instant Messaging, and
- Mobile phones.

It remains unknown whether Clean Feed, when confronted with an offensive URL, will block every website operating on a domain name or merely the specific offending material. (This represents the difference for example between YouTube – www.youtube.com being the domain name – and a specific video on YouTube).

- 2) **Content Filtering:** The second tier, operating on an opt-out basis, will block materials that are legal but potentially unwanted. The government has not delineated the scope of such material but likely examples include adult pornography and other ‘R’ rated material – content inappropriate for children but legal for adults. Circumvention will not be illegal. The filtering techniques for tier two filtering remain undefined. Potentially these could include URL blacklists, deep packet inspection, peer-to-peer content inspection, and URL and http content inspection.

National Internet Filters in Other Countries

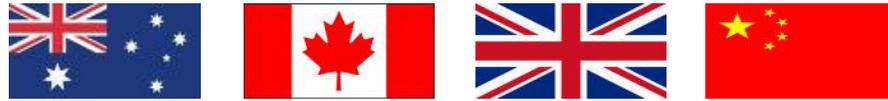
Governmental internet filtering is the realm not only of authoritarian regimes like China and Iran but also of such Western democracies as Canada, the United Kingdom, Sweden and France. In Canada and the United Kingdom informal government pressure led the countries’ major ISPs to ‘voluntarily’ institute internet filtering. The clearly articulated goal of these systems is to block inadvertent access to websites containing child pornography and child abuse materials. In countries such as France, Belgium and Germany, courts have ordered ISPs to block hate speech and the illegal peer-to-peer filesharing of copyright-protected materials.⁴ So Australia’s proposed system is unique among Western democracies: we will be the first of such nations to mandate internet filtering through formal legislation.

In Canada and the United Kingdom, using political influence instead of passing legislation mandating internet filtering may be strategic. By removing the process from the political arena Canada and the United Kingdom elude transparency and accountability. Legislating internet filtering in these countries would open the provisions to freedom of expression challenges under the *Human Rights Act 1998* (United Kingdom) and the *Charter of Rights and Freedoms 1982* (Canada); it is doubtful that mandatory internet filtering legislation would withstand such scrutiny.⁵ The same safeguards are not present in Australia. There is no Bill of Rights, nor any kind of wide human rights instrument covering freedom of expression. In theory, the constitutionally implied freedom of political communication could prevent an overly broad legislative internet filter, but case law indicates that in this context this right will be of limited consequence.⁶ The websites that Parliament blocks will thus be malleable to the political will and ethical values of the governing party *du jour*.



bepress Legal Repository

Table 1: Comparison between Australia’s proposed internet filter and filters in place in Canada, the United Kingdom and the People’s Republic of China.



	Australia	Canada	United Kingdom	People’s Republic of China
Legislating mandatory filtering at ISP level:	Yes	No	No	Yes – over 20 pieces of legislation affect filtering
Voluntary / Industry filtering at ISP level:	Perhaps – If legislation fails, ISPs may elect to filter	Yes – informal government pressure	Yes – informal government pressure	Yes – corporate self-censorship is prevalent
Opt-Out Provision:	No – Tier 1 Yes – Tier 2	No	No	No
Project Name:	Clean Feed	Cleanfeed Canada	Project Cleanfeed	Golden Shield Project known as ‘The Great Firewall of China’
Blacklist Filtering of Blocked URLs:	Yes	Yes	Yes	Yes
Purpose of Blacklist:	Unspecified	Blocking inadvertent access to child pornography materials with http protocol	Blocking inadvertent access to child pornography materials with http protocol	To block various types of illegal content
Type of Materials Blocked:	Child pornography and other unknown ‘illegal content’	Child pornography	Child pornography	Political content, graphic violence, unapproved news stories, child pornography, and other illegal content
Blacklist Maintained By:	ACMA (Australian Communications and Media Authority)	Cybertip.ca	Internet Watch Foundation	Ministry of Industry and Information; Central Propaganda Department; Ministry of Posts and Telecommunications
IP Address Blocking:	Not at this time	Not at this time	Not at this time	Yes
Deep Packet Inspection:	Not at this time	Yes	Yes	Yes
Purpose of Deep Packet Inspection:	NA	Traffic Shaping	Traffic Shaping	Traffic Shaping, Dataveillance & Surveillance
Other Heuristic Methods:	Yes	Yes	Yes	Yes
P2P:	Not at this time	Perhaps –	Perhaps –	Yes

		Content infringement (in negotiation with music industry)	Content infringement (in negotiation with music industry)	
Instant Messaging:	Not at this time	Not at this time	Not at this time	Yes
Scope Creep:	Inevitable	Yes – suicide sites, pro-terrorism sites, hate sites	Yes – suicide sites, graphic terrorist beheadings, pro-terrorism sites, hate sites	Yes – legislation written with standard vague and ambiguous clauses such as the ‘state security’ provision
Offence to Circumvent Filters:	Yes – not an offence to use a circumvention device such as a proxy for other purposes	No	No	Yes – not an offence to use a circumvention device such as a proxy for other purposes
Legislative Safeguards:	No – no Bill of Rights, constitutionally implied freedom of political communication very limited in this context and of little use as a safeguard	Limited – Charter of Human Rights does not bind corporations such as ISPs (no legislation compelling ISPs)	Limited – European Convention on Human Rights; relevant case law from the European Court of Human Rights	No – the human rights instruments are of little practical significance (Eg. Freedom of Expression is not an individual right)
Market Safeguard:	No – compulsory for all ISPs	Potentially – voluntary initiative subject to strong informal government pressure	Potentially – voluntary initiative subject to strong informal government pressure	None
Technical Safeguard:	No	Potentially – depends where the filtering routers are placed (Eg. router located on the backbone would affect all ISPs)	Potentially – depends where the filtering routers are placed (Eg. router located on the backbone would affect all ISPs)	Potentially – geographical region of access, and bandwidth capability affect ability to access materials



Technical and Legal Limits of Internet Filtering

General Attributes of Internet Filtering

One of the many myths surrounding the debate on internet filtering is that a filter operating at the ISP level will be more effective than filters that sit on the operating system of a personal computer. Up until 31 December 2008, these were freely available from the government under NetAlert's National Filter Scheme⁷. These filters operate on the exact same principles and will block identical websites. In short, the only difference is that a filter on an ISP will cost more and can be made mandatory for internet users Australia-wide.

One common problem with blacklist filters is the degradation of network speeds. The pilot tests of filtering in Tasmania found decreases in access speeds ranging from 3% to 86%.⁸ The extent of degradation depends on the amount of broadband available, passive (filter not in use) versus active (filtering of website on blacklist), and most importantly, on the type of filtering technology utilised.⁹ Statistics concerning the loss of network speed in areas with limited broadband, such as rural Australia, remain woolly. A mandatory national internet filter lies in stark contrast with the government's commitment to increase both broadband access and access speeds.¹⁰

As well, there are structural, logistical obstacles to the Australian implementation of a national internet filter. The internet in Australia developed using a free-form model with no central nodes or gateways. Internet traffic in China and Saudi Arabia, by way of contrast, flows through set 'choke points'.¹¹ This allows China, for example, to "deploy its networks to allow censorship to occur at multiple control points, from international gateways to the network backbone to regional network providers".¹² In the Australian context however:

How this distributed model compares to centralized filtering in terms of performance and effects on network speeds is not certain; filtering could be faster if placed closer to the network edge or faster if placed closer to the core where it could achieve efficiencies of scale and redundancy. It can also increase the challenge of keeping block lists up to date; as there are more network points where the lists are implemented, it becomes more challenging to ensure each list is properly updated.¹³

As of December 24, 2008, most ISPs in Australia are participating in trials of the filter. The results of these trials are yet to be finalised. It is unclear if they will be publicly available.

What Constitutes Child Pornography?

There is no universally accepted definition of "child pornography". The term is ambiguous even within Australia, where State and Federal definitions vary. At a Commonwealth level,

Child pornography material means material that depicts a person, or a representation of a person, who is, or appears to be, under 18 years of age and who is engaged in, or appears to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or is in the presence of a person who is engaged in, or appears to be engaged in, a sexual pose or sexual activity; and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive.¹⁴

Child pornographic materials include written narratives, animated cartoons (such as manga), and fictional depictions of abuse.¹⁵ The recent decision of *McEwen v Simmons*¹⁶ establishes that under New South Wales¹⁷ and Commonwealth¹⁸ law depictions of sexual acts among the children characters of the American cartoon “The Simpsons” constitute child pornography. Early last year police removed Australian artist Bill Henson’s photographs of naked prepubescent girls from a gallery under suspicion that the works were ‘child pornography’.¹⁹ Both situations have raised public concern over the scope of the definition.

URL Blacklist Filtering

URL blacklist filtering applies to the world wide web and not to the internet as a whole, meaning that the list will only block sites employing http: protocol (that is, starting with www) but will not target filesharing, chatrooms, password protected sites, encrypted images, or any other digital transmission or storage of prohibited material. The blockage of websites carries with it the very real possibility of collateral damage: an attempt to block an offensive video on YouTube could *potentially* temporarily block all content on YouTube, for example.

Similarly, in December 2008 the internet filtering system in the United Kingdom temporarily closed Wikipedia when Internet Watch Foundation (‘IWF’), a watchdog group equivalent to ACMA, found a Wikipedia-published image of a 1976 album cover²⁰ to be “a potentially illegal child sexual abuse image”.²¹ The cover features a naked prepubescent girl in a sexually provocative pose: a possible contravention of the *Protection of Children Act 1978* (United Kingdom). Nevertheless neither the British nor it seems any other courts have deemed the image illegal, and earlier in 2008 Wikipedia declined to censor the image as requested by an American complainant. The IWF did not blacklist any other sites featuring the image, such as Amazon.com. It did, however, blacklist not only the image’s URL, but also that of the accompanying Wikipedia article, which touched on the cover’s controversy but otherwise described the album’s music. The album (including said cover) is available in British stores.

Blacklisting the site accidentally blocked 95% of the United Kingdom’s residential internet users from contributing to Wikipedia.²² Publishing material that contravenes Wikipedia’s own guidelines on what is inappropriate triggers an internal anti-vandalism mechanism that prevents such participants from further contribution. The United

Kingdom's filter requires all ISPs to reroute via a small number of proxy servers – that is, when an internet user accesses a site, the request passes first through a “middleman” computer that filters blacklisted content. In these circumstances Wikipedia is unable to identify users' individual TCP/IP (the code that defines individual computers' internet access), instead attributing the IP of the remote proxy to any user trying to access Wikipedia via that proxy. By instituting a ban in the UK's major ISPs, the IWF instigated a blanket ban on all users employing those ISPs.

Responding to public outcry, the IWF, after a review process, confirmed the image to be potentially an offence against the *Child Protection Act*, but that given the “contextual issues ... and ... the length of time the image has existed and its wide availability”²³ removed the URL from its list.

Content Filtering

Content filtering (as yet not part of Australia's Clean Feed proposal) involves a number of heuristic methods including: deep packet-inspection, keyword sniffing, traffic-shaping, and algorithms developed to detect, absent human intervention to detect illegal content. Inaccuracy, over-breadth and invasion of privacy render these techniques highly controversial.

Concluding Remarks

Absent a clearly stated purpose, it is difficult to assess Australia's Clean Feed proposal, save to say that it will require a large budget required to initialize such a system,²⁴ potentially significantly reduce network speeds and interfere with people's fundamental access to information, with no definite purpose in mind. If the policy's aim is to prevent inadvertent access of prohibited material, the first question must surely be: how often do Australians stumble across such content? If we are concerned about children deliberately accessing unsavoury materials, a less expensive yet equally effective solution is to keep the household computer in the lounge-room, and install a personal filter. If we are concerned about deliberate adult access to child pornography, is a technologically-clumsy filter really up to the job? Could this instead force such users to encrypt illegal materials, making policing and prosecution increasingly difficult?

Passionate argument adorns on all sides the debate surrounding Canberra's proposed internet filtering system. Missing from all voices however is evidence-based policy; equally missing is its evidence-based refutation. Hard data and sound research about cybercrime, 'prohibited materials' and information security are in shortage. Research typically comes from partisan parties such as law enforcement agencies, government, religious groups, systems administrators and the media, and methodology is often absent. For example, the Australian Communications and Media Authority's report, 'Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety' reaches sweeping assessments of the effectiveness of types of filters and

materials, but does not provide any information about the scope, sample size, year of the study and who performed the study.²⁵ Crime statistics in the online environment are difficult due to novelty and lack of transparency. Whatever the policy, it lacks evidential support²⁶.

It is this author's hope that governments around the world will start by funding non-partisan research into the many important areas underlying cybercrime before spending money on unpredictable schemes with no specified intended outcomes.

* Alana Maurushat is Lecturer, Deputy Director of the Cyberspace Law and Policy Centre, and PhD Candidate – all within the Faculty of Law, the University of New South Wales. The author is indebted to David Vaile, Derek Bambauer, and Lillian Edwards for valuable discussion.

** Renée Watt is research intern with the Cyberspace Law and Policy Centre, Faculty of Law, the University of New South Wales.

¹ Stephen Conroy (then Shadow Minister for Communications and Information Technology), *Labor's Plan for Cyber-Safety*, Election 2007, at <http://www.alp.org.au/download/now/labors_plan_for_cyber_safety.pdf>

² Senator Stephen Conroy, *Budget provides policing for internet safety*, media release, 13 May 2008, at <http://www.minister.dbcde.gov.au/media/media_releases/2008/033>

³ The Classification Scheme of the Australian Communications and Media Authority may be found at <http://www.acma.gov.au>.

⁴ For France, see: TGI Paris, 19 octobre 2007, *SARL Zadig Production, Jean-Robert V. et Mathieu V. c/ Sté Google Inc. et AFA* and the case of *LICRA et UEJF V. Yahoo! Inc. and Yahoo France*, Tribunal de Grande Instance de Paris (Superior Court of Paris 2000). For Belgium, see: *Google Inc v Copiepresse SCRL* [2007] E.C.D.R. 5. For Germany, see case numbers: 308 O 42/06 and 308 O 248/07 (both cases heard at the Hamburg Regional Court).

⁵ With respect to Canada: Colangelo A & Maurushat A, "Exploring the limits of computer code as a protected form of expression: a suggested approach to encryption, computer viruses, and technological protection measure" *McGill Law Journal*, 22 March 2006.

⁶ *Catch the Fire Ministries Inc & Ors v Islamic Council of Victoria Inc* [2006] VSCA 284; *Lange v Australian Broadcasting Commission* (1997) 189 CLR 520; *Michael Brown & Ors v Members of the Classification Review Board of the Office of Film and Literature* [1998] FCA 319; *NSW Council for Civil Liberties Inc v Classification Review Board (No. 2)* [2007] FCA 896; *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104.

⁷ NetAlert (Australian Government), 'Internet Content Filters', at: <<http://www.netalert.gov.au/filters.html>>

⁸ Australian Communications and Media Authority, 'Closed Environment Testing of ISP-Level Internet Content Filtering' 41, 62-68, June 2008, at <http://www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf>

⁹ Australian Communications and Media Authority, 'Closed Environment Testing of ISP-Level Internet Content Filtering, available at http://www.acma.gov.au/webwr/_assets/main/lib310554/esp-level_internet_content_filtering_trial-report.pdf

¹⁰ Australian Labor Party 'Australian Labor Party National Platform and Constitution 2007' April 2007, at <<http://www.alp.org.au/platform/index.php>>

¹¹ OpenNet Initiative 'China: Country Profiles' 9 May 2007 at: <<http://opennet.net/research/profiles/china>>

¹² Bambauer D 'Filtering in Oz: Australia's Foray into Internet Censorship' *Brooklyn Law School, Legal Studies Paper No. 125* 22 December 2008 at <http://ssrn.com/abstract=1319466>; Gutmann E 'Losing The New China' 2004, 127-32; OpenNet Initiative 'Internet Filtering in China in 2004-2005: A Country Study' at <<http://opennet.net/studies/china>>

¹³ Bambauer D 'Filtering in Oz: Australia's Foray into Internet Censorship' *Brooklyn Law School, Legal Studies Paper No. 125* 22 December 2008 at <<http://ssrn.com/abstract=1319466>>

¹⁴ *Criminal Code Act 1995* (Cth) s 473.1

¹⁵ View ACMA's guidelines for prohibited content here:

<<http://www.bakercyberlawcentre.org/2008/censorship/index.htm#acma>>

¹⁶ *McEwen v Simmons* [2008] NSWSC 1292

¹⁷ *Crimes Act 1900* (NSW) s 91H(3)

¹⁸ *Criminal Code Act 1995* (Cth) s 474.19(1)(a)(i)

¹⁹ Wilson A & Wilson L 'Gallery Raid Revives Censorship Issue' *The Australian* 24 May 2008 at: <<http://www.theaustralian.news.com.au/story/0,,23749181-16947,00.html>>

²⁰ German band Scorpions' cover for the 1976 album "Virgin Killer"

²¹ Internet Watch Foundation, 'IWF Statement Regarding Wikipedia Page' December 2008 at: <<http://www.iwf.org.uk/media/news.251.htm>>

²² Doctorow C 'How to Make Child-Porn Blocks Safer for the Internet' *The Guardian* 16 December 2008 at: <<http://www.guardian.co.uk/technology/2008/dec/16/cory-doctorow-wikipedia>>

²³ Internet Watch Foundation, 'IWF Statement Regarding Wikipedia Page' December 2008 at: <<http://www.iwf.org.uk/media/news.251.htm>>

²⁴ The current government has pledged \$125.8 million to "protect children online": Senator Conroy 'Budget Provides Policing For Internet Safety' 13 May 2008 at: <http://www.minister.dbcde.gov.au/media/media_releases/2008/033>

²⁵ Australian Communication and Media Authority 'Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety' February 2008 at <http://www.acma.gov.au/webwr/_assets/main/lib310554/developments_in_internet_filters_1streport.pdf>

²⁶ The OpenNet Initiative's reports in "Access Denied" do an excellent job of canvassing filtering, including in Western democracies: <http://opennet.net/accessdenied>; both ONI's blog, at <http://opennet.net/blog>, and Nart Villeneuve's blog, at <http://www.nartv.org/>, are terrific, less formal resources; for an interesting article on the negative impacts of freely available pornography see: <<http://www.guardian.co.uk/lifeandstyle/2008/nov/23/health-wellbeing-therapy-society>>