E – BRIEF

NSW Parliamentary Library Research Service
November 2008 E-Brief 5/08

Internet Censorship and Mandatory Filtering

by Tom Edwards and Gareth Griffith

1 The Federal Government's proposal

On 20 October 2008 Senator Stephen Conroy, the federal Minister for Broadband, Communications and the Digital Economy, informed a Senate Estimates Committee that the Commonwealth Government was at 'the early stages' of developing a two-tier filtering scheme for internet content, one mandatory and directed towards Internet Service Providers (ISPs), the other optional. Senator Conroy said:

> …we are in the early stages. But we are looking at two tiers – mandatory of illegal material and an option for families to get a clean feed service if they wish.[1]

The Senator indicated that the proposal bore some resemblance to ISP filtering schemes in place in other countries, including

> …Sweden, the UK, Canada and New Zealand. This is not some one-off excursion.[2]

In February 2008, on the release of a major Australian Communications and Media Authority (ACMA) report,[3] Senator Conroy observed in a Media Release:

> The ACMA report notes that a number of overseas countries currently filter their content. ISPs in a number of countries, such as the United Kingdom, Sweden, Norway and Finland, have successfully introduced ISP level filtering.[4]

The Media Release went on to say

> The Government is undertaking a number of activities to inform the development of an implementation framework for ISP filtering, including extensive consultation with industry and examining overseas models… These filtered services will provide protection for children from internet websites containing harmful content.

2 Stakeholder responses

Responses to the Rudd Government's proposal have been predictably mixed. There are those who would like to see the mandatory tier expanded. For example, it is reported that Family First Senator Steve Fielding 'wants hardcore pornography and fetish material blocked…sparking renewed fears the censorship could be expanded beyond the category of "illegal material"'. A spokesman for Senator Nick Xenophon said 'he would look to block access to overseas online casino sites'.[5]

Others are more critical. For the Federal Opposition, Senator Nick Minchin said it would take 'a lot of convincing' for the Coalition to support the filtering plan, saying 'The argy-bargy that would result over what is in

and what is out strikes me as being almost impossible to manage and it would be a cat chasing its tail'.[6]

Greens Senator Scott Ludlam asked in Senate Estimates about the potential status of 'euthanasia material, politically related material, material about anorexia'. His concern was that a 'black list' of sites could become a 'very grey list very quickly, depending on how much the government thinks should be filtered'.

Colin Jacobs, chair of the online users lobby group Electronic Frontiers Australia said:

> I'm not exaggerating when I say that this model involves more technical interference in the internet infrastructure than what is attempted in Iran, one of the most repressive and regressive censorship regimes in the world.[7]

A more measured comment from the same lobby group reads:

> Although the proponents of the clean-feed have made claims to the contrary, there are no comparable ISP-level filtering systems operating in any democracy today. The systems typically cited as operating successfully in Europe are designed merely to prevent *accidental* access to a very small list of illegal sites containing child-abuse material.

Responding to his critics, Senator Conroy said:

> We are not trying to build the Great Wall of China. We are not trying to be Saudi Arabia, and to say that is to simply misrepresent the Government position.[8]

3 Internet regulation

At present, Australian ISPs are not required by law to install filtering/blocking software, nor block access to any sites. However, they must make available to subscribers a 'scheduled filter'[9] or optional filtered service. For their part, users are not required by law to use filtering software, nor purchase any such product that is offered or made available by an ISP.

Federally in Australia, internet content is regulated by Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth). This is a complaints based system administered by the ACMA on a co-regulatory basis with the internet industry

In summary, as amended in 2007, Schedule 5 provides for the regulation of Australian ISPs in respect to overseas-hosted content. Where the ACMA is satisfied that such content is 'prohibited content' or 'potential prohibited content', it may either refer the matter to the police (as in the case of child pornography material for example), or require the ISP to deal with the content in accordance with procedures set out in the Industry Code of Practice.[10]

Content hosts are now regulated under Schedule 7, which provides for the regulation of the new convergent technologies, such as broadband services to mobile handsets (such as a 3G handset). Specifically, Schedule 7 regulates internet content which has an 'Australian connection'. If the content is hosted in or provided from Australia and is prohibited, or is likely to be prohibited, ACMA will direct the content service provider to remove or prevent access to the content on their service.

The definition of 'prohibited content'[11] is the same for both Schedules 5 and 7 and is based on the classifications

applied by the Classification Board under the National Classification Code. The following categories of online content are prohibited:[12]

- RC classified content. That is, material which is illegal in all Australian jurisdictions and includes child pornography, depictions of bestiality, material containing excessive violence or sexual violence, detailed instruction in crime, violence or drug use, and/or material that advocates the doing of a terrorist act.
- X18+ classified content, which refers to real depictions of actual sexual activity.
- R18+ classified content which is not subject to a '*restricted access system*'[13] that prevents access by children. This includes depictions of simulated sexual activity, material containing strong, realistic violence and other material dealing with intense adult themes.
- MA15+ classified content, which is provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and that is not subject to a '*restricted access system*'. This includes material containing strong depictions of nudity, and implied sexual activity.[14]

At this stage, the Rudd Government proposal would restrict blanket mandatory ISP filtering to the illegal RC content, based on the ACMA's 'black list' of prohibited websites. The details are unclear, but it seems adults would be able to 'opt out' of the filtering of other levels of 'prohibited content', containing material that is either offensive or unsuitable for children.[15]

4 Testing ISP level filtering

In addition to censorship issues, ISP level filtering raises questions of a practical nature, concerning its reliability, scope and performance implications for the internet.

It is reported that

> Internet providers and the government's own tests have found that presently available filters are not capable of adequately distinguishing between legal and illegal content and can degrade internet speeds by up to 86 per cent.[16]

The reference is to the ACMA's June 2008 report, *Closed Environment Testing of ISP-Level Internet Content Filtering*, which found that, when filters were connected to the test network and were actively filtering, performance degradation varied 'from a very low two per cent to 87 per cent between the best and worst performing filter products'.[17]

The report went on to observe that despite the advances in ISP level technology:

> most filters are not presently able to identify illegal content and content that may be regarded as inappropriate that is carried via the majority of non-web protocols…[18]

Comment is made in this respect that neither the mandatory nor the optional filtering tier 'will be capable of censoring content obtained over peer-to-peer file sharing networks, which account for an estimated 60 per cent of internet traffic'.[19]

An earlier ACMA report found that:

> Currently available filter products can filter static web content, but have limited effect for increasingly popular communication tools such as chat and instant messaging services. Research reveals that filters are generally most effective when addressing static content of a sexual nature on commonly accessed websites expressed in English.[20]

This last finding was based on a European Commission study which also reported that 'over-or under-blocking occurred in about 25 per cent of test cases'. [21] Thus, even the most efficient filters block legal material indiscriminately.

5 Internet filtering software

As an alternative to ISP-level filtering, users can install internet filtering software on their home computers. This is supported by the Federal Government, which provides filtering software free at *NetAlert.com.au*. These filtering programs commonly operate by blocking access to websites or website pages that have been included on a 'black list' of inappropriate sites. Some programs can block access to all websites except those included on a 'white list'.[22]

While views on their effectiveness can vary, in 2007 a US District Court accepted evidence that filtering programs 'generally block about 95% of sexually explicit material'.[23]

A 2005 study on internet use in Australian homes reported on the extent to which parents use filtering software to prevent children from accessing inappropriate websites:

> Software to filter inappropriate websites was reported to be used by 35 per cent of parents: 29 per cent used filtering software on a regular basis and six per cent on an occasional basis.[24]

One question is whether an added, mandatory tier of filtering is required, at the ISP level, to achieve the Government's primary aim of providing 'protection for children from internet websites containing harmful content'?

6 UK

The Communications Act 2003 provides the overarching framework for regulating telecommunications and broadcasting, and established the Office of Communications (Ofcom) as the joint regulator of these industries. However, the Act does not deal with the regulation of internet content, and this is not a regulatory responsibility of Ofcom.

The Government's position is that the law in the UK applies on-line in the same way as it does off-line and the Government has preferred to encourage self regulation of content by the industry.

Increasing concern over internet users' access to illegal content online led British Telecom (BT) in June 2004 to be the first UK Internet Service Provider (ISP) to introduce filtering of content on its network, known as Cleanfeed. The UK Government has since encouraged all UK ISPs to adopt similar filtering systems, and in 2006 set a target that by the end of 2007, all ISPs which provided a broadband service would implement filtering at the ISP level. The existence of the target might lead the extent to which this is genuine self-regulation by the industry to be questioned. By the 16 June 2008 the Government reported that 95% of ISPs had introduced filtering.

BT Cleanfeed, and filtering systems used by other ISPs make use of a list of websites hosting illegal content outside the UK compiled by the Internet Watch Foundation (IWF).

The IWF is a self-regulatory body funded by the online industry. Within the UK it operates a "notify and take down system" where it notifies ISPs of potentially illegal content[25] hosted in the UK which it has identified, or which has been reported by internet users to its hotline. As a result of this approach less than 1% of child pornography known to the IWF has been hosted in the UK since 2003, down from 18% in 1997.

The IWF also maintains a list of child pornography websites hosted outside the UK. The list typically contains between 800 and 1200 sites, and is updated twice a day. As the list is of precise websites or web pages, the risk of over-blocking is minimised. The list only contains websites and does not extend to other internet services, such as peer-2-peer networks, instant messaging or chat room activities.

As BT itself admits, the Cleanfeed system is intended to prevent users inadvertently accessing illegal material, rather than to stop hardened paedophiles, and also will not prevent access to websites that are not on the IWF list. A number of ways in which both users and content providers could frustrate such systems have been postulated, and of most concern, is the suggestion that a user with the requisite technical knowledge could use a filtering system as an "oracle" to identify all the websites on the IWF list.

The Byron Review "Safer Children in a Digital World" reported to the Prime Minister in March 2008 and considered the need for better regulation of the internet. The Review noted that there was a strong case for network level blocking by ISPs of child pornography, material inciting racial hatred or extreme pornography that was illegal in the UK. Considering the arguments for and against the blocking of other "inappropriate content" at the network level the Review concluded that this should not be pursued. However, the Review said this should be reconsidered if the other measures it recommended failed to have an impact on the number and frequency of children coming across harmful or inappropriate content online. The UK Government accepted all the recommendations of the review, including the creation of a Council for Child Internet Safety, which was set up in September 2008.

In response to an adjournment debate in the House of Commons on internet regulation on the 16 June 2008, the UK Government said it recognised that the world had moved on since the Communications Act 2003, and explained that it had convened a "convergence" think tank which would report early in 2009, and would make recommendations for legislative change, where necessary. The Government said that in taking steps to protect the young or vulnerable online

> we need to do that in ways that do not unnecessarily impinge on freedom of speech, or try to create some kind of super-nanny internet.

The Byron Review also recommended that the Council for Child Internet Safety should examine the law on harmful and inappropriate material could be usefully clarified (including suicide websites) and explore appropriate enforcement responses. In September 2008 the Ministry of Justice

announced the findings of its review of the law on suicide websites. It found that the Suicide Act 1961 could usefully be amended to make it clear that the offence in section 2 of of "aiding, abetting, counselling or procuring a suicide or a suicide attempt" applied to the encouragement of suicide through the internet. The Ministry of Justice's announcement did not touch on the need for filtering of such sites.

7 The EU

The European Commission launched the Safer Internet Programme in 1999 as the European Union's response to the threat posed by illegal and harmful content on global networks. A revised Safer Internet Programme 2009-13 was proposed by the European Commission in February 2008, and is scheduled to be finally adopted by the end of the year. The programme will have a budget of €55 million ($105 million). Some of this funding is used to support a network of national helplines and watchdogs called INHOPE. The programme also seeks to encourage self-regulation by the EU's internet industry to tackle illegal content.

This approach has been reflected in the laws the EU has adopted on the Protection of Minors and Human Dignity in Audiovisual and Information Services, which have taken the form of recommendations, which are not binding on Member States. The most recent recommendation made in 2006 urged the online services industry to examine the possibility of creating filters 'to prevent information offending against human dignity'. [26]

8 Norway & Sweden

In September 2004, Telenor, a leading Scandinavian telecom company and KRIPOS, the Norwegian National Criminal Investigation Service, announced that they were introducing a filtering system designed to prevent access to child pornography at ISP level for all its internet customers. The system would be based on a list of child pornography websites compiled by KRIPOS.

In May 2005, Telenor and the Swedish National Criminal Investigation Department announced that a similar filtering system had been introduced for all Telenor's customers in Sweden.

9 Germany

In Germany a code of conduct was drawn up between the internet watchdog FSM and search engine providers. As of early 2005 all major search engines in Germany filter search results that are harmful to minors, based on a list provided by a government agency in charge of media classification. The move is seen as a response to pressure for voluntary self-regulation by industry at the EU level, and arguably the fear among industry that a failure to comply will result in increased legislation.

The German Federal Court of Justice ruled in December 2000 that material glorifying the Nazis and denying the Holocaust must be censored, regardless of where it is hosted. German ISPs have been ordered to block access to sites with such content. [27]

10 Italy

In January 2007 Italy passed a decree which requires ISPs to block access to child pornography websites within 6 hours of being alerted to their existence. The National Centre against Child Pornography is responsible for notifying ISPs to block sites, and creating and updating a list of sites

considered as containing child pornography.

In Italy the Autonomous Administration of State Monopolies (AAMS), a part of the Ministry of Economy and Finances, is responsible for issuing gambling licences. A law passed in 2006 required ISPs to block access to gambling websites that did not have AAMS licences. The AAMS was responsible for drawing up the list. The UK based company William Hill said it would challenge the law in the European Court of Justice on the grounds that it is incompatible with the EU's Single Market.

11 United States

The Children's Internet Protection Act (CIPA) enacted in 2000, requires schools and libraries that accept federal funds to purchase computers or internet access to block or filter obscenity, child pornography, and, with respect to minors, material that is "harmful to minors." [28]

The First Amendment right to free speech in the US Constitution has led to challenges to laws intended to regulate access to internet content. In 2003, the Supreme Court held that CIPA was constitutional.

The Child Online Protection Act of 1998 sought to restrict access by minors to commercially distributed online materials that are harmful to minors. However the Act has never been enforced following legal challenge, and in March 22, 2007, a federal district court found COPA unconstitutional and issued a permanent injunction against its enforcement, a decision which was upheld in an appellate court in July 2008. Any interference with the right to free speech must be the least restrictive alternative available. Material in the argument over the constitutionality of the Act has been the possibility of an alternative approach using blocking or filtering software. [29]

12 Canada

Based on the UK model is Project Cleanfeed Canada, a voluntary scheme designed to prevent the accidental accessing of child pornography material. According to liberatus,net:

> On 23 November 2006, eight Canadian ISPs announced that they had 'joined forces with Cybertip.ca, Canada's child sexual exploitation tipline, to launch a new voluntary initiative to help in the battle against online child sexual abuse'.

13 New Zealand

According to NetSafe, New Zealand's Internet Safety Group:

> New Zealand has no mandatory ISP level filtering. There are some ISPs who filter voluntarily, however they tend to market themselves as 'family friendly' and it is considered part of their service. [30]

This is confirmed by David Cunliffe, the relevant Minister in the outgoing Labour Government, stating:

> The New Zealand government has no current plan to follow Australia into compulsory filtering of internet connections by ISPs… [31]

The Minister referred to a trial filtering program conducted with ISPs on a voluntary basis, saying 'The trial currently blocks access to about 7,000 websites that are known to deal exclusively with child sexual abuse imagery'. He added, 'There are no plans for the programme to be

expanded to other types of illegal material'.

14 Comment

With the limited exceptions of Germany and Italy, mandatory ISP level filtering is not a feature of any of the countries reviewed. In place, rather, are voluntary ISP filtering schemes designed to prevent *accidental* access to a defined list of illegal sites containing child pornography. However, in the UK the position seems to be that the internet industry is encouraged to participate in this scheme, under threat of regulatory intervention should it fail to do so. The line between mandatory and voluntary participation is not clear-cut.

Further information on the filtering of internet content in other countries is provided by the Open Net Initiative.

In terms of the practicality of ISP-level filtering, various issues arise including the potential impact on internet speed and the indiscriminate blocking of innocuous material. There is also the point that URL based/index filtering only blocks access to pages on a pre-determined list. In other words, access would only be blocked to material that has been identified as prohibited by the ACMA.[32]

According to Senator Conroy, the Rudd Government's plans are at an early stage. The details of any mandatory filtering scheme remain to be determined.

Glossary:

Convergence – The bringing together of telecommunications, IT, the internet and television.

Filter – Software for controlling what content is accessible to a user.

Filtering – The process of actively identifying and blocking or permitting access to web content.

Host – a company or organisation that makes websites available on the internet on behalf of a third party

ISP – Internet Service Provider – a company that provides internet access.

Peer-to-peer – A system which allows individuals to share data, typically used to share multimedia files.

Protocol – A set of rules governing communication on the internet.

---

1 Commonwealth of Australia, Senate, *Standing Committee on Environment, Communications and the Arts, Estimates*, 20 October 2008.

2 Ibid.

3 ACMA, *Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety*, February 2008.

4 Hon S Conroy, 'Government welcomes ACMA report on Internet filtering', *Media Release*, 21 February 2008.

5 A Moses, 'Family First demands wider Internet filters', *SMH*, 28 October 2008.

6 Ibid.

7 A Moses, 'Critics of web filter bullied', *SMH*, 24 October 2008.

8 K Murphy and M Ricketson, 'Internet screening move hits hurdle', *SMH*, 30 October 2008.

9 The 'scheduled' filters are filters listed in the Industry Content Code of Practice developed by the Internet Industry Association and registered by ACMA.

10 The ACMA may also issue a 'standard-access prevention notice': *Broadcasting Services Act 1992* (Cth), Sch 5, cl 40(1)(c).

11 'Prohibited content' is defined by clause 20 of Schedule 7; a further category of 'potential prohibited content' is defined by clause 21.

12 Note that a separate scheme operates for 'eligible electronic publications'. As defined by clause 11 of Schedule 7 these are the online equivalent of those books and magazines available in print in Australia. In this case, the prohibited content regime mirrors that for publications under the

National Classification Scheme and refers to: RC; Category 1 Restricted; and Category 2 Restricted.

[13] 'Restricted access system' is defined by clause 14 of Schedule 7.

[14] ACMA, *Prohibited Online Content*.

[15] See generally Electronic Frontiers Australia.

[16] A Moses, 'Critics of web filter bullied', *SMH*, 24 October 2008.

[17] An earlier NetAlert report found that 'The level of performance degradation ranged from 18% through to 78%' – NetAlert, *A study on server Internet filters*, May 2006. A further finding was that 'Only one out of the six users noted any performance difference'.

[18] ACMA, *Closed Environment Testing of ISP-Level Internet Content Filtering*, June 2008, p 7. The report adds, 'This is despite developments in the use of internet technologies that have led to increased use of non-web protocols such as instant messaging and file-sharing'.

[19] A Moses, 'Critics of web filter bullied', *SMH*, 24 October 2008.

[20] ACMA, n 3, p 4.

[21] Filters may block innocuous content (over-block) or not block undesirable content (under-block).

[22] For further commentary see – G Griffith and L Roth, Protecting *Children from Online Sexual Predators*, NSW Parliamentary Library Research Briefing Paper No 10/07

[23] *ACLU v Gonzales*, 22 March 2007, District Court for the Eastern District of Pennsylvania.

[24] NetRatings Australia Pty Ltd, kidsonline@home: *Internet use in Australian homes,* Australian Broadcasting Authority and NetAlert, Sydney, April 2005, p 62.

[25] Child pornography, criminally obscene content, and content that would incite racial hatred.

[26] Recommendations 98/560/EC and 2006/952/EC

[27] Open Net Initiative, *Overview of internet filtering in Europe.* http://opennet.net/research/regions/europe

[28] "material that is harmful to minors" is defined as as any communication that —

(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

(ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value

[29] Congressional Research Service. *Protection of Children Online: Federal and State Laws Addressing Cyberstalking, Cyberharassment, and Cyberbullying*. September 2008. http://assets.opencrs.com/rpts/RL34651_20080905.pdf

[30] Personal E-mail communication, 11 November 2008.

[31] S Bell, 'No great firewall seen for New Zealand', *Computerworld*, 11 November 2008.

[32] Electronic Frontiers Australia, *Labor's Mandatory ISP Internet Blocking Plan*.