Electronic Frontiers
AUSTRALIA

PO Box 382, North Adelaide SA 5006
T +61 2 9011 1088 F +61 2 8002 4009
E email@efa.org.au W www.efa.org.au
ABN 35 050 159 188

Submission to the Department of Broadband, Communications and the Digital Economy 'Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for Refused Classification material ' consultation

February 2010

Written on behalf of the EFA by Nicolas Suzor, Kylie Pappalardo, and Irene Graham.

Introduction

Electronic Frontiers Australia Inc. (**EFA**) is a non-profit national organisation representing Internet users concerned with on-line freedoms and rights. EFA was established in January 1994 and incorporated under the *Associations Incorporation Act 1985* (SA) in May 1994. Our major objectives are to protect and promote the civil liberties of users and operators of computer based communications systems such as the Internet, to advocate the amendment of laws and regulations in Australia and elsewhere (both current and proposed) which restrict free speech and to educate the community at large about the social, political, and civil liberties issues involved in the use of computer based communications systems.

EFA does not support the introduction of mandatory ISP filtering. We believe that the proposal articulated by the Labor Government will be ineffective in achieving its goals and will severely infringe the liberties of Australians and the trust that Australians have in the National Classification Scheme (**NCS**) and the democratic process. As the effectiveness of filtering is outside of the scope of this consultation, we focus here on the second set of issues in an effort to explain how filtering could legitimately be achieved if there were sufficient justification for its introduction.

EFA makes eleven recommendations in this submission:

1. If mandatory ISP filtering is introduced, only the portion of the list of banned URLs that relate to illegal child sexual abuse material should be secretly maintained; the broader category of material that is Refused Classification but not illegal to access or possess should be treated in an identical way to offline classification of publications, films, and computer games;
2. The Classification Board is the appropriate body to oversee the classification of all material in Australia (EFA strongly supports '**Option One**' in part);
3. All decisions by the Classification Board should be reviewable by the Classification Review Board on the application of any interested person;
4. The ACMA should be obliged to notify Australian and international operators of websites when a URL they are responsible for is added to the list of banned URLs (EFA strongly supports '**Option Two**');
5. Any reviews of decisions to the Classification Board and the Classification Review Board should be taxpayer funded, but the cost structure of the Classification Board should be reviewed;
6. Any filter should display a page that informs users attempting to access blocked URLs that the page has been blocked, why the page has been blocked, links the user to an online copy of the Classification Board's decision summary, and provides means for the user to apply for review of the Classification Board's decision (EFA strongly supports '**Option Three**');
7. In the interests of legitimacy, transparency and consistency with the NCS, the filter should provide a warning page only, rather than completely block, the portion of RC URLs that are not child sexual abuse material (i.e. are not illegal to access);
8. URLs provided by highly reputable overseas agencies may be added to a mandatory filter where (a) the material is clearly child sexual abuse material; expedited review by the Classification Board is readily available;

and ongoing sampling of the integrity and quality of overseas lists with regards to the Australian classification guidelines is undertaken (EFA tentatively supports '**Option Four**');

9. Annual review of the list of blocked URLs and the processes used to generate the list should be conducted by an independent expert and tabled in Parliament (EFA strongly supports '**Option Five**');

10. Annual review should pay particular attention to and report on URLs added to the list that fall within a 'grey area' that are not clearly and incontestably illegal child sexual abuse material;

11. The Government should investigate the creation of an industry group to consider the administrative arrangements of the bodies responsible for any mandatory filtering scheme (EFA tentatively supports '**Option Six**').

Legitimacy, transparency, and the goals of ISP filtering

In addressing the legitimacy of mandatory ISP filtering, it is important to be clear about the goals that such a scheme would attempt to achieve. Clause 1 of the National Classification Code sets out the goals for classification in Australia:

> (a) adults should be able to read, hear and see what they want;
>
> (b) minors should be protected from material likely to harm or disturb them;
>
> (c) everyone should be protected from exposure to unsolicited material that they find offensive;
>
> (d) the need to take account of community concerns about:
>
> (i) depictions that condone or incite violence, particularly sexual violence; and
>
> (ii) the portrayal of persons in a demeaning manner.[1]

The classification system in Australia exists primarily to enable adults to make an informed choice about what they want to see, hear or read and what material they allow their children to have access to, through the classifications given to material and the consumer advice provided.[2] In order to achieve this policy objective, it is a legal requirement that films for cinema exhibition or on DVD, computer games and some publications be classified by Classification Board before public exhibition, sale or hire (the Board does not classify TV programs or films for TV). The current classification system commenced operation following enactment of the C'th Classification (Publications, Films and Computer Games) Act 1995, a federal act for the Australian Capital Territory under section 122 of the Constitution. The Commonwealth Act does not regulate sale, distribution, or possession of material and, as stated in second reading speech, "The extent to which classification decisions under it have effect in other jurisdictions [other than the A.C.T.] is a matter entirely for the state or territory concerned."[3] The Commonwealth Act (and related State/Territory classification enforcement legislation) was prepared following recommendations of the Australian Law Reform Commission (ALRC) which included:

---

1 *National Classification Code 2005* (Cth)

2 Second Reading Speech, Classification (Publications, Films and Computer Games) Bill 1994, Commonwealth, *Parliamentary Debates*, House of Representatives, 22 September 1994, 1381-4 <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F1994-09-22%2F0027%22>.

3 Second Reading Speech, Classification (Publications, Films and Computer Games) Bill 1994, Commonwealth, *Parliamentary Debates*, House of Representatives, 22 September 1994, 1381-4 <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F1994-09-22%2F0027%22>.

> "5.16 Recommendation. ... Classification is done for the purpose of controlling dissemination. It is not done for the purpose of controlling what a person is able to have in his or her own home. Accordingly, an RC classification does not of itself mean a person cannot possess that material. ... If the possession of material is to be banned, it should be to achieve some specific policy objective, not just because it has been declared unsuitable for commercial distribution. Banning the possession of material automatically upon it being classified RC would possibly be inconsistent with the International Covenant on Civil and Political Rights. ...
>
> Being declared unsuitable for commercial distribution does not automatically place material within any of [the ICCPR Article 19] exceptions. [...]The Commission is not convinced there is a special policy reason to ban the possession of all RC material [i.e. other than 'child pornography' material] and recommends that, in the absence of such reason, mere possession not be an offence."[4]

At the time of the above ALRC recommendation, mere possession of "RC" material (other than the sub-set that is child sexual abuse material) was an offence only in Western Australia and Queensland,[5] and Queensland subsequently de-criminalised mere possession.

Fifteen years later, during which Internet access has been widely available in Australia, it continues to be legal for the overwhelming majority of Australians to access, view and possess the bulk of content that is or would be Refused Classification in the privacy of their own homes; only the public dissemination of such content is restrained. We note that, to date, the Commonwealth Government has not advanced a special policy reason to justify prohibiting mere possession of, or preventing access to, the bulk of content that is or would be Refused Classification - a category which has been broadened significantly since 1995 to include more types of information/material on the grounds that it may be offensive to some adults.

Because of the paucity of information about the goals of mandatory ISP filtering, we assume that there are two broad options upon which the Labor Government predicates its proposed filtering scheme:

1. Introduce filtering in-line with the goals of the current National Classification Scheme in an attempt to reduce the risk of inadvertent exposure to material that some adults may find offensive,[6] and also to child sexual abuse material; or
2. Introduce filtering in a manner radically different from the goals of the National Classification Scheme in an attempt to prevent the private access to and possession of material that some adults may find offensive but which is not illegal for most Australians to access or possess.

The articulation of precise goals for mandatory filtering is extremely important not only for the justifications of introducing such a scheme, but for consideration of whether or not transparency measures can make the scheme compliant with the high standards of an open liberal democratic society. The options set out above reflect a fundamental choice that is required to be made in any implementation of a filtering policy in order to determine what level of information can be made available about filtered material to the Australian public.

---

4 Australian Law Reform Commission, *Film and Literature Censorship Procedure*, Report No. 55 (1991) Chapter 5, [5.16] <http://www.austlii.edu.au/au/other/alrc/publications/reports/55/ch5.html#Heading7>.

5 Ibid [5.15].

6 The Minister, in a recent press release, stated that "ISP filtering reduces the risk of Australians being inadvertently exposed to RC-rated material when they are online". The Minister does not articulate any additional goals for mandatory ISP filtering other than to reduce the risk of inadvertent exposure: see Senator Conroy, '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>.

The need for secrecy

Classification under the NCS in relation to publications, films, and computer games is currently conducted in an open manner. Information about the decisions of the Classification Board is publicly available in the Classification Board's online database and classification decisions are reviewable. In contrast, the Labor Government has indicated that the list of banned pages should remain secret. Generally, this appears to be based on the argument that the list poses a high risk to children if made public – a risk that outweighs any concerns about the lack of transparency in the process. The crux of this argument seems to be that material on the internet is a special category – unlike classification of books or movies where a list can be compiled that simply states the title of the object that has been refused classification, a list of internet material will necessarily include URLs or other information that would direct a reader straight to the Refused Classification material. Where the RC material is child pornography or child abuse material, this becomes a highly sensitive issue. In short, the Government cannot be seen to be compiling a list of child pornography or child abuse material that essentially tells potential offenders exactly where to find this material.[7]

On the Department of Broadband, Communications and the Digital Economy blog, in response to the question, 'Why won't the Government publish what is included in the ACMA blacklist?', Senator Conroy writes:

> These contributors are correct that the ACMA blacklist is currently protected from release under the FOI [Freedom of Information] Act. However, there is good reason for this. Distribution of child pornography is illegal under both Commonwealth and state laws. Publishing the title or internet address of child abuse material would constitute distribution of illegal material and is therefore protected from release.[8] To do otherwise would allow a person to view and download the material in jurisdictions where ISP-level filtering was not implemented. Given that most of this material relates to child sexual abuse, the publication of this information is clearly not in the public interest.[9]

While Senator Conroy is demonstrably incorrect in his statement that most of the material on the ACMA blacklist is child sexual abuse material,[10] it is nevertheless important to consider the concern of providing URLs of child sexual abuse material. There is a valid argument, at least for the third of RC material that has been identified as child sexual abuse material, that such a list should be kept secret. There is no valid argument that the other two-thirds of the list should also be kept secret. Such secrecy would be fundamentally inconsistent with the goals of the NCS as they

7 Inherent in this claim is an acknowledgement by the Government that the proposed filter would not be able to block access to this material absolutely. The filter may be circumvented by those technically savvy enough, and further, the filter will only operate in Australia. This creates risks about making the list available to an international audience, where potential offenders who are accessing the internet outside of Australia may be able to gain access to the child pornography or child abuse material at URLs appearing on the ACMA blacklist supplied by the Australian Government.

8 Senator Conroy is referring to provisions in the Commonwealth Criminal Code (contained in the *Criminal Code Act 1995* (Cth)), which sets out offences for using a carriage service for child pornography material (s 474.19) and using a carriage service for child abuse material (s 474.22). There is no authority, however, that publishing only the titles or URLs of such material would constitute criminal distribution.

9 Senator Stephen Conroy, 'Response to the question, "Why won't the Government publish what is included in the ACMA blacklist?"' *Department of Broadband, Communications and the Digital Economy blog*, <http://www.dbcde.gov.au/communications_for_business/digital_economy/digital_economy_consultation/future_directions_blog/topics/civil_and_confident_society_online/why_wont_the_government_publish_what_is_included_in_the_acma_blacklist> accessed 19 May 2009.

10 As at September 2009, it is clear that only one-third of material that is Refused Classification on the ACMA Blacklist was child sexual abuse material; two-thirds of RC material on the ACMA blacklist is legal to view and possess in Australia. RC material currently only accounts for just over half of the complete ACMA blacklist, but this submission proceeds on the understanding that the current filtering proposal will be limited to RC-only. See Environment, Communications and the Arts Legislation Committee, Commonwealth Senate, *Estimates*, 19 October 2009, 127 (Ms O'Loughlin, ACMA) <http://www.aph.gov.au/hansard/senate/commttee/S12489.pdf>.

currently stand.

The arguments against secrecy and the international experience

There are serious and valid arguments against the creation of a secret list of banned URLs. It is useful here to consider the approach of other countries to internet filtering. Senator Conroy has, a number of times, urged the Australian public to remember that 'ISPs in a number of countries, such as the United Kingdom, Sweden, Norway and Finland, have successfully introduced ISP level filtering.'[11] What the Minister has failed to point out is that these countries have introduced filtering *only* in respect to child sexual abuse material. In fact, the filtering systems in these countries are designed to prevent *accidental* access to a comparatively small list of web pages containing child pornography or child abuse material.[12] Yet while the subject-matter of these filters is significantly more narrow in scope than that of the proposed Australian filter, it is still useful to examine the approach in these countries from a transparency perspective. The United Kingdom (UK) and various countries in Europe use secret blacklists as the source of their filtering efforts.[13] The effectiveness of these secret blacklists practically and in relation to public confidence is relevant to our examination of the requirements of transparency in ensuring legitimacy of any Australian filtering regime.

In 2004, the UK's largest ISP, British Telecom, implemented filtering technology within its own network, known as the BT CleanFeed System.[14] The BT CleanFeed System blocks a list of potentially illegal URLs related to child sexual abuse content provided by the Internet Watch Foundation (IWF).[15] This list is a single undifferentiated index which typically contains 500 to 800 URLs at any one time and is updated twice a day to ensure all entries are live.[16] The UK government has subsequently encouraged all UK ISPs to implement ISP level filtering and British Telecom has offered the design of its filter to other ISPs for free so that they can tailor and deploy the systems in their own networks.[17] Notwithstanding that the IWF list is supposed to be secret, studies have shown that the BT CleanFeed System can be used to discover the contents of the secret blacklist.[18]

In Norway and Sweden, the ISP Telenor operates a filtering system using a blocking list provided by KRIPOS, the Norwegian National Criminal Investigation Service. Other countries where some ISPs voluntarily use filtering

11 Senator Conroy, 'Government welcomes ACMA report on internet filtering' (Ministerial Media Release, 21 February 2008) <http://www.minister.dbcde.gov.au/media/media_releases/2008/011> accessed 6 July 2009; ABC Radio, 'The Great Firewall of Australia', *The Media Report*, 30 October 2008 <http://www.abc.net.au/rn/mediareport/stories/2008/2405376.htm> accessed 6 July 2009.

12 See Electronic Frontiers Australia, *Labor's Mandatory ISP Internet Blocking Plan* (4 March 2008) <http://www.efa.org.au/censorship/mandatory-isp-blocking/> accessed 6 July 2009; Irene Graham, "ISP 'Voluntary' / Mandatory Filtering" (31 May 2009) *libertus.net* <http://libertus.net/censor/ispfiltering-gl.html> accessed 11 February 2010.

13 Although these lists are 'secret' only to the extent that they have not been leaked online.

14 Australian Communications and Media Authority, *Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety: First annual report to the Minister for Broadband, Communications and the Digital Economy* (February 2008) at 69 <http://www.acma.gov.au/WEB/STANDARD/pc=PC_311304> accessed 6 July 2009.

15 Internet Watch Foundation, 'Facilitation of the Blocking Initiative' (19 January 2010) <http://www.iwf.org.uk/public/page.148.htm> accessed 10 February 2010.

16 Internet Watch Foundation, 'Facilitation of the Blocking Initiative' (19 January 2010) <http://www.iwf.org.uk/public/page.148.htm> accessed 10 February 2010.

17 Australian Communications and Media Authority, *Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety: First annual report to the Minister for Broadband, Communications and the Digital Economy* (February 2008) at 69 <http://www.acma.gov.au/WEB/STANDARD/pc=PC_311304> accessed 6 July 2009.

18 S.A. Mathieson, 'Back door to the black list' *The Guardian* (26 May 2005) referencing research by Richard Clayton, doctoral student at Cambridge University's Computer Laboratory <http://www.guardian.co.uk/technology/2005/may/26/onlinesupplement> accessed 6 July 2009.

technology to block only child pornography or child abuse material include Denmark, Finland, the Netherlands and Switzerland.[19]

In the USA and Canada, some ISPs voluntarily filter lists of URLs provided by the U.S. National Center for Missing & Exploited Children (NCMEC) and Canadian Cybertip.ca respectively. In both countries, the blocking list is specifically limited to child sexual abuse material depicting pre-pubescent children, which is a narrower category of child sexual abuse material than that which is illegal under the relevant countries' criminal laws.[20]

In April 2009, Germany's cabinet announced intentions to draft a law to block access to child pornography websites.[21] The German government and the Federal Office of Crime also signed agreements with five of Germany's eight major ISPs[22] – representing 75% of the German market – to install software to block consumer access to child pornography sites.[23] It was agreed that a secret list of URLs would be created by the BKA, Germany's federal police, and any attempts by users to access addresses on the list would be blocked.[24] The purpose of the agreements was stated to be to protect children and to undermine demand and break the commercial cycle for child pornography.[25] However, critics have expressed concern about scope creep in relation to this proposal,[26] especially considering the perceived lack of transparency surrounding the secret list. Critics have stated, 'We mistrust the planned non-transparent process, we regard it as ineffective and amateurish and we believe that it is counterproductive and a possible threat to democracy.'[27] Instead of the filtering scheme, critics have questioned why the government cannot just shut down illegal sites (considering that these sites must be known before they can be included in the list) and prosecute the operators of the illegal sites.[28] In response to these concerns, in June 2009 the German government modified its plan to provide a warning upon access to blacklisted sites, rather than block access outright.[29] However, subsequently the new German coalition government (elected in September 2009) decided not to put the (former government's) law into practice and, in November 2009, the German President refused to sign the (June 2009) law. German newspapers reported that this

19 See Irene Graham, "ISP 'Voluntary' / Mandatory Filtering" (31 May 2009) *libertus.net* <http://libertus.net/censor/ispfiltering-gl.html> accessed 11 February 2010.

20 See National Center for Missing & Exploited Children, 'Statement to Correct and Respond to the Washington Internet Daily Article' (24 August 2008) <http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=3774> accessed 11 February 2010; Cybertip.ca, 'Cleanfeed Canada FAQ', Q9, <http://www.cybertip.ca/app/en/cleanfeed#anchor_menu> accessed 10 February 2010.

21 'Germany agrees law blocking child porn sites' *AFP* (22 April 2009) <http://www.google.com/hostednews/afp/article/ALeqM5gu1eHuInA96XCp4kg6PGu3-rTH-w> accessed 6 July 2009; 'Germany Institutes Censorship Infrastructure' *Slashdot* (23 April 2009) <http://yro.slashdot.org/article.pl?sid=09/04/23/0319217> accessed 6 July 2009.

22 Deutsche Telekom's T-Online, Vodafone's Arcor, Kabel Deutschland, Telefonica's O2 and Alice's Hansenet: see 'Major German online companies agree to block child porn websites' *Deutsche Welle (DW – World)* (17 April 2009) <http://www.dw-world.de/dw/article/0,,4185666,00.html> accessed 6 July 2009.

23 'Germany agrees law blocking child porn sites' *AFP* (22 April 2009) <http://www.google.com/hostednews/afp/article/ALeqM5gu1eHuInA96XCp4kg6PGu3-rTH-w> accessed 6 July 2009; 'Major German online companies agree to block child porn websites' *Deutsche Welle (DW – World)* (17 April 2009) <http://www.dw-world.de/dw/article/0,,4185666,00.html> accessed 6 July 2009.

24 'Germany Institutes Censorship Infrastructure' *Slashdot* (23 April 2009) <http://yro.slashdot.org/article.pl?sid=09/04/23/0319217> accessed 6 July 2009.

25 'Major German online companies agree to block child porn websites' *Deutsche Welle (DW – World)* (17 April 2009) <http://www.dw-world.de/dw/article/0,,4185666,00.html> accessed 6 July 2009.

26 'Germany Institutes Censorship Infrastructure' *Slashdot* (23 April 2009) <http://yro.slashdot.org/article.pl?sid=09/04/23/0319217> accessed 6 July 2009.

27 Spreeblick.com, a German weblog, on demonstrative strike (22 April 2009) <http://www.spreeblick.com/protest-gegen-internetsperren/#english> accessed 6 July 2009.

28 Ibid.

29 Rick Demarest, 'German parliament passes bill in fight against child pornography sites' *Deutsche Welle (DW – World)* (19 June 2009) <http://www.dw-world.de/dw/article/0,,4406608,00.html> accessed 10 February 2010.

means "it is now effectively stalled until the new government finds a constitutional way to kill it".[30]

An observation of the filtering systems in other European countries shows that the German critics' concerns about scope creep are most likely justified. In March 2006, the Danish filter was found to be blocking a legal Danish adult sex site, bizar.dk.[31] In July 2007, controversy erupted when the Swedish police threatened to add the world's largest BitTorrent tracker, The Pirate Bay, to the Swedish child pornography filter blacklist.[32] The police alleged that they had received complaints about child pornography being traded on The Pirate Bay site. The Pirate Bay denied these allegations and stated that if the police suspected child pornography on the site they should have issued The Pirate Bay with takedown notices first.[33] In February 2008, Electronic Frontiers Finland (Effi) demanded that the National Bureau of Investigation of Finland explain why it had blocked a site that criticised internet censorship.[34] Tero Tilus, a board member for Effi, stated, 'Some faceless official decides which sites the Finns may not see, and this decision cannot be appealed. Now he has apparently decided that net filtering may not be criticised.'[35]

A more recent example from the UK further highlights the problems associated with secret web filter systems. Between Friday 5 December 2008 and Tuesday 9 December 2008, the UK internet filter caused the online encyclopedia, Wikipedia, to be inaccessible to the British public.[36] This occurred because the IWF had added two Wikipedia URLs to their secret blacklist. The censored pages contained images of a 1976 album cover (entitled 'Virgin Killers') from the German rock band, The Scorpions.[37] The album cover showed 'a young, naked girl with her genitals obscured only by a crack in the camera lens.'[38] The cover had been controversial when first released, but was never banned in Britain or the United States.[39] The IWF concluded that the image was 'potentially illegal' and added the URLs where the image was located on Wikipedia to the blacklist.[40] The UK filter works by passing all traffic to suspect websites through a web proxy which checks the web requests and blocks only the specific URLs that are on the IWF

30 See 'Köhler refuses to sign controversial internet child porn law', *The Local (Germany's News In English)*, 28 November 2009 <http://www.thelocal.de/politics/20091128-23585.html> accessed 10 February 2010; See also 'Köhler verweigert Unterschrift fürs Filtergesetz' *Der Spiegel*, 28 Nov 2009 <http://www.spiegel.de/netzwelt/netzpolitik/0,1518,663980,00.html> accessed 10 February 2010.

31 Kristoffer S. Madsen, 'Politisk strid om politiets børneporno-filter, ComputerWorld (20 March 2006) <http://www.computerworld.dk/art/33209> accessed 10 February 2010

32 Jan Libbenga, 'Sweden may block Pirate Bay over child porn' *The Register* (9 July 2007) <http://www.theregister.co.uk/2007/07/09/pirate_bay_blocked/> accessed 6 July 2009; Eliot van Buskirk, 'Swedish Police Could Block The Pirate Bay Using Child Pornography Filter' *Wired* (9 July 2007) <http://www.wired.com/listening_post/2007/07/swedish-police/> accessed 6 July 2009.

33 It was widely speculated that this 'crackdown' on The Pirate Bay had more to do with copyright infringement concerns than pornography: see Eliot van Buskirk, 'Swedish Police Could Block The Pirate Bay Using Child Pornography Filter' *Wired* (9 July 2007) <http://www.wired.com/listening_post/2007/07/swedish-police/> accessed 6 July 2009.

34 Electronic Frontiers Finland (Effi), 'Finnish police censors a critic of censorship' (Press Release, 12 February 2008) <http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2008-02-12-en.html> accessed 6 July 2009.

35 Ibid.

36 Richard Clayton, 'Technical aspects of the censoring of Wikipedia' (11 December 2008) *Light Blue Touchpaper, Security Research, Computer Laboratory, University of Cambridge* <http://www.lightbluetouchpaper.org/2008/12/11/technical-aspects-of-the-censoring-of-wikipedia/> accessed 6 July 2009; Bobbie Johnson and Charles Arthur, 'British censor reverses Wikipedia ban' *The Guardian* (9 December 2008) <http://www.guardian.co.uk/technology/2008/dec/09/wikipedia-ban-reversed> accessed 6 July 2009; Frank Fisher, 'A nasty sting in the censors' tail' The Guardian (9 December 2008) <http://www.guardian.co.uk/commentisfree/2008/dec/09/scorpions-virgin-killer-censorship> accessed 6 July 2009.

37 Ibid.

38 See Bobbie Johnson and Charles Arthur, 'British censor reverses Wikipedia ban' *The Guardian* (9 December 2008) <http://www.guardian.co.uk/technology/2008/dec/09/wikipedia-ban-reversed> accessed 6 July 2009

39 Reportedly, the United States Federal Bureau of Investigation (FBI) had investigated the same image in May 2008. As at December 2008, no action had been taken: Bobbie Johnson and Charles Arthur, 'British censor reverses Wikipedia ban' *The Guardian* (9 December 2008) <http://www.guardian.co.uk/technology/2008/dec/09/wikipedia-ban-reversed> accessed 6 July 2009

40 This move reportedly confused many when it was discovered because the album had been on sale in British shops for over 30 years: Bobbie Johnson and Charles Arthur, 'British censor reverses Wikipedia ban' *The Guardian* (9 December 2008) <http://www.guardian.co.uk/technology/2008/dec/09/wikipedia-ban-reversed> accessed 6 July 2009

list.[41] The use of proxies meant that all traffic from the UK to Wikipedia appeared to come from the same IP address (of the proxy machine). Wikipedia uses IP addresses to 'distinguish between helpful editors who improve the content of the site and vandals who attempt to trash it.'[42] To Wikipedia, the many UK-based editors who were attempting to access Wikipedia from the same IP address appeared to be 'vandals' and Wikipedia's security system barred that IP address from the site.[43] The result was that no one using the major ISPs in the UK could access Wikipedia. If not for this unfortunate result (and the effectiveness of Wikipedia's security system) it is possible that the addition of The Scorpion's album cover image and the associated Wikipedia URLs to the IWF blacklist (even though the image is widely considered not to be child pornography) would have gone undiscovered by the public.[44]

These examples show that the concerns that opponents of mandatory ISP filtering have with the secrecy of lists of banned URLs are both legitimate and substantiated by international experience. There is a real risk that filtering could be carried out in such a way that the government could add web pages to the list of banned URLs that should not be banned. This difficulty is compounded when one considers not the core of material that can reasonably be identified as child sexual abuse material, but the penumbra of uncertainty that surrounds these definitions, where the decision to ban material is inherently contestable and politicised. Examples include literature such as Nabokov's *Lolita*, graphic novels such as *Lost Girls*,[45] and pornography involving adults who look like children.[46] In these cases, secrecy is inimical to democratic discourse and limits the confidence that the public can have in the administrative of a mandatory filtering scheme.

Resolving the tension – a split list

To the extent that the internet provides unique challenges for classification that justify secrecy in relation to the list of banned child pornography or child abuse URLs, we must weigh these arguments against the dangers of secrecy in classification. There is significant community concern about the maintenance of a secret list of banned URLs as something that is potentially incompatible with the requirements of transparency in legitimate democratic governance. In order for Australians to be confident that mandatory filtering is not being used in a way that is inimical to the interests of liberal democratic society, secrecy should be limited to the least possible amount that is required. To the greatest extent possible, any secret banned list must be independently audited, regularly internally reviewed and readily externally reviewable, and carried out by an accountable public authority that is independent from the political process.

EFA considers, therefore, that the only way in which a filtering scheme could legitimately be implemented would be to

41 Richard Clayton, 'Technical aspects of the censoring of Wikipedia' (11 December 2008) *Light Blue Touchpaper, Security Research, Computer Laboratory, University of Cambridge* <http://www.lightbluetouchpaper.org/2008/12/11/technical-aspects-of-the-censoring-of-wikipedia/> accessed 6 July 2009

42 Ibid.

43 Ibid.

44 A similar incident occurred in January 2009 in relation to the blocking of the Internet Archive's Wayback Machine: see Cade Metz, 'Demon ends porn-less Internet Archive Block' *The Register* (16 January 2009) <http://www.theregister.co.uk/2009/01/16/demon_resolves_wayback_issue/> accessed 6 July 2009; Nate Anderson, 'The accidental censor: UK ISP blocks Wayback Machine' *ars technica* (14 January 2009) <http://arstechnica.com/web/news/2009/01/the-accidental-censor-uk-isp-restricts-wayback-machine.ars> accessed 6 July 2009.

45 <http://en.wikipedia.org/wiki/Lost_Girls>.

46 See, for example, Michael Meloni, 'Classifiers refuse to common breast size specifics: Look young and you're banned', *Somebody Think of the Children*, 01 February 2010 <http://www.somebodythinkofthechildren.com/appearance-persons-age-no-comment-on-breast-size/>.

create two lists: one, which is limited to child sexual abuse material, to be kept secret; and another, which will block the broader category of RC material that is legal to access and possess in Australia, which cannot be kept secret under any sensible interpretation of the goals of the NCS. The open list would necessarily be maintained in a manner substantially identical to the way in which the Classification Board currently classifies publications, films, and computer games. All classification should be carried out by the Classification Board and classification decisions should be made publicly available. There is no suitable argument to treat online material different to offline material in this sense. Achieving such parity between online and offline classification would aide in restoring public confidence in the Government's proposed mandatory filtering system and provide some assurance that filtering is carried out in a way that is legitimate and consistent with democratic society.

EFA recommends that the definitions in the Commonwealth Criminal Code should determine whether RC content should be placed on a secret list for child pornography and child abuse material or on a broader, open list. The National Classification Code classifies as RC publications and films that

> describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not)[.][47]

This definition in the NCS is too broad to be effective. It may be suitable for a definition of 'RC', but is not suitable for a secret list. EFA believes that in order to justify imposing a secret list, the definition should be limited to that of material that is illegal to access, as defined by the Commonwealth Criminal Code, which proscribes 'child abuse material', and 'child pornography material'. 'Child abuse material' is defined as material that describes or depicts a person who

> (i) is, or is implied to be, under 18 years of age; and
> (ii) is, or is implied to be, a victim of torture, cruelty or physical abuse;
> and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive.[48]

The Commonwealth Criminal Code defines 'child pornography' as:

> (a) material that depicts a person, or a representation of a person, who is, or appears to be, under 18 years of age and who:
> (i) 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
> (ii) 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; or
> (b) material the dominant characteristic of which is the depiction, for a sexual purpose, of:
> (i) a sexual organ or the anal region of a person who is, or appears to be, under 18 years of age; or
> (ii) a representation of such a sexual organ or anal region; or
> (iii) the breasts, or a representation of the breasts, of a female person who is, or appears to be, under 18 years of age;
> in a way that reasonable persons would regard as being, in all the circumstances, offensive; or
> (c) material that describes a person who is, or is implied to be, under 18 years of age and who:
> (i) is engaged in, or is implied to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or
> (ii) is in the presence of a person who is engaged in, or is implied to be engaged in, a sexual pose or sexual activity;

47 *National Classification Code 2005* (Cth) cl 2(1)(b) (publications); cl 3(1)(b) (films); cl 4(1)(b) (computer games).
48 Criminal Code Act 1995 (Cth) s 473.1.

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive; or

(d) material that describes:

(i) a sexual organ or the anal region of a person who is, or is implied to be, under 18 years of age; or

(ii) the breasts of a female person who is, or is implied to be, under 18 years of age;

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive.

These definitions are much more appropriately tailored than the relevant section of the NCS. They provide detailed guidance as to when material will be illegal to access that does not rely solely on a subjective assessment of whether the material would be "likely to cause offence to a reasonable adult".[49] EFA strongly believes that if a secret list is to be maintained, the material on that list must only fall within the definition of material that is illegal to access and possess in Australia. For a classification and censorship scheme to be legitimate, it must be transparent to the greatest extent possible. Australians have a fundamental interest in knowing what material is being withheld from them and how it has been classified. Only where the material is illegal to access and disclosing identifying information would substantially increase the availability and dissemination of that material can a secret list be justified, and only then with sufficient transparency and review procedures in place to guarantee the integrity of the secret list.

EFA strongly recommends that if any mandatory ISP filtering scheme is implemented, only the subset of any list of RC material that is illegal to access (child pornography or child abuse material) should be kept secret.

EFA finds no possible justification for maintaining a secret list of the broader category of RC material that is consistent either with the goals of the NCS or the requirements of legitimacy and transparency in classification in a liberal democracy.

EFA strongly recommends that the definition used to determine whether material should be on a secret list should be the definitions of material that is illegal to access used in *Commonwealth Criminal Code Act 1995* (Cth).

If this option is pursued, there remains a significant question as to the maintenance of the secret component of a list of banned URLs. The Australian Government should seek to achieve a pragmatic outcome that effectively addresses the concerns raised by the availability of child sexual abuse material online but which interferes to the minimum extent possible with the democratic freedom of Australian individuals. The remainder of this submission addresses the measures proposed by DBCDE to increase transparency in the maintenance of a secret list.

Refer all material to the Classification Board

The Classification Board is the only body currently established in Australia that has the required legitimacy to determine whether online material should be banned. While EFA appreciates that the ACMA acts in good faith to oversee the current blacklist, it does not have the structural integrity or accountability that is required to guarantee legitimacy if internet access is to be subject to censorship by means of a compulsory filter.

49 *National Classification Code 2005* (Cth) cl 2(1)(b) (publications); cl 3(1)(b) (films); cl 4(1)(b) (computer games).

The Classification Board is a statutory body comprising publicly named members. In the case of offline material, titles of all banned and classified material are publicly available on the Classification Board's website, and decisions of the Classification Board can be appealed to the Classification Review Board. In contrast, decisions to add online material to the ACMA blacklist are currently made by unnamed ACMA staff and cannot easily be appealed or otherwise reviewed. If the identity, background and experience of the people within government who are making these decisions are kept secret, any potential biases or political agendas go unchallenged, and Australians will not have the ability to have faith in the classification process.

We note the concerns expressed by the (then) ALP Shadow Minister for Homeland Security (Censorship Minister), Arch Bevis, in the House of Representatives on 15 August 2007, in stating that "[t]he government...has transformed the Classification Review Board into a source of jobs for Liberal Party mates..." and "[h]ow can the Australian community have confidence in the classification watchdog when more than half of its members are representative of such a narrow constituency?"[50] Similar remarks were made concerning Board membership by the then (ALP) Manager of Opposition Business in the Senate/Shadow Attorney-General, Senator Joe Ludwig, on 20 September 2007.[51]

Given the above remarks by Labor Party politicians would serve to undermine the Australian public's faith and confidence in classification processes, and relevant legislation has not been changed in an effort to prevent 'stacking' of Boards by a current or future government, it would be ironic if the Labor Government now contends there should not be public concern about secret blacklisting and blocking of online material, irrespective of whether ACMA staff or members of Classification Board/s make decisions.

Senator Conroy has previously attempted to reassure the Australian public that the persons in charge of the ACMA blacklist are responsible and possess the requisite expertise by stating that:

> ACMA content assessors have been members of the Classification Board and/or undergo formal training provided by the Classification Board. ACMA employs a number of former National Classification Board members within the Codes, Content and Education Branch who have a combined experience of close to 20 years at the Classification Board. This experience in conjunction with the formal training and regular referrals of content to the Classification Board help to ensure consistency of classification decisions.[52]

Despite the training of ACMA officials, the ACMA does not have the expertise, accountability, and higher level of independence (in theory at least) that make the Classification Board's decisions more legitimate.

Even if it is accepted that ACMA or the Government will not purposely include web pages that fall outside the parameters of 'Refused Classification', there are currently no apparent checks and balances to guard against mistakes. For example, when the ACMA blacklist was leaked in March 2009, it was found to contain a PG-rated page of Bill Henson photographs. When questioned about this inclusion on ABC's Q&A programme, Senator Conroy claimed that it was the result of a 'technical error' within the system.[53] It is questionable whether this 'technical error' would have

50 Commonwealth, *Parliamentary Debates*, House of Representatives, 15 August 2007, 12-14 (Arch Bevis) <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F2007-08-15%2F0020%22>.

51 Commonwealth, *Parliamentary Debates*, Senate, 20 September 2007, 51-2 (Joe Ludwig) <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansards%2F2007-09-20%2F0126%22>.

52 Commonwealth, *Parliamentary Debates*, Senate, 03 February 2009, 194 (Stephen Conroy, Minister for Communications, Broadband, and the Digital Economy) <http://www.aph.gov.au/hansard/senate/dailys/ds030209.pdf>.

53 Colin Jacobs, *Conroy faces the filtering music on Q&A* (27 March 2009) Electronic Frontiers Australia

been discovered if the list had not leaked to the public. The mistaken inclusion on the RC content blacklist of web pages which do not contain Refused Classification content could have profound practical effects on the businesses and livelihoods of ordinary Australians; the leaked blacklist also contained the legitimate web pages of a tuck shop supply company and a dental practice.[54]

Another example comes as a result of questioning during a Senate ECA Committee Estimates hearing on 23 February 2009, when it became publicly known that the ACMA had wrongly assumed that a Web page on an anti-abortion web site would, if classified, be "RC". An ACMA representative stated that:

> We have kept a careful watching brief on the way the Classification Board has handled those types of images. On a previous occasion, we made a referral to the Classification Board on very similar material and it came back as 'refused classification'. So we juxtaposed the two decisions and judged it on the images. ... If we were in any doubt, we would have referred it to the National Classification Board.[55]

However, on 20 March 2009, the Classification Board classified the same page R18+, showing that the ACMA's guess was wrong. This mistake came to public light only because a link to the subject web page (hosted overseas) was placed on Australian hosted web site and the ACMA issued an 'interim' link deletion notice to the relevant Australian hosting service provider, which triggered a legislated requirement that the ACMA have the overseas hosted content classified before issuing a 'final' link deletion notice.

These examples highlight a critical concern: due to the secrecy surrounding assessment of online content, it cannot be known how many other URLs may be on ACMA's existing blacklist on the grounds of being "RC", but which would not be "RC" if classified by the Classification Board.

In order to ensure the legitimacy of any mandatory filtering policy, EFA strongly believes that only the Classification Board has the capacity to determine whether a given URL contains RC content.

EFA does not support the proposal in Option One that all material initially assessed as RC by the ACMA be placed on the RC content blacklist whilst the Classification Board undertakes its classification decision making process. This could result in material being wrongly blocked for 20 days or longer.[56] At most, only content initially assessed by ACMA as unquestionably child sexual abuse material could be added prior to a Classification Board decision, if the Classification Board becomes required to provide a decision to ACMA within 5 days (which would require legislative amendments). The ACMA should be required to have all other suspected RC material classified prior to adding same to the RC content blacklist.

In order to satisfy requirements of due process, there should also be a system established whereby a person whose web page has been blocked, or a person whose access to a web page has been blocked, can have a proper avenue of review.[57]

<http://www.efa.org.au/2009/03/27/conroy-faces-the-filtering-music-on-qa/> accessed 6 July 2009.

54 Ibid.

55 See Environment, Communications and the Arts Legislation Committee, Commonwealth Senate, *Estimates*, 23 Feburary 2009, 72, (Andree Wright) <http://www.aph.gov.au/hansard/senate/commttee/S11635.pdf>

56 Australian Government, 'Statutory Timeframes for the Classification Board and Review Board', *Classification Website* <http://www.classification.gov.au/www/cob/classification.nsf/Page/Industry_WhathastobeClassified_StatutoryTimeframes_StatutoryTimeframes> accessed 10 February 2010.

57 For example, under Part 5 of the *Classification (Publications, Films and Computer Games) Act 1995* (Cth), where a publication, film or computer game has been classified, the publisher of the film, publication or computer game or an aggrieved person may apply for review of the classification decision. The Act establishes a Classification Review Board under s 72. In accordance with s 44,

EFA strongly supports the 'Option One' proposal that all material initially assessed by ACMA as potentially RC be required to be classified by the Classification Board.

EFA does not support the 'Option One' proposal that potential RC material be added to the RC blacklist prior to classification. If any material is to be added prior to classification, EFA recommends it be limited to material that ACMA considers is child sexual abuse material and subject to a legislated requirement that the Classification Board provide a classification decision to ACMA within 5 days.

EFA strongly recommends that all decisions by the Classification Board should be reviewable by the Classification Review Board on the application of any interested person.

EFA notes, however, that the legitimacy of the Classification Board is in part predicated on its transparency. Under current practice, when the Classification Board classifies online content for the ACMA, no identifiable information associated with the classification decision is made publicly available. EFA does not consider that it is legitimate for the Classification Board to classify internet materials without providing the same title information (at a minimum, title, author and publisher) that is available for off-line publications, films, and computer games. Providing title information is not likely to increase access to RC material; there is no evidence that Australians are likely to trawl through the Classification Board decisions in order to identify objectionable material that they will then seek out. Conversely, the reverse link is important – if a particular URL has been blocked by the Australian Government, Australians must be able to seek out the decision of the Classification Board in order to determine on what grounds it was blocked, and potentially initiate a review of the decision. This is currently impossible without providing title information in the Classification Board database.

ACMA notification procedure

It is important that if any URL is banned, the operator of the relevant website should be immediately informed. Child sexual abuse material is only extremely rarely made brazenly available on public websites; in the greatest majority of cases where this sort of material can be found, it has likely been placed there by malicious attackers exploiting vulnerabilities on legitimate systems. In these cases, notification to the operator of the website is likely to result in immediate removal of the content and tightening of website security – particularly as actual knowledge of the material means that continued publication would likely constitute an offence in many countries.

Notification is also important to enable website owners to challenge a finding that material on their website has been refused classification. The ability to appeal such findings is an absolute minimum requirement for legitimacy in any mandatory filtering scheme. Both Australian website owners and international operators are entitled to this notification when their substantive rights to publish in Australia are curtailed.

A recent example from Germany shows that notifying the owners of websites is a useful step in addressing the availability of child sexual abuse material online. In an experiment conducted in May 2009, Alvar Freude of AK Zensur,

the Review Board must deal with applications for review.

the German Working Group against Internet Blocking and Censorship, sought the removal of child pornography sites listed on the various European blocking lists from the internet.[58] Fed up with arguments justifying filters on the grounds that it is often impossible or extremely difficult to have illegal content removed from the web, Freude analysed the European blocking lists via automatic procedures and wrote to each provider on whose servers the child pornography was allegedly located. A total of 348 providers in 46 countries were contacted and informed of 1943 allegedly illegal websites. 250 providers responded saying that they had investigated the claim and had found only legal content.[59] Within 12 hours, ten providers indicated that 61 child pornography sites had been removed from the internet. Among the providers that responded were providers in the United States, Holland, Denmark, Russia and Germany. Many of these providers were not aware that some of their hosted content had been included in blocking lists, but when informed were more than willing to remove the offending content as soon as possible.[60] Freude argues that his experiment demonstrates that '[t]he process to shut down websites with child pornographic content does not take longer than the transmission of a blocking list.'[61] He also argues that 'What was possible for a citizen's initiative...should be even easier for the German government and law enforcement agencies and their results should by far exceed the results of AK Zensur.'[62]

This example shows that proper notification procedures are not only important for legitimacy of a filtering scheme, but are useful in combating the availability of child sexual abuse material online.

EFA strongly supports 'Option two', where the ACMA would be obliged to notify Australian and international operators of websites when a URL they are responsible for is added to the list of banned sites.

In making this recommendation, EFA notes two caveats. The first is that under the current scheme, it is unclear whether the notification should be sent to the ISP hosting the website, or the ISPs customer, the actual operator of the website. EFA strongly believes that the operator of the website must be notified, in place of or in addition to the

58 Alvar Freude, 'Delete, don't block: It works!' (Working Group against Internet blocking and censorship (AK Zensur) Press Release, 28 May 2009) <http://www.unpolitik.de/2009/05/28/delete-dont-block-it-works/> accessed 6 July 2009.

59 This was reportedly later confirmed by samples taken of the content. This is a further example of legal content being added to lists that are supposed to only content clear instances of illegal (child pornography) content.

60 Freude notes that some of the illegal material was located on 'hacked' sites (sites that were exploited through security holes to spread external material). He states that even in these cases, the providers were grateful for the supplied information. It is important to note here that we also have a responsibility to increase computer security measures and education about these measures. It is possible that ordinary people may be hosting illegal material from their sites or servers without being aware of it, due to the presence of 'trojans' on their computer. (For a definition of 'trojan', see Wikipedia Contributors, 'Trojan' *Wikipedia*, <http://en.wikipedia.org/wiki/Trojan_horse_(computing)> accessed 6 July 2009).

Improved computer security across the board can help us to protect ourselves collectively from malicious computer attacks. For example, Lilian Edwards argues that we should conceive of network security as a security commons - that '[t]he answer must lie in the taking of collective responsibility for security on the Internet by all parties concerned.' She argues that zombie networks are like the multi-headed hydra - as we cut off one head (i.e., complain to law enforcement and have them shut down one computer), the content may just pop up somewhere else. The only long-term solution is to treat security as a broad social problem, not as an individual issue, and have everyone take responsibility to create more secure networks - ISPs, police, end users, governments all working together to ensure that, for example, anti-virus and malware protection is on all computers: Lilian Edwards, 'Dawn of the Death of Distributed Denial of Service: How to Kill Zombies' (2006) 24 *Cardozo Arts & Entertainment* 23, 57.

61 Alvar Freude, 'Delete, don't block: It works!' (Working Group against Internet blocking and censorship (AK Zensur) Press Release, 28 May 2009) <http://www.unpolitik.de/2009/05/28/delete-dont-block-it-works/> accessed 6 July 2009.

62 Ibid. Presumably, Freude is alluding here to the 88 providers who were not reported to have responded to his correspondence but who may reply to official correspondence received from the German government or the German police.

hosting provider. EFA also strongly believes that the operator should have a primary right of appeal or review against the decision to add the URL to the list, which is not the case under the current ACMA blacklist scheme.

In addition, we argue that unless there are clear and valid reasons not to do so, websites that host child sexual abuse material should be immediately informed in order that they can take immediate steps to remove it. EFA notes that it is not clear in what circumstances and why the Australian Federal Police would request that such material should remain publicly available pending investigation.

Review and Appeal Mechanisms

Option Two (and similarly Option Three) suggests that 'content owners' could be given an opportunity:

> "to seek a classification from the Classification Board if the owner believes the ACMA decision is not correct. In this case, the ACMA would ask the Classification Board to give priority to its classification of that content. Where the Classification Board has already made its classification decision, the content owner could seek a review by the Classification Review Board and provide arguments or evidence to support the review."

However, the consultation paper provides insufficient information about the above proposal to determine the merits, practicality, or usefulness of such opportunities.

The primary concern that EFA has with a right of appeal to the Classification Board lies in the cost either to content owners (especially non-commercial content providers) or to taxpayers. The consultation paper makes no mention of classification fees, let alone who would be required to pay those fees. EFA understands that the current fee structure includes the following:

- $510 – Classification Board's fee for classification of a Web page. (This fee is currently paid by ACMA to the Classification Board on occasions when ACMA applies for classification, because all Web pages, including those consisting of only text and/or non-moving images are required to be classified as if a film. Hence, the fee charged is the same as for classification of a film on DVD for sale/hire of up to 60 minutes running time, and is only $10 less than the fee for classification of an offline printed publication of up to 76 pages);
- $400 – Classification Board's Priority Processing Fee for a fast turnaround of an application for classification, i.e. a classification decision within a 5 day period, as suggested in the consultation paper;
- $8,000 – Classification Review Board's fee for review of a Classification Board classification of a Web page.

These fees, established for the principal purpose of regulating commercial sale and distribution of offline material in Australia, are demonstrative of the unsuitability of the existing classification system to the world-wide Web, where many content owners/providers are individuals and non-profit organisations, etc, not businesses, who make content available on a non-commercial basis, free of charge. If these fees are payable by the person seeking the review, it is likely that the existing fee structure would be prohibitively expensive for many non-commercial content providers to exercise a due process right of appeal.

If the government intends that ACMA (i.e. taxpayers) would pay the relevant classification fees, then significant issues arise concerning the high cost to taxpayers. Apparently each disputed ACMA assessment would cost taxpayers minimum classification fees of $910 plus the cost of ACMA staff time etc, and $8,000 in the case of review of a

classification decision. Moreover, the base $510 classification fee for any type of Web page (including short pages with only a small number of static images) seems excessive and indicates either that the Classification Board is unacceptably inefficient in its classification of online material, or that taxpayers are currently subsidising the cost to commercial businesses who seek classification of offline material for profit-making purposes

These cost concerns are compounded by the issue of priority assessment. In relation to Option Three, the discussion paper states that where an ACMA assessment is disputed, ACMA "would request that the Classification Board undertake its assessment with priority". As noted above, the Board's Priority Processing Fee is $400; unless the classification process can be made more efficient without sacrificing legitimacy, EFA notes that the cost to taxpayers or private parties may greatly exceed any perceived benefits of mandatory filtering.

EFA considers that before any mandatory ISP filtering legislation is introduced into Parliament, the issue of classification fees and who pays must be addressed and resolved (and publicly announced) in a manner that ensures either: (a) Internet content owners can obtain classification and/or review either free of charge or at a vastly reduced cost than currently; and (b) if the fees would paid by ACMA, that fees charged to ACMA are reduced significantly so that taxpayers are not subsidising, through ACMA's activities, the classification cost to commercial distributors/publishers of offline material.

In regards to ACMA's fee structure, we note that the "Fees for Classification" page of the classification.gov.au web site states that: "The Attorney-General's Department is currently reviewing the fees charged for the Classification services. Indicative fees are expected in early 2009".[63] It is unknown whether this review has been abandoned; if not, there is no indication of whether any fees may be reduced rather than increased, nor whether different or new fees applicable to ACMA for classification of Web pages were or are being considered.

EFA considers that it would be essential that content owners have the opportunity to seek classification and/or review (and whether or not the ACMA considers that a request for classification of content assessed as RC by ACMA is a "reasonable request" as proposed in Option three). However, EFA strongly doubts such opportunities would be effective or useful in terms of improving accountability or transparency of blacklisting decisions, unless available free of charge or at a vastly reduced cost. Otherwise costs would be likely to continue to be beyond the economic means of many non-commercial online content providers and also many Australians who may find they are presented with a block notice when attempting to access a Web page and wish to seek review of the decision to block the material.

EFA Strongly supports the implementation of reviews to the Classification Board and the Classification Review Board as of right to the operator of blocked web pages and to the public at large. However, EFA is extremely concerned about the high costs of such review and the uncertainty as to who will be responsible for these costs.

EFA believes that the current Classification Board fee structure is excessive to give rise to a real right of due process to non-commercial internet publishers and users.

63 Australian Government, 'Fees for Classification' *Classification Website* <http://www.classification.gov.au/www/cob/classification.nsf/Page/IndustryFees_for_Classification> as at 09 February 2010.

While EFA supports taxpayer funded reviews in order to provide necessary legitimacy to any mandatory ISP filtering scheme, we are also concerned that the aggregate costs of legitimate review will outweigh any possible benefit of the scheme.

Blocking notification page

In addition to notifying the operators of websites whose URLs are blocked, any legitimate filtering scheme must operate sufficiently transparently to enable individuals to identify when a URL has been blocked, for what reason, and how they can seek to review the decision. This ensures that (a) there is no uncertainty when pages are unavailable for other (technical) reasons; (b) the purpose and scope of filtering is clearly understood; and (c) an open political discourse can be maintained as to the role and ongoing justifications and effectiveness of the censorship regime.

If it is deemed absolutely necessary not to provide a searchable database of the Classification Board's decisions (limited, at a minimum, to child sexual abuse material, if there is sufficient justification to warrant omitting the information when similar information is available for offline material), the anonymised identifier used by the Classification Board should be made available on the blocking notification page. This would have the effect of preventing anyone from attempting to determine the content of the list from searching the Classification Board database while still allowing individuals who come across blocked material to identify why the material was blocked and how the decision can be reviewed.

Cory Doctorow has suggested an improvement to the UK filter system which he argues would promote accountability and due process in relation to the secrecy of the blacklist, and as result, reduce mistaken or erroneous inclusions.[64] Doctorow suggests that instead of the '404: Not found' message that currently appears when a user attempts to access a blocked site,[65] the following message should be displayed:

> Material blocked: this page ("TITLE") appears on the Internet Watch Foundation's blacklist of obscene material. IWF officer NAME made this notation, "REASON_FOR_BLOCKING." If you believe that this is an incorrect classification, you can appeal the decision by visiting the IWF's appeals page (link). There is no penalty for appealing this decision, and your name and other details will be kept confidential.[66]

EFA endorses Doctorow's proposal and believes it would go a long way towards fostering transparency and accountability within an otherwise closed system.

EFA strongly supports 'Option three', where the filter would display a page that informs users attempting to access blocked URLs that the page has been blocked, why the page has been blocked, links the user to an online copy of the Classification Board's decision summary, and provides means for the user to apply for review of

64 Cory Doctorow, 'How to make child-porn blocks safe for the internet' *The Guardian* (16 December 2008) <http://www.guardian.co.uk/technology/2008/dec/16/cory-doctorow-wikipedia> accessed 6 July 2009.

65 Which does not distinguish a site that is inaccessible because it has been blocked from a site that is inaccessible due to the usual technical errors that sometimes occur on the internet.

66 Cory Doctorow, 'How to make child-porn blocks safe for the internet' *The Guardian* (16 December 2008) <http://www.guardian.co.uk/technology/2008/dec/16/cory-doctorow-wikipedia> accessed 6 July 2009.

the Classification Board's decision.

Warning vs blocking

If the goals of mandatory filtering are truly to apply the classification system to online content for a purpose consistent with its use in relation to offline content, then requirements of legitimacy suggest that the filter should only warn users, not block RC material that is not child sexual abuse material (i.e. not block material that is legal to access and possess). The goals of the NCS are, generally speaking, to enable adults to make an informed choice about what they want to see, hear or read and what material they choose to allow their children to have access to. The proposed 'RC Content List' may be of some use, albeit to a very limited extent, in terms of assisting adults to avoid inadvertently accessing, in the privacy of their home, some types of content that they might find offensive, but does not even attempt to enable adults to make informed choices about whether or not to allow their children to access content that is unsuitable for children of varying ages, e.g. PG, M15, MA15+, R18+ and X18+ (hence adults who wish to use filtering for the latter purpose will continue to need to implement additional filtering covering more types of material than the proposed mandatory "RC Content list").

For the approximately two-thirds of the RC portion of the existing ACMA blacklist that is not child pornography or child abuse material material, the relevant goal of the NCS would be satisfied by a clear warning that the viewer may find the content to be offensive, and such an approach could be implemented with only minor negative impact on the the liberties of individuals and the requirements of openness in a liberal democracy. By contrast, the blocking outright of all RC material is a radical change from the purpose for which offline material is classified – primarily to regulate sale and public exhibition.

The government has not advanced a justification for why online material should be treated so differently to offline material, and the interests of individuals to be able to choose to access content that others may find offensive but that is not illegal to access is a fundamental component of liberal democracy.[67]

EFA believes that adopting a warning approach with regards to RC material would largely prevent any inadvertent access without posing a significant risk to the freedom of adults to choose what material they wish to view and particularly without blocking access to legitimate material that exists in the fringe or grey areas – material that is not clearly RC or is not clearly child pornography or child abuse material.

EFA strongly argues that in the interests of legitimacy, transparency and consistency with the NCS, the filter should provide a warning page only, rather than completely block, the portion of RC URLs that are not child sexual abuse material (i.e. are not illegal to access).

67 Charles de Secondat Montesquieu, The Spirit of the Laws (Anne M Cohler, Basia Carolyn Miller, & Harold Samuel Stone trans., 1989) 155 (Book 11, ch 3) ("Liberty is the right to do everything the law permits"); see further Brian Z Tamanaha, *On the Rule of Law: History, Politics, Theory* (2004) 52.

Incorporation of content from international lists

EFA is tentatively supportive of incorporating lists of child sexual abuse material produced by highly reputable overseas agencies in any potential filter. Before such lists can be incorporated, detailed analysis of the methods used to generate the lists and the integrity of the lists should be undertaken. The administrating body should issue a public report detailing its findings for any list it determines to be suitable for Australian use. Review must be readily available for all URLs incorporated from international lists, and ongoing measures to ensure the integrity of these lists must be put in place. Material that may be Refused Classification but is not child sexual abuse material should only be added if it is determined to be refused classification by the Classification Board.

EFA tentatively supports 'Option four', where URLs provided by highly reputable overseas agencies can be added to the mandatory filter provided that:

- **only material that is clearly child sexual abuse material should be added in this manner;**
- **expedited review of blocked URLs by the Classification Board is readily available; and**
- **ongoing comprehensive and statistically valid representative sampling of the integrity and quality of overseas lists with the Australian classification guidelines is undertaken by the Classification Board.**

Review and report

Any list that is developed should be subject to review, on a regular basis, by independent auditors who can verify the suitability of all URLs on the ACMA blacklist and order or recommend the removal of any that are clearly not RC material.[68] The auditors would need to be sufficiently independent of ACMA and the Government to ensure proper accountability. Further, ACMA and the Government must be seen to respond to the auditor's recommendations in a reasonable manner. The identities of the auditors (if not the individual auditors, then at least the auditing organisation) should be made publicly available in order to promote transparency and accountability and inspire community trust.

The independent auditors will be able to discover and correct obvious mistakes in the blacklist and can do their best to prevent scope creep of political material or material that clearly falls outside the RC classification. However, it will be more difficult for them to make determinations about material that is more nuanced, more prone to subjective

68 The auditors would need to seek exemption from criminal prosecution for accessing or possessing child pornography and child abuse material in the course of checking the URLs on the blacklist (but only for this purpose and in this capacity). They would therefore need exemption from sections 474.19 and 474.22 of the Commonwealth Criminal Code in the *Criminal Code Act 1995* (Cth) and they would need to seek exemptions or secure defences under the equivalent State laws - see, for example, *Crimes Act 1900* (ACT) s 65; *Crimes Act* 1900 (NSW) s 91H; *Criminal Code* (NT) s 125B; *Criminal Code* 1899 (Qld) s 228D; *Criminal Law Consolidation Act 1935* (SA) s 63A; *Criminal Code Act 1924* (Tas) s 130C; *Crimes Act 1958* (Vic) s70; *Classification (Publications, Films and Computer Games) Enforcement Act 1996* (WA) s 60(4).

analysis, and not clearly inside or outside the scope of material that the Government and the public would expect to see filtered. Auditors should be required to provide some sort of annual report on the amount of URLs and type of content that exists in these contestable grey-areas to ensure that the scheme is operating in an acceptable manner. Particularly, auditors should provide a statistical analysis of the proportion of blocked content that is clearly child sexual abuse material compared to the proportion of content that is not so clearly identifiable, with particular regard to categories of (a) artistic expression (as highlighted in the public debate about Bill Henson's photographs in 2008,[69] or the IWF's blocking of images of the Scorpion's CD cover[70]); (b) pornography containing consenting adults who are deemed to appear under the age of consent;[71] (c) material that involves the representation of child pornography or child abuse material (two recent examples include a video of a circus performer swinging a baby, eventually rated MA;[72] and the conviction of an Australian man for possession of cartoon representations of the Simpsons children engaged in sexual acts[73]);

This list highlights the main difficulty with classification and censorship is not in the core of most obviously repugnant material, but in the penumbra of material which necessitates a subjective analysis of community values and an inherently contestable political choice. It is this area of uncertainty that renders classification and censorship potentially illegitimate, and it is this area of uncertainty that must be given the greatest attention in any ongoing independent review of a legitimate censorship scheme.

EFA strongly supports 'Option five', where annual review of the list of blocked URLs and of the processes used to generate the list will be conducted by an independent expert and tabled in Parliament.

EFA strongly argues that the report should pay particular attention to URLs added to the list that fall within a 'grey area' that are not clearly and incontestably illegal child sexual abuse material.

69 See David Marr, 'Henson images cleared for general release', *Sydney Morning Herald*, 02 June 2008 <http://www.smh.com.au/news/arts/board-clears-henson-images/2008/06/01/1212258645397.html>.

70 Frank Fisher,'A nasty sting in the censors' tail' *The Guardian* (9 December 2008) <http://www.guardian.co.uk/commentisfree/2008/dec/09/scorpions-virgin-killer-censorship> accessed 6 July 2009.

71 See, for example, Michael Meloni, 'Classifiers refuse to common breast size specifics: Look young and you're banned', *Somebody Think of the Children*, 01 February 2010 <http://www.somebodythinkofthechildren.com/appearance-persons-age-no-comment-on-breast-size/>.

72 See Asher Moses, 'Baby swinging video classified MA', *Sydney Morning Herald*, 03 September 2009 <http://www.smh.com.au/technology/technology-news/over-the-top-childabuse-video-rated-ma15-20090903-f95t.html> (accessed 9 February 2010).

73 See Jenna Hand, 'Child abuse cartoon collector sentenced', *Canberra Times*, 03 February 2010 <http://www.canberratimes.com.au/news/local/news/general/child-abuse-cartoon-collector-sentenced/1740781.aspx>; Belinda Kontominas, 'Simpsons cartoon rip-off is child porn: judge', *Sydney Morning Herald*, 08 December 2008 <http://www.smh.com.au/news/national/simpsonsstyle-cartoon-is-child-porn/2008/12/08/1228584707575.html>.

Review by industry group of classification processes

EFA notes that the suggestion that an industry group be formed to consider the administrative arrangements of any mandatory ISP filtering scheme is relatively underdeveloped in the discussion paper. In general terms, EFA supports such a move to the extent that it will create an effective and legitimate means for public oversight of any classification scheme. The constituency, structure, and powers of this industry body would be critically important considerations in ensuring that it would be effective and legitimate. Without further details, however, EFA is reluctant to provide any further comment on the formation of such a group.

EFA tentatively supports 'Option six', which involves the formation of an industry group to consider the administrative arrangements of the bodies responsible for mandatory ISP filtering.