Internet Society of Australia
A Chapter of the Internet Society
ABN 36 076 406 801

C/- Maddocks, Level 7, 140 William Street
Melbourne, Victoria 3000
Accounts: P.O. Box 351, Glenorie NSW Australia 2157

To: Transparency Measures

Department of Broadband, Communications and the Digital Economy

By email: transparencymeasures@dbcde.gov.au

16 February 2010

MANDATORY INTERNET SERVICE PROVIDER (ISP) FILTERING; MEASURES TO INCREASE ACCOUNTABILITY AND TRANSPARENCY FOR REFUSED CLASSIFICATION (RC) MATERIAL

The Internet Society of Australia (ISOC-AU) welcomes this opportunity to comment on the Department's Consultation Paper 'Accountability and Transparency for Refused Classification Material'.

ISOC-AU is a non-profit society founded in 1996, which promotes the Internet development in Australia for the whole community. ISOC-AU is a chapter of the worldwide Internet Society and is a peak body organisation, representing the interests of Internet users in Australia.

ISOC-AU's fundamental belief is that the Internet is for everyone. We provide broad-based representation of the Australian Internet community both nationally and internationally from a user perspective and a sound technical base. We have a longstanding and ongoing commitment to the effective representation of these interests in self-regulatory processes in the telecommunications, domain name and Internet-related services industries. We also consistently promote the availability of access to the Internet for all Australians.

We acknowledge that the Minister's announcement on 'Measures to improve safety of the internet for families" in December 2009 represents Government policy and is not the subject of comment in this consultation process. We would nevertheless like to set out our position on this issue as the basis for our comments on the consultation paper, as follows:

1. GOVERNMENT DECISION ON INTERNET SAFETY

ISOC-AU supports Government policies that promote Internet safety, particularly for children. Specifically, we support the Government's announced expansion of cyber-safety education programs on Internet use run by ACMA for both kids and their parents. We also support the continuation of the ACMA cyber-safety Online Helpline program that provides information on safer ways to access and use the Internet.

The additional Government support will extend ACMA's educational activities to assist parents and teachers to deal with cyber-safety risks, reduce waiting times for schools to participate in ACMA's cyber-safety outreach program and increase the Cyber-Safety Online Helpline operating hours to ensure it is available when children are most at risk. These are all important and effective steps to increase cyber safety in Australia.

We note the Government's proposed grants program to encourage the introduction of optional filtering by ISPs. While individual families should be able to choose to have an Internet filter in their homes, they should be as effective and easy to use as possible. We note that under the previous policy, when many filters were made available at no cost to families, the take up of such filters was relatively low. We suggest that research be undertaken into the reasons for the low take up rate. Were the filters difficult to use; did they block too much content, or not enough? Addressing those questions could improve the take-up rate for families that choose to install Internet filters in their homes.

We also acknowledge with the Government's paper, Cyber Security Strategy that recognises the importance of a range of coordinated strategies, both national and international, to address both cyber security and cyber safety issues.[1]

2. ISP 'FILTERING'[2]

We do not support the Government's announced policy to require ISPs to block Refused Classification (RC) rated material hosted on overseas servers. ISPs should not have a role in determining content that their customers access. Their only proper role is to transfer packets from the sender to the recipient(s).

We also do not support the announced policy because we do not believe it will be practical or effective. It will not prevent access to a vast array of unacceptable material on the Internet either because it is delivered by means other than the web or because the URL of the material varies with each access. As the Enex Test Laboratory Report (the Report) recognised, with the ease of changing domain names and IP addresses, any such list can never be considered as either complete or current. Further, blocking of RC material will not stop children from viewing material that is inappropriate for them.

The Government's announcement suggests that the Report supports the efficacy (and utility) of blocking URLs on a very small blacklist. However, the Report highlighted that it is not feasible to filter traffic accessed through HTTPS, peer-to-peer, instant messaging, or any mechanism other than simple web traffic, including any sites using dynamic database-driven content where the URL varies with each access.

Other criticisms of the Enex test results, as set out in the Report, include:

- The test method tested scalability against the size of the blacklist but did not test the scalability of each of the solutions for high traffic levels – that is, results do not show how each solution varied in performance due to large amounts of traffic or a high rate of URLs per second

1 Attorney-General's Department, Cyber Security Strategy, 2009, at p. 6

2 Both the terms' filtering' and 'blocking' are used in the Government's policy statement of December 2009. Because all that will be required of ISPs is that they block access to URLs, the term 'blocking" is the correct term to use.

- There was no visibility of ISP topologies to identify where multiple filtering boxes might have been required to cover an ISP's complex service area so the test method does not provide any guidance to the likely cost to an ISP to implement a compliant filtering solution.

Because we believe that ISP blocking of RC material hosted overseas will not be effective and it has the potential to slow or damage the operation of the Internet for a wide range of users, including business, we do not support mandatory ISP blocking. In addition, our concern is such mandatory blocking will lead parents into a false sense of security, leading them to reduce their vigilance and oversight of their children working on the Internet.

3. REFUSED CLASSIFICATION MATERIALS

We oppose mandatory ISP blocking of URLs identified as containing RC material hosted overseas. If the Government proceeds with this policy, however, we make the following comments on both the use of the RC classification as the basis for blocking URLs and on questions asked in the Consultation paper.

As a guiding principle, ISOC-AU believes that, to as great an extent as possible, online regulation should be no more onerous than regulation in a similar offline context. Generally, RC material includes content that would be highly offensive to most people in any environment (child sexual abuse, bestiality, and sexual violence including rape) and should not be available.

However, as we noted in an earlier submission to the 2003 Review of Schedule 5 of the Broadcasting Services Act, (see www.isoc-au.org.au/Submissions/) the Internet is an enabling technology that provides access to a wide range of material. Policy solutions for off line material such as books, movies or computer games cannot be easily translated to the Internet.

Recommendation:
Where possible, Australia's laws should apply in the same way to RC material online as they do offline.

Our other concern with the use of the RC classification is that it includes many topics of legitimate public debate.

Under the RC classification guidelines, such material includes 'the detailed instruction of crime or drug use'.3 There are many 'crimes' for which the publication of detailed instruction on their implementation could be dangerous to society. However, the use of some drugs, or the nature of some 'crimes' such as euthanasia or the advocacy of informal voting or a form of voting which is legal but unconventional[4] are the subject of legitimate public discussion and debate, and should not be automatically included in a list of content to be blocked from the Internet. There is also quite legitimate debate about whether images that are readily available publicly (painting, photography or sculpture) should be classified as RC and therefore blocked.

3 Ibid.
4 See Langer v The Commonwealth [1996] HCA 43.

We also suggest that it may be appropriate to consider whether the list of material to be blocked be entirely outside of Government control, and developed by a group such as the Internet Watch Foundation.

Recommendation:
Before the classification of RC is used as the basis for blocking URL sites, it should be reviewed by an independent panel to ensure that only it only covers content that could be highly offensive to most of the public. Material that is the subject of legitimate public discussion and debate should not be blocked.

The Government should also consider whether the development of a list of material to be blocked could be done by an independent, respected organisation such as the Internet Watch Foundation.

4. OPTIONS TO INCREASE ACCOUNTABILITY AND TRANSPARENCY

The Consultation Paper lists six options to increase the accountability and transparency for the development of material put onto the RC content list. Our comments on the options are as follows:

Option One: Reference of all Material to the Classification Board for Confirmation of Classification.

The effect of this option would be to move responsibility from ACMA to the Classification Board for classification of all potentially prohibited content. While this would ensure consistency in the interpretation of classification guidelines, it may place an undue burden on the Board for classification of all prohibited and potentially prohibited material. An assessment should be made on how this option would impact on the workload of the Board before proceeding with consideration of the option.

Option Two: ACMA Notification Procedure.

Under existing legislation, if ACMA receives a complaint about material hosted overseas, AMCA must assess the content. It ACMA is satisfied that such material would be prohibited or potentially prohibited material, and the material is of 'a sufficiently serious nature' to warrant referral to a law enforcement agency, it must do so as well as refer the complaint to the relevant ISP under a Code (if in force) or order the ISP to take reasonable steps to prevent users from accessing the content.[5]

Under the Government's proposed policy change, once ACMA receives a complaint about what it then considers (after assessment unless Option One is followed) RC material hosted overseas it would put the URL on the list of sites to be blocked by ISPs. Under this option, ACMA would then notify owners of content hosted overseas (if the owner is readily identifiable and contactable) if their content has been classified as RC.

Websites are an increasingly important component for any business or organisation. Site owners (where known and contactable) should therefore be promptly informed that their site contains RC material and may be blocked. This will give an opportunity for legitimate site owner to have the classification reviewed or, in the case where a site has been hijacked, notification of the fact and the opportunity to rectify the situation.

[5] Clause 40, Schedule 5 *Broadcasting Services Act 1992*.

Recommendation:
We strongly support ACMA notifying site owners in a timely manner that their site content has been classified as RC.

Option Three: Blocking Notification Page and Appeal Mechanism

Under this option, end users seeking to access a blocked site would be advised that the content has been blocked, and possibly how a review of the RC classification can be sought.

Again, we strongly support this option. It will provide an opportunity for overseas owners of content who are not easily contactable to nevertheless learn that their content has been blocked and how to seek a review of that classification. It will also give end users information on how they can seek review of the classification of the content they are seeking.

Recommendation:
We strongly support a blocking notification page being used when a site has been blocked because it contains RC material.

Option Four: Incorporation of Content from International Lists

From the wording of the Minister's media release, this option appears to be part of the policy announced by Government already, and does not appear to be necessary.

Option Five: Review by an Independent expert and report to Minister and Parliament

This option would have an independent expert review classification processes annually, and report to Parliament and the Minister.

It is not clear what an independent expert undertaking an annual review of the classification scheme would add to the existing processes. It may also add uncertainty of classifications already made by adding another layer of review. The Classification Board has already developed guidelines that set out the factors to be taken account of for each level of classification, and there is a Classification Review Board to review classification decisions. Further, the Classification Board already reports annually to the Attorney-General on its work. If necessary, that report could be expended to include specific mention of classification of Internet content.

Option Six: Review by Industry Group of RC Content List Classification Processes

Under this option, an industry group would be formed to consider the administrative arrangements that ACMA and the Classification Board have in place to assess complaints and classify applications about online content.

We support this recommendation, but go further. We believe that such an industry group must include representatives of end users of the Internet. This will ensure that the processes used by ACMA and the Classification Board are not only administratively efficient, but clear, accessible and usable from the end user's perspective.

We also believe that, as stated above that the industry group must review RC classification guidelines before they are applied to material on the Internet that is to be blocked. As stated above, we believe there is material that could be classified as RC under current classification guidelines, but is the subject of legitimate public discussion and debate, and should be accessible on the web. We also believe the industry group should regularly review guidelines for material that is to be blocked.

Recommendation:
We support the formation of an industry group that includes representatives of Internet users as well as other industry members. We also recommend that the Industry Group be tasked with a review of the suitability of the RC classification as the benchmark in determining whether material should be blocked on the web.

The proposed scheme for blocking RC material hosted overseas should also include a mechanism whereby both website owners and users can seek review of the classification of material that has been classified as RC and blocked. Such review process should be independent of the original decision maker, and available quickly and at low cost.

In the case of businesses, a wrongful classification could have significant implications for that business. For end users, it will provide a mechanism to ensure that sites that do no more than provide legitimate (if controversial) public discussion are available. Indeed, if Options 2 and 3 are adopted as we advocate, they will only be effective if there an independent and quick appeal process to review such classification. Such mechanism could be an independent review panel within ACMA, or allow appeals to the AAT.

Recommendation
We believe that blocking regime should include a review process that is independent of the original decision maker, inexpensive and can quickly respond to review requests.

We will be happy to provide further comments on issues raised by this Consultation Paper

Tony Hill
President
Internet Society of Australia
President@isoc-au.org.au

Holly Raiche
Executive Director
Internet Society of Australia
ed@isoc-au.org.au