



SENATOR THE HON STEPHEN CONROY

MINISTER FOR BROADBAND, COMMUNICATIONS AND THE DIGITAL ECONOMY
DEPUTY LEADER OF THE GOVERNMENT IN THE SENATE

Internet filtering

Thank you for your correspondence concerning internet service provider (ISP) filtering. I appreciate your interest in this important issue.

I am aware that the issue of ISP filtering has attracted criticism from people who are concerned that it will lead to censorship of the internet.

Freedom of speech is fundamentally important in a democratic society. For many years however, most Australians have accepted that there is some material which is not acceptable, particularly for children.

The genesis of this is in civil society where social conflict is governed by the imposition of rules that restrain citizens from harming one another and society as a whole accepts that the public interest requires that those rules are enforced.

This is why we have the National Classification Scheme (the Scheme) for classifying films, computer games, and publications. Under the Scheme, it is illegal to distribute, sell or make available for hire material that is classified Refused Classification (RC).

The internet is already subject to regulation which prevents ISPs or other internet content providers from hosting prohibited content as defined under the *Broadcasting Services Act 1992* within Australia. Prohibited content is determined by reference to the Scheme. We also have strong criminal laws aimed at preventing people from possessing or distributing material relating to child sexual abuse, including over the internet.

The Australian Government recognises that the internet is an essential tool for all Australian children through which they can exchange information, be entertained, socialise and do school work and research. The ability to use online tools effectively provides both a skill for life and the means to acquire new skills.

Cyber-safety commitment

The Government has committed \$125.8 million over the next four years to a comprehensive range of cyber-safety measures, including law enforcement, filtering and education. Measures include:

- Expansion of the Australian Federal Police (AFP) Child Protection Operations Team - funding to detect and investigate online child sex exploitation;
- Commonwealth Director of Public Prosecutions - funding to help deal with the increased activity resulting from the work of the AFP to ensure that prosecutions are handled quickly;

- ISP-level filtering - funding to develop and implement ISP filtering, including undertaking a real world 'live' pilot;
- Education activities - funding to the Australian Communications and Media Authority (ACMA) to implement a comprehensive range of education activities;
- Websites / Online helpline - funding to ACMA to improve current government cyber-safety website resources and to make them easier for parents to use, and to provide up-to-date information. ACMA will also develop a children's cyber-safety website to provide information specifically for children, and improve the online helpline to provide a quick and easy way for children to report online incidents that cause them concern;
- Consultative Working Group - funding for an expanded Consultative Working Group. This group will consider the broad range of cyber-safety issues and advise the Government, to ensure properly developed and targeted policy initiatives;
- Youth Advisory Group - funding for a Youth Advisory Group which will provide advice to the Consultative Working Group on cyber-safety issues from a young person's perspective; and
- Research - funding for ongoing research into the changing digital environment to identify issues and target future policy and funding.

International cooperation in regard to online safety is crucial. The Government is pursuing an international agenda for collaborative action on cyber-safety. Progress on this was made through my recent engagement at the Organisation for Economic Cooperation and Development (OECD) forum in Seoul in June 2008. The Seoul Declaration for the Future of the Internet Economy states that participating economies agree to 'Ensure a trusted Internet-based environment which offers protection to individuals, especially minors and other vulnerable groups'.

Education

The above initiatives will tackle the issue of cyber-safety from a number of directions. More importantly, this approach is based on the key role parents and carers have in the online safety of children, and provides them with the necessary information to assist with this task.

In particular, ACMA's Outreach program has been expanded to provide additional general cyber-safety awareness presentations to teachers, parents and students which highlight the key issues and strategies to minimise potential online risks. The program will also include professional development on online safety issues for existing and trainee school teachers.

ISP filtering

A part of the Government's plan is to examine the introduction of ISP-level filtering. The Government's policy will be developed through an informed and considered approach, including industry consultation and close examination of overseas models to assess their suitability for Australia.

Filtering technologies have been adopted by ISPs in a number of countries including the United Kingdom, Sweden, Norway and Finland, predominantly to filter child pornography. In these countries ISP filtering has not affected internet performance to a noticeable level.

Laboratory trial and live pilot

ACMA has completed a laboratory trial of a sample of the available ISP filtering technologies. The trial looked specifically at the effect of a range of filter products on network performance, effectiveness in identifying and blocking illegal content, scope to filter non-web traffic and the ability to customise the filter to the requirements of different end-users.

The laboratory trial indicated that ISP filtering products have developed in their performance and effectiveness since they were last assessed in 2005. The Government is now proceeding with a 'live' pilot which will provide valuable information on the effectiveness and efficiency of filters installed in a 'real world' ISP network. The live pilot is proceeding in close consultation with the internet industry.

The Government is committed to working closely with the internet industry to address the concerns of network degradation, over and under blocking, circumvention and costs. These concerns will be carefully considered during the pilot and will further inform the Government's cyber-safety policy.

The Department of Broadband, Communications and the Digital Economy (the Department) has prepared material on a list of Frequently Asked Questions (FAQs) regarding ISP filtering. This list is available on the Department's website at www.dbcde.gov.au/cybersafetyplan.

These FAQs will be updated regularly to provide you with the most up to date information on ISP filtering issues.

ACMA Blacklist

The existing ACMA blacklist is a list of internet web pages which are defined as 'prohibited' under Australian legislation. The list has been in place since 2000 and currently contains around 1300 URLs.

ACMA has also negotiated agreement with the UK Internet Watch Foundation (IWF) facilitating access to the IWF's list of child abuse image URLs.

ACMA is also working with the Australian Federal Police to arrange access to the USA National Centre for Missing and Exploited Children list of child abuse image websites.

In consultations with ISPs, concerns have been raised that filtering a blacklist beyond 10 000 URLs may raise network performance issues, depending on the configuration of the filter. The pilot will therefore seek to also test network performance against a test list of 10 000 URLs.

This will be a closed network test and will not involve actual customers. The list of 10 000 sites will be developed by the technical organisation assisting the Department on the pilot, which has access to lists of this size. As this test is only being performed to test the impact on network performance against a list of this size, and actual customers are not involved, the make-up of the list is not an issue.

The ACMA blacklist is developed by complaints by the public about online content to the ACMA hotline. ACMA does not arbitrarily assess and classify content. Online content is assessed in accordance with the National Classification Scheme. The Scheme was established by the *Classification (Publications, Films and Computer Games) Act 1995*. Content which is the subject of a complaint is assessed by ACMA and in some instances referred to the National Classification Board for classification.

The ACMA complaints process has been established by the Australian Parliament through the *Broadcasting Services Act 1992*. If content is found to be prohibited and is hosted in Australia (i.e. located on a computer or server in Australia), ACMA will direct the content provider to remove or prevent access to the content. If content is found to be prohibited and is hosted overseas, ACMA must add the material to its blacklist.

ACMA officers and Classification Board members applying the Scheme are highly trained and apply criteria set out in the Scheme's legislative framework. Further, decisions made by the Classification Board can be reviewed by the Classification Review Board.

The scope of the definition of prohibited content in legislation cannot be expanded without changes to legislation being passed by Parliament.

Thank you for your interest in this matter. I hope this information will be of use.

Yours sincerely



Stephen Conroy
Minister for Broadband,
Communications and the Digital Economy