



SENATOR THE HON STEPHEN CONROY

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

Cyber-safety and internet service provider filtering

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

The Australian Government recognises that the internet is an essential tool for all Australians through which they can exchange information, be entertained, socialise, 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.

Unfortunately the internet can also be used inappropriately. It has provided a powerful new medium which can be used to distribute material which is not acceptable to most Australians, particularly children.

The complexity of the issue is why the Government has always maintained there is no silver bullet solution to cyber-safety. In developing our approach we have been informed by the Government's pilot of ISP level filtering and extensive industry feedback about the most appropriate way to improve safety online. In particular our approach has been informed by the constructive input of Australia's four largest ISPs, who came forward with a set of principles which the Government has taken into account.

The Government's approach involves a comprehensive suite of measures to address the range of issues and challenges faced by families when they are online. These measures build upon the Government's existing cyber-safety plan which includes law enforcement, education and information, research and international co-operation. \$125.8 million was allocated to this plan in the 2007-08 budget, which included funding for 91 Australian Federal Police officers to the Child Protection Operations Team.

The Government has recently announced three new measures to enhance its existing cyber-safety program, all from within the existing funding:

- Introduction of mandatory ISP-level filtering of Refused Classification (RC) content in order to reduce the risk of inadvertent exposure. RC material includes child sexual abuse imagery, bestiality, sexual violence, detailed instruction in crime, violence or drug use and/or material that advocates the doing of a terrorist act.
- A grants program to encourage ISPs to offer additional filtering services to households on a commercial basis and optional basis.
- Funding of \$17 million over five years for a range of education, awareness and counselling services based on recommendations from the Government's 300 strong Youth Advisory Group, and advice from its Consultative Working Group on Cyber-safety.

These measures tackle the issue of cyber-safety from a number of directions and provide parents and carers with the necessary information to assist with this task.

ISP level filtering of RC Content

The Government will introduce legislation to require ISPs to block URLs (a specific address of content that leads to a web page) of overseas hosted content which is rated RC. This is content that is currently unable to be hosted within Australia.

RC rated content is illegal to distribute, sell, display or make available for hire in any format in Australia: one cannot obtain such material on the shelves of libraries, newsagencies or in the cinema. It certainly cannot be viewed on television or hired on a DVD.

Enex Testlab, an independent testing laboratory, recently completed a live pilot into the effectiveness and efficiency of ISP level filtering. The pilot involved nine ISPs of varying sizes and their customers, and assessed a number of different filtering technologies.

Enex found that a defined list of URLs can be filtered with 100 per cent accuracy, and negligible impact on internet speed. Telstra's own testing has provided the same results.

This pilot, and the experience of ISPs in many western democracies, shows that ISP level-filtering of a defined list of URLs can be delivered with 100 per cent accuracy. It also demonstrated that it can be done with negligible impact on internet speed.

Filtering technologies have been adopted on a voluntary basis by ISPs in a number of countries including the United Kingdom, Canada, Sweden, Norway and Finland, predominantly to filter child pornography. In these countries, ISP filtering has not affected internet performance to a noticeable level. Germany has passed legislation to block such content and Italy has issued a Ministerial decree.

Some opponents of the policy are trying to misrepresent the figures in the Enex Testlabs report by suggesting that a figure of less than ten per cent is substantial. To put that into the context of real time, Australia's largest ISP, Telstra, undertook its own testing that showed the impact on internet performance would be less than one seventieth of the blink of an eye!

Under the National Classification Scheme and related enforcement legislation, it is already illegal to distribute, sell or make available for hire RC rated films, computer games and publications.

This material is currently subject to take-down notices by the Australian Communications and Media Authority (ACMA) if it is hosted in Australia. However, ACMA is unable to directly regulate content hosted overseas.

The Government will therefore introduce legislative amendments into Parliament to require all ISPs, starting twelve months from the passage of the legislation, to filter RC material hosted on overseas servers.

The Government has always said that filtering is not a silver bullet solution and that it is possible that filtering may be circumvented by a technically competent user; however, it is part of a suite of measures that will help to reduce the risk of inadvertent exposure to RC material, particularly by children.

The Government will discuss with industry measures to help smaller ISPs to filter the RC content list if they cannot access a filtered wholesale or re-sold service.

RC content list

The RC Content list will be compiled based on public complaints to ACMA, which will be assessed using existing criteria set out in the National Classification Scheme. Where the material is found to be RC, it will be added to the list.

ACMA will also add the URLs of known child abuse material through sharing lists with highly regarded international agencies after an assessment of the rigor of the processes used by these agencies to compile their lists.

ACMA is receiving additional funding to enhance the security of the RC Content list and to automate its transmission to ISPs.

Accountability and transparency

The Government is seeking submissions from the public on additional measures to improve the accountability and transparency of processes that lead to RC material being placed on the RC content list.

Some of the options raised include the use of block pages and appeal mechanisms, notification to website owners of RC content, and a review of classification processes by an independent expert and report to the Australian parliament.

The consultation paper is available at www.dbcde.gov.au/cybersafetyplan.

Additional optional ISP level filtering

ISPs will be encouraged to offer additional filtering services through the availability of government assistance. This is not mandatory.

For families that wish to have a wider range of material filtered, including potentially X18+ content and gambling sites, the Government will establish a grants program to encourage ISPs to offer these services on a commercial basis. This will help parents to choose what they want filtered.

Education, awareness and counselling

To further provide Australian internet users, particularly children, with a safer online environment, additional funding has been allocated to ACMA to continue and expand education activities to help deal with cyber safety risks, including cyber bullying.

In particular waiting times for schools participating in the ACMA cyber-safety outreach program will be reduced, and the operating hours for the Cyber-Safety Online helpline will be increased to ensure its availability when children are most at risk.

Information on both the existing and new cyber-safety measures is available at www.dbcde.gov.au/cybersafetyplan. This information includes the Enex report on the ISP filtering live pilot, frequently asked questions, and the public consultation paper on measures to improve accountability and transparency of the RC content list.

Thank you for your interest in this matter. I trust this information will be of assistance.

Yours sincerely

A handwritten signature in black ink that reads "Stephen Conroy". The signature is written in a cursive style with a loop at the end of the word "Conroy".

Stephen Conroy
Minister for Broadband,
Communications and the Digital Economy