

7 Technical Reasons Mandatory Filtering Won't Deliver Real Child Safety

Our peer-reviewed analysis demonstrates that the proposed filter would not deliver the kind of safety for kids online that the Government is looking for. Here are seven technical reasons the proposed plan will not deliver real online safety.

In November 2008, following the Cyber Safety Plan, the Rudd Government released the Internet Service Provider Content Filtering Pilot – Technical Testing Framework, which proposed a live-ISP filtering pilot. The pilot was designed to test the ability of ISP level filtering to block content from versions of the Australian Communications and Media Authority (ACMA) blacklists for websites containing Restricted Content (RC).

The implementation of mandatory filtering is a massive technical and logistical undertaking.

1. The testing did not follow the technical testing framework

The ISP filtering pilot/trials, and the related report from Enex Testlabs, both of which were relied on in the formulation of the filtering policy by the government, did not follow the Department of Broadband, Communications and the Digital Economy's own 2008 Technical Testing Framework.

The Internet Service Provider Content Filtering Pilot – Technical Testing Framework set out a number of aims for live pilot tests, but the pilot tests failed to address these issues.

The Testing Framework recommended testing blacklists of 10,000 URLs but the version of the ACMA Blacklists tested only included 1000 URLs.

The framework recommended correlation and comparison between different filtering solutions, but the pilot tests undertook no comparisons of this kind.

The framework recommended testing the impact of filtering on ISPs and end-user, but only tested the impact on end-users.

The framework recommended that over-blocking and under-blocking be assessed, but tested only for the impact of over blocking sites.

The framework recommended that the pilot seek information on privacy and security from end-users, but the pilot failed to fulfil this commitment.

2. Initial tests of ISP level filtering were unrepresentative

The initial tests included only 9 ISPs out of a possible 500 in Australia.

These ISPs were self-selected.

Telstra was not included in the pilot tests.

We have no way of telling how far we can extrapolate the results of the pilot tests, because no information is available about the number of customers participating in them.

3. Tests were conducted at very low speeds

The speed of the proposed National Broadband Network is 100 megabits per second or 12 megabits per second for wireless.

Yet the pilot tests were undertaken at 8 megabits per second.

The results cannot be extrapolated to the higher band-width connections.

Continued >

4. Proposed system will slow down the internet

The best performing filter caused only a two (2) percent degradation in performance across the network, but was among the least effective filters.

5. The proposed system will not work for high-volume sites

The filter would not work for high volume sites such as Wikipedia, YouTube, Facebook, Twitter, as the impact of the filter on Internet access speeds would be too great.

The Enex report, and a separate report from Telstra, acknowledged that filtering systems would struggle to handle the filtering of high volume sites, with the Enex report stating in situations where there is a potential for very high traffic ISP level filtering “could cause additional load on the filtering infrastructure and subsequent performance bottlenecks.”

6. The proposed system is simple to bypass

Every system tested in the pilot could be circumvented by up to 37 test methods.

Simple tactics like publishing web-links as https:// links instead of http:// means that content filtering cannot be applied to those links.

No additional software is required, and the end user does not need to perform any complex configuration.

This technology is already built into users’ web browsers.

7. Blocked content can still be distributed easily

A large proportion of child sexual abuse content is not found on public websites, but in chat-rooms or peer-to-peer networks.

We know the proposed filtering regime will not effectively protect children from this objectionable material because of the ease with which blocked content can still be distributed.

There are a number of ways to distribute RC which sidestep mandatory ISP level filtering. RDP (remote desktop protocol), bit torrent, Email, FTP, IRC, Usenet and twitter can all be used to distribute RC.

This means that if the filtering is sidestepped using the methods mentioned above, it can then very easily be distributed via other methods.