

We, the Australian Library and Information Association, Google, Inspire Foundation, Yahoo!, Internet Industry Association, Internet Society of Australia, and System Administrators Guild of Australia agree that Australia needs to take *effective* action to ensure that internet users, and particularly children, have a safe experience online.

In December 2009, Minister Stephen Conroy announced the details of the government's proposals for mandatory filtering by ISPs of online content in the Refused Classification (RC) category. We welcome the Minister's invitation for consultations on the proposed policy.

Mandatory filtering of RC material is a significant Australian public policy proposal that should matter to every parent, young person, school and business. A discussion designed to achieve the balance between protecting children, preserving the benefits of internet access and treating adults like adults is welcome.

As 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.

In fact, the policy may give parents a 'false sense of security' encouraging them to reduce their supervision.

We are concerned that the scope of content to be filtered is too wide. Filtering all RC material could block content with a strong social or educational value.

The implementation of mandatory filtering is a massive technical and logistical undertaking. We note with concern that 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 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 sites, such as YouTube, to have pages on the filtering list, this could result in significantly higher traffic rates passing through the filter, even though the specific pages being accessed are not those on the blacklist. This could cause additional load on the filtering infrastructure and subsequent performance bottlenecks".

According to a large body of peer-reviewed research on the matter the most effective way to protect our children on the internet is achieved by adopting a strategy containing the following three **Core Principles**:

- **Education:** Properly funding a ***national comprehensive cyber-safety education program*** for children and parents on how to avoid inappropriate material and stay safe online. If any element of online safety is to be mandatory, it should be education.
- **Policing:** Significantly increasing and funding the level of oversight by the government and federal police focused on the locations, such peer-to-peer, where child sexual abuse materials are disseminated.
- **Technical Measures:** If the government and the broader political system are determined to implement technical measures as part of online safety efforts, then we believe Australia can learn from the approaches adopted in peer countries, particularly in Europe. The strong consensus internationally is for ISPs, police and government to work together in partnership targeting a clearly defined and narrow band of child sexual abuse material.
  - Under this filtering regime:
    - there would be little to no impact on the internet's performance or greatly increased costs to users;
    - there would be an environment in which adults are able to choose whether to have their service filtered or not.

We urge further adjustments to the government's proposal in the interest improving online safety for young people and look forward to working with the government to that end.