17

Proposal for a mandatory filtering system

17.1 A significant amount of attention in this Inquiry focused on a proposed national, mandatory filtering scheme so that internet service providers (ISPs), can remove access to Refused Classification material online. Other ways of restricting access will also be outlined. Refused Classification material includes child sex abuse, bestiality, extreme violence including rape, detailed instructions on crime or drug use, and advocating a terrorist act. The Government has stated that Refused Classification C content has no place in our society and therefore should not be available in the internet.

17.2 Significantly, three of Australia's largest ISP's, Telstra, Optus and Primus, have agreed to voluntarily block child abuse material at the server level. Webshield, and ItXtreme have also volunteered to block this content.

Background

17.3 The role of the Australian Communications Media Authority (ACMA) in regulating online content is to administer the co-regulatory scheme established under the *Broadcasting Act 1992* (the Act). Complaints about online content can be made to ACMA and, if the material is found to be prohibited or potentially prohibited, it must either:

- issue an interim or final take-down notice (for content hosted in Australia); or
- refer the content to industry accredited Family Friendly Filters (for content hosted overseas) under a recognised alternative access-prevention arrangement outlined within a registered Code of Practice.

17.4 The online content co-regulatory scheme is under-pinned by the National Classification Scheme (NCS), applicable to films, computer games and certain publications. Determinations about prohibited/potentially prohibited material are made by reference to classification categories established under the NCS.

17.5 ACMA must refer Australian-hosted content that is potentially prohibited to the Classification Board for classification before it can take action. Content hosted overseas may be referred to the Board.

17.6 Prohibited or potentially prohibited content is assessed against the following classification categories:

- Refused Classification, including offensive depictions of children and material advocating terrorists acts;
- X18+;
- R18+ items not subject to restricted access systems; and
- Certain limited MA15+ content classified MA15+, provided for profit or on payment of a fee and not consisting of one or more images and/or text.

17.7 There are no technical issues preventing the adoption of filtering a list of URLs, and many ISPs around the world have been doing so voluntarily 'for many years'.[1]

17.8 Late in 2010, Telstra Corporation, Optus and Primus agreed to introduce voluntary filtering of child abuse URLs on ACMA's list of prohibited sites. These ISPs cover about 70 percent of all Internet users in Australia. About 30 percent of ACMA's black-listed sites included depictions of child abuse and child sexual abuse material.[2] Recently, Webshield, and ItXtreme have also volunteered to block child abuse material at the ISP level. The Government will continue to encourage other Australian ISPs to follow the example of these ISPs.

17.9 ACMA is working to develop measures to enable these prohibited sites to be transmitted to participating ISPs on an automated and secure basis. It

1 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS6-7.

2 Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011; Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, pp. CS4, 5, 8; Ms Sharon Trotter, Acting Executive Manager, Security safety and e-Education Branch, Australian Communications and Media Authority, p. CS6.

awaits responses to invitations to these three ISPs to begin trialling that transmission.[3]

17.10 The Department of Broadband, Communications and the Digital Economy was hopeful of getting the cooperation of other ISPs to filter voluntarily material on ACMA's blacklist, by working with the Internet Industry Association. That body has announced that it will assist in encouraging a wider range of ISPs to adopt voluntary filtering.[4] Until recently, ISPs have refused to take action on blocking Refused Classification material.

17.11 There is no evidence of reluctance by ISPs to take down Refused Classification material, and it is not clear that legislation would be any more effective than a voluntary arrangement. The user policies of large multi-national websites are 'very broad' and cover a 'much wider range' of material they can take down, compared to what is described as 'inappropriate' in the Act.[5]

17.12 Under its powers in the Act, ACMA also issues industry codes to ISPs, and these co-regulatory instruments are enforceable immediately they are registered. Compliance is 'close to universal' and probably as high as would be achieved by legislation.[6]

17.13 Mr Mark Newton made the point that about two-thirds of Australian households do not have school age children and applying restrictions to these households would be poor targeting.[7]

17.14 Further, according to ACMA surveys, between 40 and 50 percent of parents use filtering devices at home. Considerable evidence was presented to this Inquiry on the range of such devices.[8] These devices more material than Refused Classification content.

---

3 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS4, 11.

4 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS5-6, 4.

5 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS14.

6 Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association, *Transcript of Evidence*, 11 June 2010, p. CS43.

7 Mr Mark Newton, *Submission 15*, p. 5.

8 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS8, 12.

17.15 There are many commercial and free filtering options available, at many levels:

- search engines, such as Bing, Yahoo! and Google;
- browser level, including Microsoft; and
- software applications, such as a product of a US company Blue Coat.[9]

17.16 However, there is a lack of awareness by parents.

17.17 While most participants concentrated on expressing views of the filtering of Refused Classification material, Symantec Corporation noted that less than 50 percent of small to medium businesses in Australia had security systems installed and operating. Only when they became victims of fraud or identity theft did such businesses seek out educational resources or assistance from government agencies, or the police.[10]

Support for the proposal

17.18 BraveHearts saw ISP filtering as part of a 'holistic' approach to online threats. It argued that material such as child pornography, already blacklisted by ACMA, breached Australian laws and it was illegal to produce, own and distribute it. It should not be available online. This organisation supported a second tier of filtering that would allow families, organisations or businesses to request optional filtering of other objectionable material, such as promotions of terrorism, suicide, drug use or adult pornography. It was aware that no filtering systems were foolproof, and that they can be circumvented.[11]

17.19 The Victorian and Tasmanian Synod of the Uniting Church gave four reasons for requiring ISPs to block Refused Classification material:

- Sale and distribution of this category is already banned in all other media, including the Internet hosted in Australia;

9 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS8, 23.

10 Mr Craig Scroggie, Vice President and Managing Director, Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, p. CS35.

11 BraveHearts, *Submission 34*, p. 10.

- They have a 'crucial role' in preventing the domestic consumer from accessing it by accident, and in preventing those who do not know how to access it but are curious, as well as those who are at an early stage of developing or feeding a sexual interest in children;
- It undermines the commercial trade in images of child abuse and actively disrupts its success; and
- It is reasonable to expect ISPs to accept some responsibility for what their clients seek to view, and for the material to which they provide access.

17.20 The Synod did not see placing such obligations on ISPs as a replacement for education and awareness programs and law enforcement, but as a complementary measure to a wider cyber-safety strategy. Requiring ISPs to be socially responsible and not facilitate trans-national criminal activity would assist in providing increased cyber-safety to young people who would otherwise become victims of the demand for commercial child sexual abuse materials.[12]

17.21 Family Voice Australia supported the proposal for mandatory ISP-level filtering, noting that opponents' arguments could be addressed because:

- There would be minimal degradation to Internet performance;
- The right to free access to information has always been qualified by the need to protect the community, and there was no logical reason why the Internet should be different;
- The implementation of any filtering scheme would be protected by scrutiny in the Parliament and in the media; and
- Even if a total blockage of all Refused Classification material cannot be achieved, a significant reduction was a worthwhile goal. [13]

17.22 It believed that including some of the following features when the proposed scheme was implemented could improve cyber-safety:

- Providing an R18+classification for computer games;
- Excluding X18+ material; and

12 Victorian and Tasmanian Synod of the Uniting Church, *Submission* 93, p. 4.

13 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS5, 6.

- Ensuring that ACMA's black list was not simply compiled from complaints and the supply of lists of child abuse sites from overseas enforcement agencies. [14]

17.23 Family Voice Australia also suggested that a tender should be sought for a system based on a web crawler that actively seeks out URLs containing prohibited material.[15]

Concerns about the proposal

17.24 Ms Robyn Treyvaud noted that, as technology being used at schools can be bypassed using proxy sites, if mandatory filtering was introduced there would be no way of knowing what students were accessing.[16]

17.25 The NSW Secondary Principals' Council stated that consideration needed to be given to differentiating filters for staff and students. It is difficult for school personnel to follow-up an issue when the site is blocked to staff.[17]

17.26 While Professor Marilyn Campbell supported filtering pornography out, she thought that filtering only worked when children were actually protected from accidentally going into inappropriate sites.[18]

17.27 The Northern Territory Government stated that there was a significant role for researchers to develop filtering software that was 'effective and non-cumbersome'.[19]

17.28 Symantec Corporation noted that, in the past, young people had not been stakeholders in proposals for filtering. Unless they were included, they would find ways around the technology.[20] Young people's views on Internet filtering are discussed below.

17.29 The Australian Privacy Foundation believed that the current proposal had been developed and debated without the expected level of investigation of issues, such as the nature of purported harms, the limits and application of

14 Family Voice Australia, *Submission 50*, pp. 6-7.

15 Family Voice Australia, *Submission 50*, pp. 6-7.

16 Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS36. See Chapter 8 for schools' duty of care.

17 NSW Secondary Principals' Council, *Submission 32*, p. 1.

18 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS36.

19 Northern Territory Government, *Submission 84*, p. 10.

20 Mr Craig Scroggie, Vice President and Managing Director, Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, p. CS34.

various remedies and regulatory models against current/future versions of those harms and comparisons with other options.[21]

17.30 The Victorian Office of the Child Safety Commissioner stated that it was important to strike the right balance between filtering harmful material, particularly for younger children, while still enabling older children access to information about issues relevant to them.[22]

17.31 The Australian Library and Information Association opposed filtering on the basis of freedom of access of information and would like to find a balance between censoring adults and protecting children.[23]

Other views

17.32 The Queensland Catholic Education Commission has online filtering, and there is monthly feedback to schools about sites that are accessed in each case. It believed, however, that the major focus should be on the development of positive e-security habits for all users, rather than on technological solutions such as filtering. These simply present a challenge to those who are 'computer savvy, and are rapidly superseded as technology advances. The Commission saw filtering as part of a package, and emphasises giving skills to students to have the right attitudes. It saw putting key values in place, and giving some specific skills and attitudes, as the most effective way of dealing with Cyber-safety.[24]

17.33 Referring to 'problematic Internet use', Netbox Blue noted that if a filter was installed, many people would consider that their technological problem(s) had been solved.[25]

17.34 The Safer Internet Group reiterated that the proposed filter would give parents/carers a false sense of security about online safety, and that it has changed the way the world viewed Australia.[26]

17.35 Facebook has two concerns about the proposal:

---

21 Australian Privacy Foundation, *Submission 83*, p. 4.

22 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 4.

23 Australian Library and Information Association, *Submission 16*, p. 8.

24 Queensland Catholic Education Commission: *Submission* 67, p. 4; Mr Michael Wilkinson, Executive Secretary, *Transcript of Evidence*, 17 March 2011, pp. CS28, 27.

25 Mr John Pitcher, Director of Strategic Business Development, Netbox Blue, *Transcript of Evidence*, 8 July 2010, p. CS17.

26 Safer Internet Group, *Submission 12*, p. 1; Australian Library and Information Association, *Submission 16*, p. 9.

- It will distract people from other things that need to be done to make the Internet safe; amd
- Filtering attracts social costs, as there may be a 'chilling effect' on expression. It also has economic costs, as some investment in innovative ways to use new information in Australia will go elsewhere if there is a government screen.[27]

17.36 Professor Karen Vered did not think that the government needed to dictate 'a kind of blanket filtering', and believed that parents/carers should make their own decisions about purchases, installation and learning how to use it. Filtering would be costly and put Australia at an even greater disadvantage internationally. It would also make Australian ISPs responsible for problems they had not caused, as they are not responsible for 'unsavoury material' from foreign sites. If Australian ISPs were to be made responsible for filtering, their costs would be passed onto consumers.[28]

17.37 Moreover, technological barriers are not a solution, as they are not going to help young people develop their ability to discriminate, evaluate and act under circumstances where they are required to exercise their own judgement.[29]

17.38 While supportive of the Government's initiative in proposing to filter child pornography and extremely violent content, Symantec Corporation noted that filtering did not solve issues such as fraud, identity theft, or cyber-bullying.[30]

17.39 The Alannah and Madeline Foundation confirmed that home filtering was not often applied, despite the widespread availability of systems. When it was applied, there was a risk that parents/carers were given a false sense of security about access to inappropriate content, or the risk of their children being contacted by strangers online. Parents/carers were then encouraged to think that their children could be left to go online

27 Internet Industry Association, 'Facebook on mandatory ISP filtering', 13 May 2010, <http://www.iia.net.au/index.php/component/content/article/80/826-mozelle-thompson-facebook-on-mandatory-isp-filtering.html>, accessed 3 March 2011.

28 Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, p. CS38.

29 Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, p. CS37.

30 Mr Craig Scroggie, Vice President and Managing Director, Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, pp. CS18-19.

unsupervised. 'Software cannot replace the eyes and awareness of an engaged parent or carer.'[31]

Feedback from young Australians

17.40 The Committee's *Are you safe?* survey asked participants what they believed could be done to make the internet safer. Though young people appear to welcome localised internet filters installed on personal computers, they are less receptive of an ISP-level filter.

31 Alannah and Madeline Foundation, *Submission 22*, p. 29.