16

New technologies

16.1 It is important that Australia maximises opportunities presented by new and emerging technologies allowing for the evolution of digital economy and interactive educational opportunities. These technologies are usually accompanied by protective mechanisms to deal with risks online. Although this Report has examined behavioural aspects of promoting cyber-safety and reducing cyber-bullying, new technologies can form part of a multi-faceted solution.

16.2 Inspire Foundation emphasised the opportunities provided by technological advances to impact positively on the lives of young people:

> in order to utilise and not diminish this potential, the approach to addressing issues of cyber safety must be cross-sectoral, multi-faceted and dynamic, reflecting the complexity of the online environment itself.[1]

16.3 BoysTown points out that this provides the opportunity for Australia to enhance online services, and suggested that:

> the Australian Government increase its funding for research into the use of new communication technologies and online help-seeking amongst young people to provide an evidence base for the engagement of youth in relation to health and other issues of concern.[2]

---

1 Inspire Foundation, *Submission 3*, p. 12.

2 BoysTown, *Submission 29*, p. 18.

Safeguards

16.4 The Australian Communications Consumer Action Network (ACCAN) considers that 'the best way for consumers of all ages to safely navigate the online environment is to be empowered with relevant, reliable and useful cyber-safety information.' It proposed that:

> Consumers should be provided with the tools to take more responsibility for their own cyber-safety. ACCAN proposes the development of an Online Competency Skills Test in Online Security (the Online Security). This test would help consumers assess how well they understand cyber-safety issues and could provide details of what steps they can take to better protect themselves and links to further online security information.[3]

Recommendation 24

That the Australian Communications and Media Authority facilitate the development of and promote online self assessment tools to enable young people, parents/carers and teachers to assess their level of awareness and understanding of cyber-safety issues.

16.5 The Department of Broadband, Communications and the Digital Economy has introduced a number of initiatives such as the *Stay Smart Online* E-security education package, E-security Awareness Week and ScamWatch. Another example is *SpamMATTERS*, created by the Australian Communications and Media Authority (ACMA), enhancing the positive effect of the *Spam Act 2003* (Cth).[4]

16.6 The American Online Safety and Technology Working Group was established in 2008 and comprises representatives from the Internet industry, child safety advocacy organizations, educational and civil liberties communities, the government, and law enforcement communities. Technology is now available to address issues such as password security:

> A survey conducted on over 250,000 user social networking accounts by BitDefender found that over 75% used the same

3 Australian Communications Consumer Action Network, *Submission 1*, p. 3.

4 Australian Communications Consumer Action Network, *Submission 1*, p. 5.

> password for multiple accounts. This means an attacker may secure a victims password to gain control of an account by simply enticing them to establish an account at site already controlled by the attacker.[5]

Some solutions

16.7 Participants in the Inquiry suggested many different solutions to cyber-safety abuses, demonstrating that many technologies are available but also that they are accompanied in most cases by in-depth cyber-safety policies.

16.8 As examples, four of these proposals, drawn from participants in Queensland, are outlined below.

Family Friendly Filter

16.9 From its experience in dealing with schools across Australia, Netbox Blue saw five cyber-safety threats:

- Access to inappropriate web content;
- Access to online forums with a risk of predators;
- Communication of bullying messages by email, social networking sites, or text;
- The risk of 'cyber addiction' to online gambling, or social networking sites, and
- The impacts of the proliferation of social media applications and other Internet-related activities on learning.

16.10 It believes that, for students' safety on the Internet, four pillars need to exist before there is any chance of combating these online threats.

- Up-to-date policies for all Internet, social networking sites, and mobile devices inside and outside schools need to be created and implemented. These must include clear consequences for inappropriate actions, must be kept up to date and communicated regularly to all stakeholders;
- Stakeholders need education about dangers, and on ways of minimising or dealing with them;

5 Amorlog International *Submission 4.1*, p. 3.

- Technological enforcement is necessary, both inside and outside schools, on all school-owned equipment to help prevent or block any inappropriate use, and alert appropriate school authorities; and
- Regular reviews of attempted policy breaches are necessary to improve education and manage individual behaviour, with clear consequences for offenders.[6]

16.11 For a school of 750 students and 100 staff, and depending on the features adopted, the cost of the Family Friendly Filter would be 6.4 cents per day per user.[7]

Throttling bandwidth

16.12 In the second term of 2011, the Queensland Catholic Education Commission will be trialling throttling bandwidth on school networks when students logon to specific sites, so that their speeds are slowed to the point that they are almost useless.[8]

Central monitoring of access

16.13 While not as obvious as throttling bandwidth, there are other programs that can monitor from a central position, in a school library for example, what sites are being accessed. Thus, when students begin a class at any level in a school library, they are told that the teacher librarian has the ability to see which computer each of them is using, for how long, to whom they have sent emails and what sites they have accessed. When students know that they are being monitored in this way, it is found that inappropriate access 'suddenly lessens considerably'.[9]

Australian Protected Network

16.14 Web Management InterActive Technologies is developing systems that build online communities and relationships essential for success in business. It noted that, although there are many solutions to cyber-safety issues, these have little uniformity or longevity. Nor is there a uniform way to contact parents/carers about the range of available cyber-safety

6 Mr John Fison, Chairman, Netbox Blue, *Transcript of Evidence*, 17 March 2011, p. CS48.

7 Mr John Fison, Chairman, Netbox Blue, *Transcript of Evidence*, 17 March 2011, p. CS51.

8 Ms Anita Smith, Senior Education Officer, Student Wellbeing , Learning and Teaching Services, Brisbane Catholic Education, *Transcript of Evidence*, 17 March 2011, pp. CS27-28.

9 Ms Karen Bonnano, Executive Officer, Australian School Library Association, *Transcript of Evidence*, 17 March 2011, pp. CS33-34.

options. To be effective, measures must be integrated, become accepted, rather than a one-off government program.[10]

16.15 It has developed the Australian Protected Network (APN) that would put control in the hands of parents/carers, allowing them to set limits on sites accessed by their children. It is a framework which enables users to control and shape their 'online view', by putting in a basic level of protection. Users then modify the approach according to their needs.[11]

16.16 If implemented, the APN would produce a point of contact for each Internet user in Australia, and information can easily be forwarded to them.[12]

16.17 Among its features, APN:

- Allows/disallows access to different classes of product or web site. One selection could be the blocking of all direct external ISP access and disallowing web access to chat web sites. Another selection might simply block criminal/fraud activity and online gambling;
- Aggregates data from other services that provide information on compromised equipment and prevents access to that equipment; and
- Seeks out compromised equipment and as far as possible attempts to inform owners of their problems, as well as providing links to possible solution providers, i.e. anti-virus solutions or patches for their operating system.

16.18 The safety and security of user information is maintained at all times. Users have full access to all data they supply into the system and are able to maintain or remove their information at any time. Under no circumstances is identifiable information collected or used without the full acknowledgement of the user. This means that proxy server access logs are not used as part of normal system operations at any time.[13]

16.19 There has been a lot of comment that there is no point in implementing safety measure because young people can get around them. Netbox Blue reaffirmed, however, that:

---

10 Web Management InterActive Technologies: *Submission* 96, p. 4; Mr James Collins, Managing Director, Computer Programmer/Systems Analyst, *Transcript of Evidence*, 17 March 2011, p. CS49.

11 Web Management InterActive Technologies, *Submission* 96, pp. 6-7.

12 Mr James Collins, Managing Director, Computer Programmer/Systems Analyst, Web Management InterActive Technologies, *Transcript of Evidence*, 17 March 2011, p. CS49.

13 Web Management InterActive Technologies, *Submission* 96, p. 7.

> it is important for people to realise that technology can be designed and deployed to make it incredibly difficult for kids to get around it and that that technology does exist. The public and organisations like schools need to be educated that there are solutions which can prevent the problem occurring and which, alongside adequate education, are a really critical part of the solution and that they should not give up because somebody tells them, 'Look, the kids will always get around it,' because that is just not true.[14]

16.20 Netbox Blue's Chairman also made the point that:

> There are ways of accessing content on the web that most school children know that the IT managers in the schools are blissfully unaware of.[15]

16.21 Internode added that when children can get around clever technology, they do not need it any longer.[16]

Industry advances

16.22 The Committee received a wealth of information from international and Australian companies such as Facebook, Google, Yahoo!7, ninemsn, Microsoft and Internode outlining new technological advances and importantly the accompanying cyber-safety initiatives. As there is an enormous amount of information on cyber-safety available, the lack of implementation of adequate protective measures may in part reflect the fact that users are overwhelmed.

16.23 Evidence to this Inquiry has also identified a number of areas where the cooperation of these companies could make an enormous difference to cyber-safety in Australia. While it is appreciated that these companies tend to be outside Australia's jurisdiction, most have demonstrated a willingness to assist law enforcement offices and product users.

16.24 In 2010, Telstra, Optus and Primus, agreed to introduce voluntary filtering of child abuse URLs[17] and this covers 70 percent of internet users in Australia. Work is also underway to obtain similar agreements with other

14 Mr John Pitcher, Director of Strategic Business Development, Netbox Blue, *Transcript of Evidence*, 8 July 2010, p. CS9.

15 Mr John Fison, Chairman, Netbox Blue, *Transcript of Evidence*, 17 March 2011, p. CS56.

16 Mr John Lindsay, General Manager, Regulatory and Corporate Affairs, Internode, *Transcript of Evidence*, 8 July 2010, p. CS9.

17 Ms Andree Wright, Acting General Manager, Consumer, Content and Citizen Division, Australian Communications and Media Authority, *Transcript of Evidence*, 3 March 2011, p. CS4.

ISPs. Internationally, filtering is done on a voluntary basis and Department of Broadband, Communications and the Digital Economy was not aware of mandatory filtering in any country.[18]

16.25 The Internet Industry Association referred to the Family Friendly ISP scheme which accredits ISPs that comply with best practice and under the present industry codes they are required to make filters available.[19]

16.26 Additionally, there are many free filtering options, and between 40 and 50 percent of parents/carers already use some type of filtering.[20] There are also relatively inexpensive filters available commercially.[21]

Mobile phones

16.27 My Mobile Watchdog enables parents to monitor their child's mobile phone.[22] Device Connections provided the following data based on the recent ACMA Communications Report 2007/2008 which found that:

> Australian family households with young people aged eight to 17 were generally technology rich. Most families had three or more televisions and three or more mobile phones. Almost every household had a computer, DVD player and access to the internet. Parents reported just over half of children (54%) had their own mobile phone.[23]

16.28 Device Connections reported that:

- 99 percent of girls and 80 percent of boys aged 15-17 years own mobile phones;
- 81 percent of girls and 70 percent of boys aged 12-14 years own mobiles; and

---

18 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. CS5.

19 Mr Peter Coroneos, Chief Executive Officer, The Internet Industry Association, *Transcript of Evidence*, 11 June 2010, p. CS10.

20 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.

21 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. CS12.

22 Mr Geoffrey Sondergeld, Director, Device Connections, *Transcript of Evidence*, 17 March 2011, p. CS48; Device Connections, *Submission 51*, p. 3.

23 Device Connections, *Submission 51*, p. 9.

- 22 percent of girls and 15 percent of boys aged 8-11 years own mobile phones.[24]

16.29 Further, Device Connections stated that:

- Girls spent an average of 23 minutes per day on mobiles (seven minutes talking, 14 minutes texting, one minute TV and one minute 'other'); and
- Boys spend an average of 13 minutes per day on mobiles (four minutes talking and nine minutes texting).[25]

16.30 Young people primarily used their mobiles to contact family (60 percent), and 36 percent used them primarily to contact friends.[26]

16.31 The system developed by Device Connections can also assist with law enforcement investigations, as it can produce reports that meet evidential requirements in terms of pictures, communication that has occurred, etc.[27]

16.32 Device Connections would like to see this option made available at the point of sale for all mobiles purchased on behalf of young people:

> we have had discussions with the various telecommunications carriers because we could deploy our solution and make it available for every parent for every phone; at the point of purchase they would have a potential solution.[28]

16.33 It added that:

> We would love to see coordinated engagement with the telecommunication carriers to assist in, obviously, their being able to provide a solution across the country so that every mobile phone, whether it was prepaid or post paid, a bit like, 'Do you want fries with that?'; if it is for your child, 'Would you like some form of monitoring? It is $4 or $5 or $10', or whatever the amount is. So, some coordination with the telco carriers and then, based on that, obviously there are all of the ISPs, the internet and education. That coordinated approach that Mr Fison spoke about would certainly add to this, but you cannot ignore the telco carriers and the role that they can play in providing a coordinated national

24 Device Connections, *Submission 51*, p. 9.

25 Device Connections, *Submission 51*, p. 9.

26 Device Connections, *Submission 51*, p. 10.

27 Mr Geoffrey Sondergeld, Director, Device Connections, *Transcript of Evidence*, 17 March 2011, p. CS54.

28 Mr Geoffrey Sondergeld, Director, Device Connections, *Transcript of Evidence*, 17 March 2011, p. CS60.

> response, because they are the ones providing, in a lot of instances, the data that is driving access to the various pages.[29]

16.34 There are already a number of cyber-safety initiatives released by the telecommunications companies:

> so they are fully aware that they are putting the device in the child's hand today, but at the same time they have a social responsibility to assist parents managing the misuse of those particular devices. Secondly, they would rather have the device operating in a safe way than the parent turning it off and throwing it in the cupboard, because then there is zero data being used. All of the transactions that occur, there is messaging, there is plenty of traffic.[30]

16.35 Mr James Collins added that:

> having run an ISP and been in that situation, it is a lot nicer to run an ISP which has no problems. That is what they really want to have. They do not want have faults. They do not want to have helpdesk calls. When they are fully protected you do not get as many.[31]

16.36 Yahoo!7 also call for a cyber-safety booklet to be issued with every mobile phone purchased by parents for young people so there is an opportunity to be aware of these issues.[32] Some companies already provide this.

16.37 The NSW Secondary Principals' Council suggest that:

> Perhaps parents could register a mobile phone as a 'teen phone' and then automatically get some filters attached to the phone plan that parents have the right to administer.[33]

16.38 Introducing such changes would require the cooperation of suppliers.

---

29 Mr Geoffrey Sondergeld, Director, Device Connections, *Transcript of Evidence*, 17 March 2011, p. CS60.

30 Mr Geoffrey Sondergeld, Director, Device Connections, *Transcript of Evidence*, 17 March 2011, p. CS61.

31 Mr James Collins, Managing Director, Computer Programmer/Systems Analyst, Web Management Interactive Technologies, *Transcript of Evidence*, 17 March 2011, p. CS61.

32 Ms Samantha Yorke, Legal Director, Asia Pacific Region, Yahoo!7, *Transcript of Evidence*, 21 March 2011, p. CS15.

33 NSW Secondary Principals' Council, *Submission 32*, p. 3.

Recommendation 25

That the Consultative Working Group on Cybersafety investigate possible improvements to the information provided to parents at the point of sale of computers and mobile phones.

16.39 BoysTown noted that 70 percent of calls on their help lines were from mobiles, and that this percentage is increasing.[34] Accordingly, it requested the Committee to consider:

> that negotiations occur with the telecommunication providers in relation to affordable access to crisis help lines because it was seen by that committee, after all the evidence that they sifted through, that that was one of the most effective ways that people, particularly young people, can be diverted from suicide in Australia.[35]

16.40 BoysTown emphasised the importance of mobile phones:

> our real concern here is about children and young people who are contacting us increasingly about mental health concerns, self-injury concerns and suicide not being able to access our professional counselling service because of cost issues with mobile phones. This issue really has to be addressed urgently.[36]

Recommendation 26

That the Minister for Broadband, Communications and the Digital Economy negotiate with mobile phone companies to increase affordable access to crisis help lines, with a view to ensuring greater accessibility by young people seeking assistance.

34 Ms Tracy Adams, Chief Executive Officer, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS11.

35 Mr John Dalgleish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS11.

36 Mr John Dalgleish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS12.

Young people and technology

16.41 Professor Karen Vered emphasised the need to consider 'what young people are doing with the media and technology and not what the media and technology are doing to them.[37] Similar, Mr Craig Scroggie commented,

> Whilst technology plays a role in protecting against some of these things, it is important to remember what technology does not do. It does not stop a child from posting personal information on their social networking account. It cannot prevent a child from connecting to a PC that does not have parental restrictions at an internet cafe. It cannot stop a child innocently accepting a sexual predator posing as another teenager, as a friend, on Facebook. It cannot stop a memorial site being desecrated. Technology cannot do these things.[38]

16.42 Netbox Blue advised that technological solutions encompassing everything for a school of 750 students and 100 teachers would cost 6.4 cents per day per user.[39] For a parent license to monitor five mobile phones, the cost would be $14.95 per month.[40] Implementation of the Australian Protective Network costs 0.4 cents per day.[41] The cost of these protections is not prohibitive.

16.43 Further, most companies producing technological solutions already have educational resources about cyber-safety for young people and parents/carers.

37 Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, p. CS36.

38 Mr Craig Scroggie, Vice President and Managing Director, Asia Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, p. CS12.

39 Mr John Fison, Chairman, Netbox Blue, *Transcript of Evidence*, 17 March 2011, p. CS51.

40 Mr Geoffrey Sondergeld, Director, Device Connections, *Transcript of Evidence*, 17 March 2011, p. CS51.

41 Mr James Collins, Managing Director, Computer Programmer/Systems Analyst, Web Management Interactive Technologies Pty Ltd, *Transcript of Evidence*, 17 March 2011, p. CS52.