2

Young people in the online environment

2.1   This chapter describes how the online environment impacts on young people in Australia. This will include entry to that environment, and the roles of schools and public libraries within it. It lists the various stakeholders who are able to have an impact on the online engagement of children and young people less than 18 years of age.

2.2   Most young people in Australia have regular access to this environment, and it plays an important role in their education, social connections and recreation.

2.3   Consulting with young Australians was a key priority for the Committee. It developed specific opportunities to capture the views of young Australians – a group that is otherwise unlikely to make formal submissions to a Parliamentary inquiry. Consultations included an online survey, a primary school visit and a high school forum. Interestingly, as a direct result of the survey and its school visits, the Committee began to receive submissions from young Australians.

Stakeholders

2.4   Children/young people are 'the key stakeholders' in their engagement with the online environment. Their contribution is 'absolutely critical' in the development of greater safety provisions because adults have as much to learn from young people as they need to learn.[1]

---

1   Ms Lauren Oliver, Internal Consultant, Youth Empowerment and Participation, Berry Street, *Transcript of Evidence*, 9 December 2010, p. CS5; Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, pp. CS34-35.

2.5   Apart from the community itself, other important Australian stakeholders controlling or able to influence engagement in that environment include:

- parents/carers;

- Commonwealth, State and Territory Government agencies, particularly those with regulatory roles;

- schools and teachers;

- Internet service providers;

- content providers;

- public libraries;

- researchers; and

- traders.

2.6   These stakeholders have opportunities to assist young people to learn to behave appropriately online. Parents/carers, families and the broader community need to be engaged in regular support to assist young Australians to protect themselves and be safe online, as well as to develop responsible behaviour. The Australian Council for Educational Research believed that this will require community support programs for parents/carers and students in a range of locations, as well as regular dialogues about suitable strategies for online protection and responsible behaviour.[2]

2.7   All stakeholders, including young people themselves, have important roles ensuring that cyber-safety in the online environment is a reality rather than an empty concept. Many participants in this Inquiry emphasised the importance of the inclusion of young people in discussions about such things as filtering online content, if only because some of them would be able to find a way around any technology that was introduced.[3] Supervised computer access and filtering technology can reduce the risks for young people but, as children become more 'tech savvy', blocking and monitoring strategies are less effective.[4]

---

2   Australian Council for Educational Research, *Submission 20*, p. 8.

3   See, for example: Centre for Children and Young People, *Submission 31*, pp. 1-3; Australian Communications and Media Authority, *Submission 80*, p. 6; Consultative Working Group on Cybersafety, *Submission 113*, p. 15; Mr Craig Scroggie, Vice President and Managing Director, Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, p. CS34; Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS18.

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

> Children don't use online technologies as technologies, they use them as enablers for social and cultural interaction.[5]

2.8 'Children' or 'young people' are not homogenous groups in terms of their online capabilities, and an American researcher has divided them into the following categories:

- Those who are savvy, with the knowledge and skills to make good decisions about their online behaviour and know when to stop and withdraw;

- Those who are naïve with some skills, needing to be educated and 'topped up'; and

- Those who are vulnerable, having trouble at school or home, or both. When teenage angst comes into play and they disengage momentarily, they become vulnerable if they look for communities online with whom to engage. Young people with mental health problems, who are the most vulnerable, seek to belong online but lack the skills to disengage when they encounter inappropriate behaviour.[6]

2.9 Research on social networking by the Australian Communications and Media Authority (ACMA) clearly indicates that a greater number of young people are moving to the savvy category by, for example, not disclosing names or passwords and adopting safer practices.[7]

2.10 While Facebook has a minimum joining age of 13 years, concerns were expressed about the effectiveness of age verification mechanisms, for example, how such limits can be enforced on nine year old children who are 'tech-savvy'. The South Australian Office for Youth noted that its 2010 survey identified quite a number of children, particularly some only ten and 11 years old, changing their dates of birth so that they could join Facebook.[8]

---

5   Mr Mark Newton, *Submission 15*, p. 4.

6   Dr Barbara Spears, Senior Lecturer, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS32.

7   Dr Barbara Spears, Senior Lecturer, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS32.

8   Superintendent Bradley Shallies, National Coordinator, Child Protection Operations, Australian Federal Police, *Transcript of Evidence*, 11 June 2010, p. CS17; Mrs Tiffany Downing, Director, South Australian Office for Youth, *Transcript of Evidence*, 3 February 2011, p. CS20.

2.11   The Internet Industry Association pointed out that there are practical problems with age verification for some under the age of 18 years.[9]

> One of the challenges ... is that there are not really mechanisms in most Western societies to verify whether you are a kid; they are all geared towards verifying that you are an adult, whether with a driver's licence or something else. So we do things like 'age gating', so that if you put in the wrong age once, a cookie on your machine will block you. We also, through algorithms, try to detect patterns of speech and things that look like you are not likely to be over 13, and we remove people. We also take complaints from teachers or other people in the network that you are involved in if you do not belong there, and we remove people. I think the last statistic I heard is that Facebook removes 20,000 people a day, or people who are underage.[10]

2.12   Berry Street reported that for vulnerable young people:

> Probably in line with the behaviour of their 'mainstream' peers, over 76% of respondents to date have indicated that they have lied about their age online and just under 70% have chatted with people they don't know face-to-face. We found that 46% had been bullied via mobile phone or the internet, and 38.5% had bullied others in this way. Hacking and cracking into the social networking sites of other people also figured relatively highly on the list of risky behaviours.[11]

Real and virtual worlds

2.13   Unlike their parents/carers, most young people use technology 'holistically': communicating, learning, socialising, playing, researching, and doing homework, so that their online lives blend seamlessly with their offline lives. There are some young people who do not have a clear demarcation between the online (virtual) world and the offline (real) world. For them, the two worlds exist symbiotically.[12]

---

9   Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association, *Transcript of Evidence*, 11 June 2010, p. CS18.

10   Hon Mozelle Thompson, Advisory Board and Policy Adviser, Facebook, *Transcript of Evidence*, 21 March 2011, p. CS5

11   Berry Street, *Submission 95*, p. 11.

12   Alannah and Madeline Foundation, *Submission 22*, p. 8; Australian Federal Police, *Submission 64*, p. 3.

2.14   They grew up in the online environment as 'digital natives' or 'online natives', rather than as the 'digital immigrants' of older generations. For such young people, the terms 'online' and 'offline' are differentiated only by other generations and where they straddle both worlds. Their involvement with that environment is an essential means to and part of their interactions with other people. In many cases, it seems that their parents/carers are unable to assist because they are busy, or not very interested in or knowledgeable about 'technology'.[13]

2.15   In some circumstances, young people who are not able or willing to differentiate between the two worlds can be at even greater risk of harm in the online environment than their peers who are able to absorb warnings about safety and risks. Threats to cyber-safety now extend well beyond school gates to any Wi-Fi connected or home network.[14] These treats can be significant because of the rapid rate of emerging new technologies.

2.16   Therefore, as part of their approach in the online environment young people need to exercise reasonable care and responsibility online. The key components of the necessary holistic response to cyber-safety should be based on 'education, law enforcement, international cooperation, appropriate products and parental supervision'. A smart, ethical and socially aware online experience requires individuals to adopt responsible online behaviour and, to achieve this, it was suggested that effective education programs are needed.[15]

Entry to the online environment

2.17   Until recently, many adults were not familiar with the online environment. Now, however, 61 percent of mothers aged 45 to 65 have a Facebook page and Dr Helen McGrath also argued that parents and older adults are 'a lot more savvy' than most people believe.[16] Many still use it in very functional ways: to pay bills, to search for information or to

---

13   See Australian University Cyberbullying Research Alliance, *Submission 62*, p. 8; Ms Georgie Ferrari, Chief Executive Officer, Youth Affairs Council of Victoria, *Transcript of Evidence*, 11 June 2010, p. CS27; Interactive Games & Entertainment Association, *Submission 110*, p. 3.

14   Mr John Pitcher, Director of Strategic Business Development, Netbox Blue, *Transcript of Evidence*, 8 July 2010, p. CS3.

15   Telstra Corporation, *Submission 14*, p. 3; Mr Darren Kane, Corporate Security and Investigations and Officer of Internet Trust and Safety, Telstra Corporation, *Transcript of Evidence*, 8 July 2010, p. CS3.

16   Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS61.

communicate with other people, etc. Teachers use it for these and a wider range of purposes, including as a teaching tool and to build cognitive skills in students.[17]

2.18   However, young people use the online environment in different ways and for different reasons, depending on their age, particular circumstances and interests:

- Pre-school children begin to learn how computers work. Their online activity may include visiting children's websites and communicating with family and friends through email;

- Primary school children feel more confident using other applications such as chat rooms. Some may search for prohibited material; and

- For high school children, the Internet is a necessity to assist with research for projects and homework. This age group seeks more freedom and independence in their use of the Internet, and they increasingly use the online environment as a social tool. These young people may also want to explore prohibited material.[18]

2.19   Research published by ACMA in 2007 indicated that 'first-use' of the Internet is at about five years old, but stated that there was anecdotal evidence suggesting that many children go online at progressively younger ages. Just under half of families are regularly involved with the Internet access of those six to ten years old. Earliest learning about the online environment can be through recreational activity, such as visiting the website associated with a favourite TV show.[19] Cyber-safety education in schools usually does not begin until Year 2.[20] Professor Karen Vered added that:

> Of course, it seems sensible that schools introduce cybersafety
> when they introduce computers and online access. Unfortunately,
> it is just too late, because children have already developed a set of
> habits and practices. They are not necessarily bad ones, but it
> would be nice if we could devolve that education to an earlier

17   Alannah and Madeline Foundation, *Submission 22*, p. 8.

18   BraveHearts, *Submission 34*, pp. 2-3.

19   Australian Communications and Media Authority, *Submission 80*, p. 3; Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, p. CS36. See also Australian Council on Children and the Media: *Submission 75*, pp. 12-13: Ms Lesley-Anne Ey, Executive Committee Member, *Transcript of Evidence*, 3 February 2011, p. CS50; BoysTown, *Submission 29*, p. 5.

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

starting point, bring it into preschools, bring it into kindies and bring it into leisure environments especially, since schools also prohibit the type of websites and media engagements in which children first acquire their skills. At school, you are really not going to be given time to go play with Club Penguin. School does not have time for that. The most fortunate children are going to be those who have had those peer groups and have played with siblings, extended family et cetera and have enhanced that peer learning.[21]

Recommendation 1

That the Minister for School Education, Early Childhood and Youth consider the feasibility of assisting preschools and kindergartens to provide cyber-safety educational programs for children as part of their development activities.

2.20 The Alannah and Madeline Foundation noted that entry to the general online environment had changed considerably in the past few years. There are now approximately 2.2 million Australian children actively engaging online.[22] Although ages do vary, it was suggested that Year 5 (ten or eleven years old) is the most common entry point into the social networking environment.[23]

2.21 After very young children are introduced to computers, the use of mobile phones and other wireless devices follows. Once in this environment, there are many other places where access is available, including schools, public libraries, homes of friends, etc. Some will be unsupervised.[24]

2.22 ACMA's research *Click and Connect: Young Australians' use of online social media* (2009) found that as children age they spend more time online:

- Children eight to nine years old use the Internet for an average of one hour, six minutes every two days;
- Young people 16 to 17 years old average three hours, 30 minutes on the Internet every day;

---

21 Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, pp. CS36-37.
22 Alannah and Madeline Foundation, *Submission 22*, p. 7.
23 Association of Independent Schools of SA, *Submission 19*, p. 8.
24 Childnet International, *Submission 18*, p. 1.

- Younger children are more interested in individual activities online, such as playing games; 83 percent of eight to 11 years old reported online gaming as the most popular use of the Internet; and

- By comparison, young people aged 12 to 17 use the Internet mainly for social interaction—81 percent of 12 to 17 years old nominated social networking services as their main reason for going online.[25]

2.23   This research demonstrated a high level of use of social networking services:

- Young people, aged 12 to 17, have a very high level of use of social networking services. Approximately 97 percent of 16 to 17 years old surveyed reported using at least one of these services, compared to 51 percent of children aged eight to 11 years.

- Fifty four percent of those 12 to 17 years old claim that 'chatting to friends from school' is their main reason for using social networking services. A survey conducted by the Australian Bureau of Statistics, *Children's Participation* (2009), indicated that younger children used the phone primarily to contact family rather than friends.

- By comparison, only 17 percent of those 12 to 17 years old claim to use the Internet to 'make new friends'. [26]

The most popular on-line activities for children between the ages of 5 and 14 years include educational activities (85%), on-line gaming (69%) and listening or downloading music (47%). Using the Internet for social interaction were also popular activities: e-mailing (36%), accessing chat rooms or instant messaging (32%) and utilising social networking sites (22%).[27]

2.24   *Click and Connect* also demonstrated that children and young people have a high awareness of cyber-safety risks, and identify activities such as 'posting personal information' as high risk behaviour. Despite this, some young people deliberately engage in risky behaviours, and the tendency to do this rises with age. Of those aged 16 to 17 years:

- Sixty-one percent report accepting 'friend requests' from people they do not know offline.

- Seventy-eight percent claim to have personal information, such as a photograph of themselves, on their social networking profile pages, compared to 48 percent of eight to nine year olds.

25   Australian Communications and Media Authority, *Submission 80*, pp. 3-4.

26   Australian Communications and Media Authority, *Submission 80*, p. 4.

27   BraveHearts, *Submission 34*, p. 3, citing the Australian Bureau of Statistics (2009).

- Seventeen percent of those 12 to 17 years old claim that one of their top three reasons for using social networking services is to 'make new friends'.

- Conversely, use of privacy settings on profile pages appears to be greater amongst the older age groups.[28]

2.25   The Australian Youth Affairs Coalition provided the following data:

> Young people use the Internet for an average of one hour and 17 minutes each day which includes:
>
> - Almost 50 minutes of using the internet for messaging, visiting social websites and emailing,
>
> - 15 minutes for games online against other players, and
>
> - 13 minutes for homework on the computer and/or Internet.[29]

2.26   Young people access the online environment by a variety of means, and therefore adequate frameworks must be in place to protect them from on-line threats as much as possible. Some of these places may not have the same level of controls as those at home or school. In particular, rules and supervision at friend's homes may be different to those in place at the child's own home.[30] Also in places such as Internet cafes or bookstores, restrictions to online access by young people may be vague or not enforced.

2.27   Government regulators have a role in providing information and programs about online risks. It seems that few young people or parents/carers go to the appropriate websites, so that they are often ignorant about both the risks and ways of avoiding them.[31]

2.28   While there is a great deal of material available about cyber-safety, many parents/carers are often not able to discern what is most valuable or useful. In addition, those who are likely not to engage with schools are likely to be the ones whose children are having problems with cyber-safety. For differing reasons, therefore, parents may not be able to attend sessions on cyber-safety when schools arrange them.[32]

---

28   Australian Communications and Media Authority, *Submission 80*, p. 4.

29   Australian Youth Affairs Coalition, *Submission 28*, p. 8, citing McGrath H (2009) *Young People and Technology: A review of current literature* (2nd Edition), published by the Alannah and Madeline Foundation.

30   BraveHearts, *Submission 34*, p. 5.

31   Hon Mozelle Thompson, Chief Policy Adviser, Facebook, *Transcript of Evidence*, 11 June 2010, pp. CS36-37.

32   Ms Kate Lyttle, Secretary, Australian Parents' Council, *Transcript of Evidence*, 30 June 2010, p. CS17; Mr John Pitcher, Director Of Strategic Business Development, Netbox Blue, *Transcript of Evidence*, 8 July 2010, p. CS26-27; Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS62.

2.29   It was suggested that one way to give parents/carers more intensive opportunities to become aware of these issues was to have their children make the presentations, thus providing the chance for a 'double learning' process.[33]

Disadvantaged young people

2.30   Some young people do not have access to computers in their home, or their access is severely limited. In addition, there are at least four specific groups whose access to the online environment is less than that of the great majority of their age groups. Lack of effective access makes it difficult for such children and adolescents to participate in the activities and social networking that are important to them, and undermines their ability to develop the skills they will need. Effective access is required if they are to develop into responsible, safe and resilient users of the online environment.[34]

2.31   Assistance to such children is vital so that all young people can have the same opportunities online as their peers. There is little if any research about the numbers of young people who are disadvantaged, or degrees of disadvantage, in this environment. It is not clear how 'effective access' should be defined, or how such young people could be supported. It is therefore difficult to prescribe and implement effective plans to correct this situation.[35]

2.32   The Victorian Child Safety Commission referred to effective access to include support for the child while using the technology enabling them to develop the skills to be responsible and resilient users of the technology:

> Lack of effective access to ICT makes it more difficult for children to participate in the activities and social networks that are important to children today and undermines their ability to develop the skills they require when they leave care.[36]

2.33   It is clear, however, that those young people who engage in risky behaviour online often also engaged in risky offline behaviour. There is a pressing need for more research into the cyber-safety needs of the most

33   Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS66.
34   Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 2.
35   Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 1.
36   Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 2.

vulnerable members of our society, including those with mental health problems.[37]

2.34 Young people affected by abuse and trauma may not know what 'safe' looks like, let alone how to make themselves safe. Berry Street thought that supporting such adolescents to develop protective behaviours is 'a huge priority'. Such behaviours should be incorporated into their daily lives, but translating these messages into the online environment presents additional challenges.[38]

> Most [existing programs] tend to be targeted at mainstream audiences, taking what I would call an almost safe harbour approach. This potentially leaves the more vulnerable children at heightened risk and may explain why some children unwittingly expose themselves to significant risk in the face of numerous safety programs and extensive messaging. It may therefore be a fundamental although well-founded error to approach cybersafety in isolation without considering the wider spectrum of behavioural issues confronting society. Cybersafety, in closing, must have synergies with other prevention and policing strategies.[39]

2.35 The Victorian Office of the Child Safety Commissioner requested that consideration be given to children in care:

> in the United Kingdom the Home Access program and other initiatives have sought to ensure that 'Looked After Children' are provided with accesss to computers and the internet.[40]

2.36 Some of the young people in care may be subject to rulings that they are not to have contact with their families. Through social networking sites, they are sometimes approached, or remain in touch, when they should not be. In such situations, teaching protective behaviour is complex.[41]

---

37 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, pp. CS5-6, CS19; Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June, 2010, p. CS15; Associate Professor Sheryl Hemphill, Senior Research Fellow, Murdoch Children's Research Institute, *Transcript of Evidence*, 9 December 2010, p. CS27.

38 Ms Sherree Limbrick, Director, Statewide Programs, Berry Street, *Transcript of Evidence*, 9 December 2010, pp. 4-5.

39 Superintendent Bradley Shallies, National Coordinator Child Protection Operations, Australian Federal Police, *Transcript of Evidence*, 11 June 2010, p. CS8.

40 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 2.

41 Ms Lauren Oliver, Internal Consultant, Youth Empowerment and Participation, Berry Street, *Transcript of Evidence*, 9 December 2010, p. CS6.

2.37   Many of those responsible for young people in care have low levels of
        skills and 'extremely low' knowledge of technology, its uses and
        opportunities. Considerable work has therefore been done by Berry Street
        to build competence and confidence in those who already carry out
        complex jobs in looking after young people in care.[42]

2.38   Vulnerable children are often unwittingly at heightened risk in spite of
        safety programs and extensive messages about unwise behaviour on the
        basis that most programs are targeted at mainstream audiences. It may
        therefore be a fundamental, though well-founded, error to approach
        cyber-safety without considering the wider spectrum of behavioural issues
        confronting our society. The Victorian Office of the Child Safety
        Commissioner commented that current cyber-safety strategies had not yet
        addressed the issue of keeping either group safe online.[43]

2.39   There is 'relatively limited understanding' about the use of the online
        environment by disadvantaged young people, and growing concern that
        disparities in access, quality and skills would reinforce existing disparities
        in health and social outcomes. Of course, for some disadvantaged groups,
        the Internet has enabled freedom of expression and engagement where
        face-to-face contact is often difficult. This highlights the potential for new
        online technologies to create new processes of social inclusion.[44]

Vulnerable young people

2.40   The Victorian Office of the Child Safety Commissioner drew attention to
        two groups of about 5,000 'vulnerable' children in Victoria:

- those who are in out-of-home care, removed from their parents
  because of abuse or neglect. The factors that make such children
  more vulnerable to abuse in the 'real' world also make them more
  vulnerable in the 'virtual' world. The level and type of their access to
  this environment can vary; and

- those who have been identified as 'high risk' because of such factors
  as low satisfaction with their lives, sexual or physical abuse, poor
  family relationships or parental conflict. Some are living on the

---

42 Ms Sherree Limbrick, Director, Statewide Programs, Berry Street, *Transcript of Evidence*,
    9 December 2010, p. CS5.

43 Australian Federal Police, *Submission 64*, p. 4; Superintendent Bradley Shallies, National
    Coordinator, Child Protection Operations, *Transcript of Evidence*, 11 June 2010, p. CS8.
    Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 3-4; Mr Bernard Geary,
    Child Safety Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS76.

44 Australian Psychological Society, *Submission 90*, p. 7.

streets, some are already socially excluded. They may live in dysfunctional families, with parents who have changing live-in partners. Both online and offline, such young people are at risk of becoming either victim or perpetrator of abusive behaviour.[45]

Young people with disabilities

2.41   The Australian Communications Consumer Action Network noted that the 20 percent of Australians with a disability had particular circumstances requiring specialised tools and support to access the online environment. Such support was vital for disabled young people.[46]

2.42   After a roundtable convened in June 2010 to discuss online issues effecting those with disabilities, the Network summarised its concerns:

- vulnerability;

- barriers to confidence;

- gaps in awareness, and

- improved accessibility to websites.[47]

Young Indigenous people in remote communities

2.43   If a reliable assessment could be made, it is likely that some of those living in remote Indigenous communities would be the most disadvantaged children in Australia in terms of their access to the online environment.

Young people in regional areas

2.44   Many Australian children live in regional or remote areas where, for example, Internet or mobile phone connections are non-existent or limited. They are disadvantaged by comparison with those who live in larger

---

45   Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 2; Consultative Working Group on Cybersafety, *Submission 113*, p. 13; Mr Bernard Geary, Child Safety Commissioner, Victorian Office of the Child Safety Commissioner, *Transcript of Evidence*, 9 December 2010, pp. CS70, 76; Mr Richard Egan, National Policy Officer, Family Voice Australia, *Transcript of Evidence*, 9 December 2010, p. CS54; Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, p. CS37, 42.

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

47   Australian Communications Consumer Action Network, available at: http://www.accan.org.au/news_item_full.php?id=99, accessed 20 January 2011.

centres and, in particular, may not have any experience with cyber-bullying.[48]

Privacy

2.45   Little is known about the attitudes of Australian young people to privacy. A recent American report suggested that children can see some online interactions as private, and were concerned about their parents/carers breaching that privacy.[49] Similar feedback was given during the Committee's High School Forum in Hobart.

2.46   Young people may have a limited capacity to assess the implications of divulging their own information, and therefore rely on others to ensure that their interests and safety are protected. The online environment is an area where they can be at risk, so that a breach of their privacy can be substantial, including trauma and identity theft.

2.47   The *Privacy Act 1988* (Cth) does not make special reference to young people, on the basis that they have the same rights to privacy as adults. In practice, primary care-givers would usually be responsible for exercising their rights under the Act until individuals reached levels of maturity and understanding to make independent decisions.[50]

2.48   The complexity of the issue is highlighted by the argument that children and young people sometimes require protection from themselves.[51]

2.49   Privacy will be examined in more detail in Chapter 5, as part of the consideration of the threats to cyber-safety.

Schools

2.50   Specific cyber-safety programs and measures in some of the States and Territories are outlined in Chapter 14.

2.51   Schools are optimally placed to support students to be cyber-safe. Raising the awareness of young people before, or as, computers are introduced

---

48   Queensland Council of Parents and Citizens' Associations, *Submission 99*, pp. 1-2.

49   Office of the Privacy Commissioner, *Submission 92*, p. 5; Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 4-5.

50   Office of the Privacy Commissioner, *Submission 92*, p. 4.

51   FamilyVoice Australia, *Submission 50*, p. 2.

into the curriculum can be a preventative step – ensuring young people are better equipped against the risks they are likely to encounter online.[52]

2.52 Many schools have in place policies and filters provided by the local education authority. Schools with effective behaviour management systems, and vigilant supervision of student use of computers provide additional layers of support and protection. In many schools however, policies are not consistently followed by teachers, or are not widely known or understood by teachers, students or parents/carers.[53]

2.53 The Alannah and Madeline Foundation suggested that Australian schools had 'much ground' to make up in producing 'robust, acceptable' policies reaching beyond their gates to include parents and the wider community.[54]

2.54 The Australian Government's provision of laptops for every student in Years 9 to 12 is intended to give unprecedented access, creating borderless classrooms and blurring boundaries between school and home.[55] The Government's National Secondary School Computer Fund is helping schools to provide new computers and ensure that all students in these grades have access to facilities.

Libraries

2.55 The Australian Library and Information Association noted that libraries, especially school and public libraries, are key access points for the Internet for Australian children. They are an integrated, connected and collaborative network, and are therefore able to impact young people's engagement online. The responsibilities of libraries to provide safe environments are taken very seriously, to the extent that user behaviour policies and other measures have been developed to increase online safety.[56]

2.56 *The ALIA Internet access in public libraries survey 2008* found that there are separate internet terminals for use by children at 33 percent of responding

---

52 Association of Children's Welfare Agencies, *Submission 35*, p. 3.
53 Alannah and Madeline Foundation, *Submission 22*, p. 8.
54 Alannah and Madeline Foundation, *Submission 22*, p. 8.
55 Alannah and Madeline Foundation, *Submission 22*, pp. 7-8.
56 Australian Library and Information Association, *Submission 16*, pp. 5- 6; Mrs Sue Hutley, Executive Director, Australian Library and Information Association, representing the Safer Internet Group, *Transcript of Evidence*, 8 July 2010, p. CS28.

libraries.[57] Further parental consent was required for children to use the internet by 77 percent of library respondents with variations dependent on age and almost a third of responding library services required parents to be present with children using the internet.[58]

School libraries

2.57   Outside classrooms, school libraries are the main location for the delivery of messages about the online environment. Library staffs are familiar with Internet-use policy and procedures at their schools, and with current information and research about safe online practices.

2.58   Teacher librarians are valuable and crucial partners in delivering important messages about these practices through teaching and learning programs. These focus specifically on digital information literacy development, including being literate across multiple areas within the ever-changing online environment.[59]

2.59   These libraries are places of learning and discovery; safe and secure spaces for students that have Internet access. They have constant adult supervision and are only open when there is supervision. Further, school libraries play an important role in teaching students about

- Searching for, selection, analysis and creation of, material;

- How to develop responsible cyber-safety behaviour;

- Becoming aware of ethical practice;

- The impact of their digital footprints; and

- Good cyber behaviour habits for use after their formal learning finishes.[60]

2.60   Teacher librarians are in central positions because they touch the lives of everyone in those school communities. They are therefore well-placed to support and deliver digital information literacy across all curriculum areas and age groups, including parents/carers.

---

57   Australian Library and Information Association, *Submission 16, p. 5.*
58   Australian Library and Information Association, *Submission 16, p. 6.*
59   Australian Library and Information Association, *Submission 16*, p. 6.
60   Unless specified otherwise, material in the rest of this section was drawn from Australian School Library Association, *Submission 72* and *Transcript of Evidence*, 17 March 2011, pp. CS32-38.

2.61   While technology has changed them, libraries can also be sanctuaries: for some students, the safest places in their schools.

2.62   The Australian School Library Association believed that digital information literacy, of which cyber-safety is an integral part, is not being taught because of lack of training and professional development in either pre- or in-service professional training.

2.63   Being a responsible digital citizen requires appropriate, responsive behaviour with regard to the use of technology. A digital information literacy program in a school setting would focus on the following:

- Etiquette;

- Effective communication;

- Information literacy taught in the content of teaching and learning programs;

- Equity of access and participation;

- Social responsibility and ethical behaviour;

- Collaboration and creativity in a safe environment;

- Safe practices (e-safety and health safety);

- Critical thinking and evaluation; and

- Cultural and social awareness of the information environment.

2.64   The Australian School Library Association believed that the potential of teacher librarians to contribute to better outcomes for students within safe learning environments is untapped. As these personnel support all levels within a school, they are well-placed to integrate cyber-safety into digital information literacy programs and to provide professional learning for all of its teachers.

2.65   As a result of Building the Education Revolution, more than 3,000 new libraries have been built in primary schools. Most have been designed so that there is a movement away from the 'traditional' library environment. In many of them, there are trolleys allowing Netbooks to be moved around the library and connect to a wireless network, or plugged in to a direct connection. Such spaces are learning and information environments where students can use tools provided by the school or ones that they bring from their homes.

2.66   Where there are 'Acceptable Use' policies at schools, both students and their parents/carers are required to sign acknowledgement agreements.

These indicate that students must abide by the school's Internet access policies, and that they have rights and responsibilities. These policies ensure that students are aware of consequences if they break the access rules. These can vary but, if the school is practising other social skills programs, they have to be part of the overall education process.

2.67   The Australian School Library Association believed that teacher librarians are often not considered to be part of the general classroom program. Their role is often overlooked and they are engaged in a range of miscellaneous tasks, their professional development often neglected so that it must be pursued at their own expense.

Public libraries

2.68   There is a network of over 1,500 public libraries in Australia and they are community hubs, the hearts of their communities. This network is the key provider of safe and free access to information and services. These libraries are recognised as trusted, neutral and non-threatening spaces for individual or group social inclusion.[61]

2.69   While cyber-safety training is already being delivered at libraries around the country, for seniors as well as young people, the Australian Library and Information Association noted the need for more support to provide more training for staff in the use of the Internet and cyber-safety.[62]

2.70   Since 2002, public libraries have continued to develop and improve Internet services for children. A survey in 2008 showed there were separate terminals for use by children at 33 percent of responding libraries, compared with 20 percent in 2005 and 16 percent in 2002. Websites linked to material especially recommended for young people increased to 56 percent (up from 52 and 47 percent respectively).[63]

2.71   Parental consent is required for children to use the Internet by 77 percent of respondents, an 8 percent increase since 2005. While more than half the responding libraries require this consent to the age of 18, the youngest age where it is not required was eight years. Almost a third of responding libraries required parents to be present when children used the Internet, although the age to which this was required varied widely.

---

61   Australian Library and Information Association, *Submission 16*, pp. 2, 5; Mrs Sue Hutley, Executive Director, Australian Library and Information Association, representing the Safer Internet Group, *Transcript of Evidence*, 8 July 2010, p. CS28.

62   Mrs Sue Hutley, Executive Director, Australian Library and Information Association, representing the Safer Internet Group, *Transcript of Evidence*, 8 July 2010, pp. CS28-29.

63   Australian Library and Information Association, *Submission 16*, p. 5.

2.72 Access to the Internet for young people in libraries appeared to be closely linked to the values of individual communities. Requirements for parental consent varied within jurisdictions and metropolitan libraries, except for Tasmania where one regulation covered the state.[64]

Public libraries in NSW

2.73 Public libraries across NSW provide free Internet access for the community. They form a critical element in community development, supporting life-long learning, literacy and education.

2.74 The *Library Act 1939* (NSW) guarantees everyone in the community access to libraries. All have conditions of use relating to public Internet access, and conditions of vary between local authorities. It is common for parents/carers to be required to give permission for children to use the Internet. The State Library provides free access, including by wireless, for laptops or PDAs. It recognised the privacy of users and did not monitor the information or sites accessed.

2.75 While young people are not formally supervised in NSW public libraries, there are guidelines for use of the online environment within them. The responsibility to supervise their young people remained at all times with parents/carers.[65]

Public libraries in the ACT

2.76 Libraries ACT, formerly the ACT Library and Information Service, forms part of the network of public libraries in Australia.[66]

2.77 The ACT Government provides free Internet access in its libraries, promoting community access to information. Community use is high, and a project has begun to provide wireless facilities in addition to desktop computers.

2.78 Users are required to accept an access policy before they use terminals, and an Internet blocking facility has been installed preventing access to sites identified in the Australian Communications and Media Authority's blacklist. Computers are in areas where there is a balance between privacy and supervision.

---

64 Australian Library and Information Association, *Submission 16*, p. 6.

65 NSW Government, *Submission 94*, p. 45.

66 Material in this section was drawn from ACT Government, *Submission 82*

2.79   Libraries ACT recognises the role of parents/carers in supervising young people in libraries generally, and for online access generally. Staff uphold policies on appropriate use and educate all users, specifically parents/carers, on cyber-safety measures that they can adopt. When children become library members, their parents/carers sign a declaration that they understand and uphold ACT Library and Information Service's policies.

Consultation with young people

2.80   Sociologists have described young people as 'having been born into an age where they are unable to rely on anything, yet have incorporated this uncertainty into their lives [and exude] optimism and a sense of confidence.'[67] The optimism and confidence of young Australians in exploring, utilising and navigating new technologies is often over-looked.

2.81   As recent research confirms, young people are the most valuable resource in the development of cyber-safety awareness programs.[68] It is therefore vital that young people's perspectives are incorporated into the cyber-safety debate in ways that empower them and develop meaningful policies and programs.

Youth Advisory Group

2.82   The Youth Advisory Group was formed in 2009. It provides a forum where young people can talk directly to the Government about cyber-safety. [69]

2.83   In its first year, it consisted of 304 secondary students from 15 schools across the country and provided advice on cyber-safety issues such as cyber-bullying, mobile phone safety, privacy and online computer games. This advice lead to the announcement of two important initiatives: the Cybersafety Help Button and the Teachers' and Parents' Advisory Group on Cybersafety.

---

67 Dr Hilary Yerbury, 2010, 'Who to be? Generations X and Y in civil society online', in *Youth Studies Australia,* 29(2): 25-32.

68 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cyber-safety, A Living Lab: Research Report*, Cooperative Research Centre for Young People, Technology and Wellbeing.

69 Unless specified otherwise, material in this section was drawn from Consultative Working Group on Cybersafety, *Submission 113*, pp. 34-35.

2.84   The expansion of ACMA's cyber-safety education, awareness-raising and counselling services was also informed by feedback from the Youth Advisory Group. The Authority's *Cybersmart* website and online helpline implemented a number of features consistent with initial advice from the Youth Advisory Group.

2.85   In 2010, the Youth Advisory Group was expanded to include 500 primary and secondary students aged from eight to 17 years, from 30 schools nationally. It provided advice through the *y@gonline* site and at face-to-face meetings, dealing with five main areas of concern: cyber-bullying, socialising online, scams and fraud, online games and digital citizenship.[70]

2.86   A Consultative Working Group on Cybersafety and Youth Advisory Group summit was held in June 2010, where its members, parents and teachers provided views on a range of Government cyber-safety programs and initiatives. These included the Cybersafety Help Button and the Teachers' and Parents' Advisory Group, the *budd:e* cyber-security educational modules and the *ThinkuKnow* program administered by the Australian Federal Police.

2.87   A slightly different format will be used for the Youth Advisory Group in 2011. Ten one week consultation spheres are proposed, representing State/Territories, metropolitan and regional areas, Indigenous communities and National Broadband Network rollout sites. The Consultative Working Group is particularly interested to talk to schools near these rollout sites, to see how their students view the Network.[71]

2.88   Each sphere will include 100 to 200 primary or secondary students from between ten and 20 schools in a designated area or community. In total, there will be about 1,300 Youth Advisory Group members from about 130 schools.[72]

2.89   The Youth Advisory Group has commented on the array of social networking sites and games, and the associated features and conditions. Before they can join a site or play a game, young people are confronted by long and detailed, usually legalistic material on the terms and conditions

70   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. CS22.
71   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. CS22.
72   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. CS22.

of participation. More often than not, they scroll to the bottom and click their agreement without reading it, as they are looking for an easy way to understand the key features of these sites and games. As a feature of the Cybersafety Help Button, the Consultative Working Group on Cybersafety is looking to make it possible for anyone interested to find out about the features of sites and games, and what they need to understand about them.[73]

2.90   The Consultative Working Group on Cybersafety has taken very seriously advice that the Youth Advisory Group has given. It considered that this Group would be critical to further development of cyber-safety policy, and acknowledged that it will be essential that all stakeholders be responsive in considering the Group's advice.[74]

2.91   One of the Working Group's members stated that involvement with the Youth Advisory Group had brought 'enormously valuable feedback'. There was a continuing need to analyse what adolescents actually said to each other on the Internet so that inappropriate behaviour could be detected.[75]

Committee's consultations

> Cyber safety, as you very well know, is a big thing! it isnt to be taken lightly, not anymore anyway... What you need to be doing, is come to us teens and just ask us the best way to get through to us. asking other adults isnt very smart because what they were taught or told and their ideas are probably quite different to a teenagers.[76]

---

73   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. CS22-23.

74   Mr Abul Rizvi, Deputy Secretary, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS22; Consultative Working Group on Cybersafety, *Submission 113*, p. 35. Mr Rizvi is the Chair of the Consultative Working Group.

75   Mr Darren Kane, Corporate Security and Investigations and Officer of Internet Trust and Safety, Telstra Corporation, *Transcript of Evidence*, 8 July 2010, p. CS25; Ms Samantha Yorke, Legal Director, Yahoo!7, *Transcript of Evidence*, 8 July 2010, p. CS25; Mr John Pitcher, Director of Strategic Business Development, Netbox Blue, *Transcript of Evidence*, 8 July 2010, p. CS37.

76   Rachel, *Submission 126,* p. 1

Are you safe? Survey of Australian youth

2.92   As noted above, the Committee launched its *Are you safe?* online survey on the National Action Day Against Bullying and Violence, 18 March 2011, at Macgregor State School in Brisbane. This survey closed on 6 May 2011.

2.93   It was completed by 33,751 respondents from around Australia, by children and young adults ranging from five years to 18 years of age. 18,159 respondents completed the 12 years and under survey; 15,592 respondents completed the 13 years and older survey.

2.94   The results and comments received by the Committee through the survey are discussed throughout this Report.

Primary school visit

2.95   On the National Action Day Against Bullying and Violence, Friday 18 March 2011, the Committee visited MacGregor State School in Brisbane to formally launch the *Are you safe?* survey. Its students were the first students to complete the survey.

2.96   Members of the Committee also led small group discussions with students. These groups then reported back to the Committee as a whole and in camera evidence was formally taken from these presentations.

2.97   Group discussions generated many useful insights, and some groups developed practical recommendations for their peers to protect personal information. Discussions centred on the following key topics:

- Anonymity and disclosure of personal information on the Internet;

- Concerns about personal safety and avenues to seek help when feeling unsafe;

- Targets, prevalence and motivations of cyber-bullying and avenues to seek help;

- The success of current education programs and the degree of parental or guardians knowledge as a source of support and guidance; and

- Specific recommendations on how Australians can increase their own cyber-safety, and initiatives that can reduce cyber-bullying in our communities.

High school forum

2.98   Hosted by the Tasmanian Parliament in Hobart, the Committee held a High School Forum on Wednesday, 20 April 2011. The forum allowed the Committee to hear substantively from young adults in an environment where participants told of their experiences online and offered their insights into how safety in the online environment can be enhanced.

2.99   The Committee invited 45 students from a mix of public and private, co-educational and single-sex high schools and colleges from around the Hobart region. Participating schools included:

- Ogilvie High School;

- St Michaels Collegiate;

- Tasmanian Academy - Elizabeth College;

- Calvin Christian School;

- Cosgrove High School;

- New Town High School; and

- Guildford Young College.

2.100   The structure of the forum allowed Committee members to ask questions or pose scenarios to participants that were then debated amongst the participants.

Comments

2.101   The holistic view of technology taken by many young people has implications for their safety in the online environment. As at June 2010, the Alannah and Madeline Foundation reported that more than 1.6 million young Australians had received cyber-safety lessons in the classroom, yet rates of cyber-bullying, 'sexting', identity theft, breaches of privacy and sexual exploitation continue to rise.[77]

2.102   Roar Educate believed that fear has been a major driver of the national response to cyber-safety issues, supported by 'sensationalist media reporting' of incidents. This focused 'considerable attention' on the negative features of the online environment, rather than the many positive

---

77   Alannah and Madeline Foundation, *Submission 22*, p. 28.

benefits to education and life generally that come from 'safe, ethical and responsible' use of technology.[78]

> I do not think we should be panicking even though most of the Cyberbullying is unbelievably hurtful and terrible. We cannot give the message to parents especially that, if a child is cyberbullied, therefore they can only commit suicide. That is what is linked somehow in the messages which sometimes the media is sending for sensationalism. We have to address that as well.[79]

2.103   The Consultative Working Group on Cybersafety has identified the following key messages about cyber-bullying:

- The online environment is generally a positive place for young people, so that the situation is not all bad;

- Strategies for dealing with face-to-face-bullying are also effective for cyber-bullying;

- There is still time in Australia to put strategies in place to prevent serious problems, but 'action should be taken now';

- Young people need to be involved in developing solutions, as their involvement means that measures undertaken are likely to be accepted;

- Cyber-bullying is a behavioural issue that needs to be dealt with by the wider community, not only by schools;

- It is important not to punish the victim by removing access to the online environment when cyber-bullying is reported; and

- State and Territory educational authorities need to pursue coordinated responses to this problem.[80]

2.104   The Consultative Working Group on Cybersafety emphasised the variation in cyber-safety risks faced by Australian young people across the online environment. The nature and implications of the following abuses are likely to be significant, and have long-term negative implications, for the individuals involved, their families, the Australian community and its digital economy:

---

78   Roar Educate, *Submission 100*, p. 6. See also Australian Psychological Society, *Submission 90*, p. 8.

79   Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS9.

80   Consultative Working Group on Cybersafety, *Submission 113*, p. 15.

- ■ Cyber-bullying;
- ■ Inappropriate handling of the individual's and others' private information;
- ■ Exposure to and creation of inappropriate content;
- ■ Computer gaming addictions; and
- ■ Sexual predation.[81]

2.105   The Mental Health Council of Australia noted research from 2009 into Cyber-Safety from the Child Health Promotion Research Centre at Edith Cowan University on five major risks for young people:

- • Cyber-stalking, grooming and sexual solicitation;

- • Cyber-bullying;

- • Exposure to illegal and inappropriate material;

- • Promotion of inappropriate social and health behaviours and

- • Identity theft, privacy and online security.[82]

2.106   The many ways of interacting in the online environment expose people to a wider public than is possible offline. Young people often post personal and identifying material without thinking, or perhaps even being aware, of, any possible consequences. For example, sexting can have long term consequences for an individual as a potential employee.[83]

2.107   The range of risks confirms the concerns of organisations, such as the Queensland Catholic Education Commission, about the need for a clear definition of 'cyber-safety' and identification of the key issues, to deal with some of the myths surrounding the term. It believed that the concept of cyber-safety should be framed within the larger issue of student protection in general, reaching out to the responsibilities of peers, teachers, parents/carers and school authorities.[84] The Australian Youth Affairs Coalition emphasised the need to ensure that cyber-safety strategies address peer relationships.[85]

2.108   The chapters in Part 2 describe a range of threats to cyber-safety, with responses and strategies addressed in subsequent sections. Chapter 3 focuses on cyber-bullying, Chapter 4 on cyber-stalking, online grooming

81   Consultative Working Group on Cybersafety, *Submission 113*, p. 14.

82   Mental Health Council of Australia, *Submission 52*, pp. 3-4. See also iKeepSafe, *Submission* 101, p. 5, for the results of another study of online risks for young people.

83   Australian Psychological Society, *Submission 90*, p. 11. See Chapter 4 for sexting.

84   Queensland Catholic Education Commission, *Submission 67*, pp. 2, 6.

85   Australian Youth Affairs Coalition, *Submission 28*, p. 7.

and sexting, Chapter 5 on privacy and identity theft, and Chapter 6 on other significant cyber-safety threats. Chapter 7 examines how young people decide to post information online and their awareness of online risks.