1

Introduction

1.1 The online environment is an integral part of modern economic and social activities, and a vast resource of information, communication, education and entertainment.

1.2 This chapter introduces the online environment, platforms and access and the relevant cyber-safety issues and outlines the responsibilities of the Australian governments. The chapter concludes with an overview of the inquiry process and an outline of the report.

The online environment

1.3 The online environment is an essential tool for all Australians, including children and young people less than 18 years of age. [1] The ability to use online tools effectively provides both a skill for life and the means to acquire new skills.

> The Internet brings with it many advantages and benefits to children; their use of media permits them to gain and share knowledge in a variety of new and engaging ways. The Web 2.0 world allows children to create and share their own content and express their ideas, thoughts and experiences on a worldwide stage. The Internet allows children to go far beyond their homes

---

1 In this Report, where appropriate, 'child'/'children', 'adolescents', or 'young people'/'young adult(s)' will be used interchangeably, as appropriate, to mean people under the age of 18 years.

> and communities; they are able to explore the world, immerse themselves in different cultures, different geographies and different periods in history with the click of a mouse. The skills they learn through their online exploration in early life prepare them for their future, providing them with not just knowledge but also with abilities far beyond those skills that can be taught in the classroom.[2]

1.4 The power and usefulness of the online environment, and of social networking sites in particular, was convincingly demonstrated during the widespread floods in Queensland early in 2011.[3]

> The Internet has brought unprecedented freedoms to millions of people worldwide: the freedom to create and communicate, to organise and influence, to speak and be heard. The Internet has democratised access to human knowledge and allowed businesses small and large to compete on a level playing field. It's put power in the hands of people to make more informed choices and decisions. Taken together, these new opportunities are redefining what it means to be an active citizen.[4]

1.5 This environment brings significant benefits by sharing information, allowing them to keep in touch, at work and at play. As of 21 March 2011, Facebook advised the Committee that:

> Facebook has nearly 11 million active users who have visited the site in Australia within the past 30 days. Over nine million users visit every week and over seven million visit every day.[5]

1.6 It is also a valuable tool for breaking down physical boundaries. There are more mobile phones in Australia than people, 78 percent of households have computer access and 72 percent have Internet access.[6] Almost half of the mobile phones have an Internet capability and one-third of users

---

2 Family Online Safety Institute, *Submission 38*, p. 3.

3 AAP, 'Authorities learn to 'tweet' in disasters', 30 March 2011 accessed at http://www.cio.com.au/article/print/381497/authorities_learn_tweet_disasters/ on 5 April 2011; ABC News 'Disaster authorities move to use social media more, 4 April 2011 accessed at http://www.abc.net.au/news/video/2011/04/01/3182048.htm on 5 April 2011.

4 Google, *Submission 13*, p. 1.

5 Hon Mozelle Thompson, Advisory Board and Policy Adviser, Facebook, *Transcript of Evidence*, 21 March 2011, p. CS3.

6 Alannah and Madeline Foundation, *Submission 22*, p. 7.

access the Internet regularly on their phones.[7] The benefits can be multifaceted, for example, for Indigenous young people:

> For an Indigenous child it may be a connection to culture. It may be a connection to religious and spiritual pursuits. It may be a connection to family in other countries. Whatever that may look like for a child or young person, it is something that in a non-digital world they may have limited or very challenging access to.[8]

1.7 This environment is not static, and Australians are 'utterly voracious' in their adoption of online technologies. As they are introduced, new applications are therefore likely to be taken up enthusiastically by interested individuals and groups in the community. Some students continue to use email, however, there has been a rapid uptake of more portable technologies and social networking sites to communicate.[9]

1.8 Dr Helen McGrath's research from 2009 suggests that young people use the Internet for an average of one hour and 17 minutes per day, including almost 50 minutes for messages, visiting social websites and emails; 15 minutes for games online against other players, and 13 minutes for homework on the computer and/or the Internet.[10]

1.9 While there are potential safety issues for all those who go online, for the vast majority of users, the online environment is a positive and safe place.[11] In Australia:

> In the 12 months prior to April 2009, an estimated 2.2 million (79%) children accessed the Internet either during school hours or outside of school hours. The proportion of males (80%) accessing the Internet was not significantly different from females (79%). The proportion of children accessing the Internet increased by age,

7 Telecommunications Industry Ombudsman, *Submission 46*, p. 4, citing a Nielsen Company survey, April 2010.

8 Ms Lauren Oliver, Internal Consultant, Youth Empowerment and Participation, Berry Street, *Transcript of Evidence*, 9 December 2011, p. CS13.

9 Mr John Fison, Chairman, Netbox Blue, *Transcript of Evidence*, 17 March 2011, p. CS58.

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

11 Safer Internet Group, *Submission 12*, p. 2; Mrs Sue Hutley, Executive Director, Australian Library and Information Association, representing Safer Internet Group, *Transcript of Evidence*, 8 July 2010, p. 36.

> with 60% of 5 to 8 year olds accessing the Internet compared with 96% of 12 to 14 year olds.[12]

1.10 The benefits of online applications for young people in our society are accompanied by exposure to a range of potential dangers. Some of the most obvious include cyber-bullying, access to or accessing illegal and prohibited material, online abuse, inappropriate social and health environments, identity theft and breaches of privacy.

> One thing that both the online and offline world have in common is that many of these risks are created by the children, either putting themselves in harm's way or harming other children. The high profile risks, which have been reported by media, include the dangers of sexual exploitation and solicitation, online harassment and exposure to inappropriate images. However, the principal risks that come with Internet use by children today are the problems of cyberbullying, sexting, and self-harm websites.[13]

1.11 In addition to cyber-safety issues, this environment can also be a veil for an array of criminal behaviour including various online threats, the sale of illicit drugs and, increasingly, the sale of illegal pharmaceuticals.[14]

1.12 Young people have a limited capacity to make decisions about their own information. As they must rely on others to ensure that their interests and rights are protected, they are particularly vulnerable to a range of safety and criminal activities online.[15]

1.13 The Government's commitment to addressing cyber-safety issues for young people is reflected in the establishment of this Inquiry in March 2010 as the response of the Australian Parliament to community concerns about the impact of threats to young people from the online environment.

1.14 Australian authorities have considered problems caused by cyber-crime. A National Cyber-Crime Working Group was established in May 2010 to enable jurisdictions to work cooperatively to combat these crimes.[16]

1.15 Online crime has no borders and evidence can be transitory, highly perishable and, often, located overseas. Potential online threats are

12 Alannah and Madeline Foundation, *Submission 22*, p. 7, citing Australian Bureau of Statistics 8246.0 –' Household Use of Information Technology, Australia, 2008-09', April 2009, accessed 16 May 2010.

13 Family Online Safety Institute, *Submission 38*, p. 4.

14 Australian Customs and Border Protection Service, *Submission 109*, p. 3; Australian Federal Police, *Submission 64*, p. 2.

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

16 Attorney-General's Department, *Submission 58*, p. 2.

becoming more sophisticated through the use of networks to distribute material, and the protection of material by encryption.[17]

1.16 Significant research has been published over many years about the attitudes and behaviour of those less than 18 years of age in Australia. Given the speed of recent changes in the range and affordability of ways to enter the online environment, there is a lack of longitudinal data. Methodologies used differ from study to study making comparisons difficult in terms of its impact on that important group. In the absence of such studies, many bodies and groups appear to have developed ways to correct perceived problems in this environment, perhaps without an adequate evidential basis.[18]

1.17 One witness did not think that 'much more research is required', as so much is already available:

> We all know what the problem is ... We have to solve it ... a greater understanding of what is available from technology could help the broader community focus...[19]

Defining the online environment

1.18 Throughout this Inquiry, the term 'online environment' was widely used without any attempt to define it.[20] The Stride Foundation drew attention to some of the components of this environment, generally delivered through Internet platforms.[21]

1.19 This environment covers many means of informing and communicating with people. It is invisible, and for most urban Australians, can be accessed virtually: anywhere, at any time, from many devices, using any of those technological means. For most Australians, this environment can also be accessed with relative ease from a wide variety of locations: at home, work, school, libraries, university, TAFE colleges, public

17 Australian Federal Police, *Submission 64*, p. 13; Commonwealth Director of Public Prosecutions, *Submission 49*, p. 1.

18 Australian Privacy Foundation, *Submission 83*, p. 1; Mr John Dalgleish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS20; Dr Barbara Spears, Australian University Cyber-bullying Alliance, *Transcript of Evidence*, 3 February 2011, p. CS9.

19 Mr John Fison, Chairman, Netbox Blue, *Transcript of Evidence*, 17 March 2011, p. CS59.

20 Terms such as 'Online/environment', 'technology'/'technologies'/'new communication technologies', 'information and communications technology/ies', as appropriate, will be used interchangeably in this Report.

21 Stride Foundation, *Submission 6*, p. 4.

institutions such as art galleries, Internet cafes, coffee shops, book stores, etc.[22]

Platforms

1.20 The online environment allows users to do many things, including for example: sending/receiving emails/texts; sending images and making phone calls via Skype; paying bills; searching for and downloading material from websites (including for e-books); retrieving music, TV programs or movies; taking and sending photographs; joining chat rooms or live discussion forums; writing blogs; listening to FM or digital radio, etc.

1.21 Apart from the mobile phone, the Internet remains the best known, and most used platform or application in the online environment. As Professor Landfeldt noted, the Internet is a 'very fragmented world' with a large number of computing devices connected via communication links all using some common standards, such as the Internet Protocol. It is a platform on which a wide range of different and accessible content can be found.[23]

1.22 The most commonly accessed content is within one of these services, the world wide web. It is far from certain that it will remain the dominant platform for information exchange and retrieval in the future.

> There are now some very interesting developments from Stanford University and Berkeley that together have come up with an alternative routing infrastructure that goes to the core of forwarding traffic on the internet, changing the very fabric of forwarding. This is gaining traction with the big manufacturers ... There are also big efforts in putting anonymisation into the network and security so that, instead of having completely open channels for all communication, you are looking more at securing your data transfers, because it is not up for grabs for the entire world. It is very easy to wire tap and look at data that goes across the internet today. But there are clear signs that there is a lot of interest in changing that.[24]

22 Australian Council for Educational Research, *Submission 20*, p. 1.

23 Associate Professor Bjorn Landfeldt, University of Sydney, *Transcript of Evidence*, 24 March 2011, p. CS28; *Submission 122*, p. 2.

24 Associate Professor Bjorn Landfeldt, University of Sydney, *Transcript of Evidence*, 24 March 2011, pp. CS28-29.

1.23 The online environment is constantly changing, with newer alternatives fast gaining ground. The ability to communicate has expanded greatly in the past few years through the widespread use of social networking sites. In Australia, the fraction of peer-to-peer traffic is ever-increasing and the uptake of alternative media consumption is growing, particularly live streaming video and audio.[25]

1.24 The Internet is the most frequently used source of information and advice for young people. This opens up a range of possibilities, including concerns that access might be to the 'not-so-great' sites that also exist. Of course, as well as these online resources, there are organisations like Berry Street and the Inspire Foundation offering support to young people on a range of issues through their mental health and well-being programs.[26]

1.25 Many people now navigate via a Global Positioning Satellite. Gaming consoles such as Xbox and Playstation can also be part of the online environment, as can other communications services such as YahooMail and MSN.

1.26 The Internet and other platforms can now be easily accessed on increasingly capable mobile phones and smartphones, tablets, personal digital assistants, etc. These are more powerful and provide greater options for communication than advanced desktop machines of only a few years ago.[27] Laptops have become smaller and lighter, and 'notebook' variants are highly portable.[28]

1.27 The online environment has changed greatly following the introduction of popular social networking sites and feeds, such as Facebook, Bebo and Twitter and includes sites for the very young such as Club Penguin. Individuals elect to join these sites, providing photographs and information about themselves and their activities. Other people are asked to join as 'friends', to be in contact and exchange information and photographs, etc. Originators have some control over the release of personal information. The contents of individuals' account are monitored by the sites. Considerable publicity has been given to the risks implicit in the use of these sites.

---

25 Associate Professor Bjorn Landfeldt, University of Sydney, *Submission 122*, pp. 2-3, 4; *Transcript of Evidence*, 24 March 2011, p. CS27.

26 Associate Professor Sheryl Hemphill, Senior Research Fellow, Murdoch Children's Research Institute, *Transcript of Evidence*, 9 December 2010, p. CS23; Ms Megan Scannell, Senior Project Manager, Victorian Office of the Child Safety Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS72; Inspire Foundation, *Submission 3*, p. 1.

27 Civil Liberties Australia, *Submission 23*, p. 1.

28 Australian Council of Educational Research, *Submission 20*, p. 2.

1.28 As the applications mentioned above are not intended to be a definitive list, in this Report the broadest possible range will be treated as belonging to the online environment.

Access to the online environment

1.29 The System Administrators' Guild of Australia referred to Australian Bureau of Statistics' figures which showed that, at December 2009, there were over nine million business and personal subscribers to Internet services in Australia. ABS also found that, in 2009, 72 percent of Australian houses have Internet access, and that 79 percent of children five to 14 years old used the Internet. At that time, homes were slightly more usual sites for usage than schools: 73 to 69 percent.[29]

- Computers were available in more than 71% of households with 3–4 year olds, increasing to more than 90% of homes with 7–8 year olds, and in almost all households with 8–17 year olds (98%).
- Internet access was available in more than 65% of households with 3–4 year olds, increasing to more than 72% of homes with 7–8 year olds, 87% of homes with 8–11 year olds, and more than 90% of households with 12–17 year olds.
- Eighty-four percent of 7–8 year olds sometimes used the Internet at home to find information for school, send emails, chat online, surf the internet, play games, or to access/download music or movies.
- Among 8 to 17-year-olds, use of the Internet for homework and leisure activities increased with age, from 61% of 8–11 year olds, to 83% of 12–14 year olds and 88% of 15–17 year olds.
- Some 74% of parents of 7–8 year olds in the study were happy with their child's media use.[30]

1.30 While these figures suggest an online society, some people do not own computers. Public libraries, government cafes for older people or Internet cafes are often their only means of access to the Internet, emails, etc. While

29 System Administrators' Guild of Australia, *Submission 71*, p. 2 citing Australian Bureau of Statistics, 2009, Household Use of Technology, Australia, 2008-09 at http://abs.gov.au/ausstats/abs@nsf/mf/8146.0/.

30 Australian Institute of Family Studies, *Submission 39*, p. 2 citing the Australian Communications and Media Authority, 2009, *Use of electronic media and communications: Early childhood to teenage years.* Finding from *Growing up in Australia: The Longitudinal Study of Australian Children (3 to 4 and7 to 8 year olds)* and *Media and Communications in Australian Families (8 to 17-year-olds), 2007,* Canberra ACMA.

some places are not accessed often by the community, for some users, they may be their only access points.[31]

1.31 Research by the Australian Communications and Media Authority (ACMA) in 2009 showed that:

> The Internet is a regular part of the everyday lives of children and young people aged eight to 17 years, and it is used regularly within both school and home environments.

1.32 ACMA added that the use of the Internet, including finding information for academic purposes, and social networking can become regular from the age of 12.[32]

1.33 Australia now has a generation of people who have never been without online access and have integrated it fully into their lives. Another generation, brought up in the time of other communications systems, may not fully understand or utilise technology in the same way. In between these groups, there are many other people whose interest and skills in the online environment depend on the situation in which they find themselves. The latter groups can feel disempowered in situations where young people may know far more about the online environment than they do.[33]

1.34 People less than 18 years old can easily bypass physical access points which may have filters or other safety measures. [34] Many submissions dealt with a proposed mandatory, national, filtering system.

1.35 That there are groups of parents/carers with different levels of expertise, time and interest is important when considering ways to integrate these groups into school communities. This issue will be addressed in Chapter 10.

1.36 Worldwide, Facebook has over 500 million active users: less than 12 percent are less than 18, more than half are over 35, while the fastest growing demographic is between 40 and 60 years old.[35] It has been estimated that 'about half' the Internet users in Australia are on Facebook. An Australian study revealed that 61 percent of all mothers aged from 45

31 Inspire Foundation, *Submission 3*, p. 4; Tutoring Australasia Pty Ltd, *Submission 26*, p. 1.

32 Australian Communications Media Authority, 2009, *Click and Connect: Young Australians' use of online media* (cited by the Australian Council for Educational Research, *Submission 20*, p. 3.)

33 Ms Hetty Johnston, Founder and Executive Director, BraveHearts, *Transcript of Evidence*, 17 March 2011, p. CS41.

34 Australian Youth Affairs Council, *Submission 28*, p. 8.

35 Hon Mozelle Thompson, Advisory Board and Policy Adviser, Facebook, *Transcript of Evidence:* 21 March 2011, p. CS1; 11 June 2010, pp. CS23.

to 65 years had a Facebook page. Nevertheless, young people and adults use this technology in different ways. Dr McGrath considered that all adults do not organise their social lives using social networking sites, and often fail to understand this use of technology.[36]

1.37 While most Australian children have access to the online environment at a variety of places and via a range of platforms, there are other groups who are disadvantaged. Lack of access to the online environment can have particular impacts on some children, [37] and this will be addressed in Chapter 2.

1.38 The Interactive Games & Entertainment Association pointed out that new and evolving technologies are and will be central to the lives of young people, to be adapted, discarded, rapidly and often indiscriminately. The Association believed that young people should be granted freedom to explore and interact in the online environment. At the same time, steps must be taken to minimise inherent risks and to provide the same levels of caution exercised as in the 'real' world.[38]

1.39 Protection of young people is compacted by the rapid evolution of technology, and the fact that education, research and the law inevitably lag behind these developments. [39] While access is easy and varied, many young people are not aware of or disregard possible consequences of their actions in the online environment. These consequences can be serious and last forever.

'Cyber-safety'

1.40 The term 'cyber-safety' was used widely throughout the Inquiry. As it was largely undefined, its meaning and scope were unclear and there is a need to identify the key issues to clarify some of the myths surrounding it.[40]

1.41 Mr Geordie Guy stated that it was 'a made-up term or a '"neologism"... native to the Australian government, child protection agencies... and

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

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

38 Interactive Games & Entertainment Association, *Submission 110*, p. 3.

39 Mr Darren Kane, Director, Corporate Security and Investigations/Officer of Internet Trust and Safety, Telstra Corporation, *Transcript of Evidence*, 8 July 2010, p. CS24.

40 Australian Privacy Foundation, *Submission 83*, p. 1; Queensland Catholic Education Commission, *Submission 67*, p. 2.

organisations seeking to commercially supply solutions to the perceived problem', and that there was no such globally accepted term.[41]

1.42 The Office of the Privacy Commissioner noted that it is 'a broad concept that concerns minimising the risks to children online from a range of negative influences including inappropriate social behaviours, abuse, identity theft and breaches of privacy.' [42] This concept will be used in this Report.

1.43 The Australian Psychological Society noted that, while there are risks in the online environment, they were often 'over-exaggerated' with the media portraying worst case scenarios. 'Technology' is often blamed for behaviour rooted in wider social problems, and in the range of issues characterising adolescence.[43]

1.44 Most young people are aware of cyber-safety measures and have incorporated these practices into their everyday online activities. The 'average' young person seems to have mechanisms to deal with online risks: good family or peer-to-peer relationships and critical decision-making skills. It is often the marginalised young people, disconnected from the community, for whom cyber-safety can become an issue.[44]

Adult responses to cyber-safety issues

1.45 The Cooperative Research Centre for Young People, Technology and Wellbeing noted that conventional approaches to cyber-safety for young people tend to focus on risk management, typically through educational and regulatory means.[45]

1.46 The Centre believed that thinking about cyber-safety in these terms failed to acknowledge the expertise of young people in technology and the use of the Internet. Most cyber-safety programs are delivered at schools, removed from other settings, such as family or work, and the social relationships with peers, parents/carers and other adults in which young people regularly engage.

---

41 Mr Geordie Guy, *Submission 105*, p. 3.

42 Office of Privacy Commissioner, *Submission 92*, p. 3.

43 Australian Psychological Society, *Submission 90*, p. 8.

44 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence,* 11 June 2010, p. CS32.

45 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, pp. 9-10

1.47 The focus on cyber-safety and risk management means, therefore, that there is relatively little evidence about adults' concerns about the online environment, and particularly about young people's use of social networking sites. The Centre stated that it is vital that young people's perspectives are incorporated in the cyber-safety debate in ways that empower them and develop meaningful policies and programs.[46]

1.48 Parents/carers have the ultimate responsibility for educating and protecting their children, including in the online environment. Adults and young people use technology in different ways, and new communications technologies are becoming increasingly foreign to many parents/carers, thus 'reducing their ability to protect their children.' More often than not, children know more about the Internet and mobile phones, etc, than adults. Rapidly emerging new technologies are increasingly leaving many adults behind.[47]

1.49 Moreover, parents/carers often feel an additional lack of involvement or control because they do not fully understand how their children use their knowledge about the online environment, and are fearful about online risks. Teachers may also have a limited understanding of children's use of technology. Parents/carers and teachers can therefore have such limited understanding and awareness of the issues that they are 'very reluctant' to deliver, and totally lack confidence in delivering, such curriculum material or information about cyber-safety as is available in Australia.[48]

1.50 As seen by adults, threats implicit in the online environment include:

- predators;
- cyber-bullying;
- 'Internet addiction'; and
- lack of sleep.[49]

1.51 Some young people are 'fearless but naïve' and dismissive of these risks and fears. They can be more concerned about slow Internet connections and viruses on their computers. For example, the Alannah and Madeline Foundation noted that 'nearly all' the young people it has interviewed

46 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, pp. 9-10.

47 BraveHearts, *Submission 34*, p. 4.

48 Alannah and Madeline Foundation, *Submission 22*, p. 8; Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS32.

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

have experienced or witnessed cyber-bullying, and consider it 'common and extremely unpleasant'. [50] With other online threats, these matters will be addressed in Part 2 and the results of the Committee's *Are you safe* online survey are provided throughout the report.

Australian Government responsibilities

1.52 Many Australian Government Departments and agencies have policy and regulatory responsibilities in the online environment.

1.53 The **Department of Broadband, Communication and the Digital Economy** is responsible for developing a vibrant, sustainable and internationally competitive broadband, broadcasting and communications sector and through this, promote the digital economy for the benefit of all Australians.

1.54 Within that Department, the **Australian Communications and Media Authority** (ACMA) has been operating in cyber-safety space for more than ten years. Via the Online Content Scheme, in the *Broadcasting Services Act 1992* (the Act), its role is:

- to investigate complaints about prohibited and potentially prohibited online content, and
- to facilitate a system of co-regulation where the internet industry develops codes of practice that are registered by the Australian Communications and Media Authority.[51]

1.55 Under the Act, the Authority is also responsible for liaison with regulatory and other relevant overseas bodies to develop cooperative arrangements for the regulation of the Internet. This includes issuing take-down notices to Australian hosts of prohibited content, and a blacklist of a range of inappropriate sites.

1.56 ACMA undertakes research into the online environment, and has a significant range of effective educational programs. Increasingly, 'a large part' of its role, resources and activities is in delivering a broad range of cyber-safety, educational and awareness programs.[52]

1.57 Chaired by a senior officer from the Department, the **Consultative Working Group on Cybersafety** was established in 2008 to advise the

50 Alannah and Madeline Foundation, *Submission 22*, pp. 8-9.

51 Australian Communications and Media Authority, *Submission 80*, p. 1.

52 Australian Communications and Media Authority, *Submission 80*, pp. 1, 13; Consultative Working Group on Cybersafety, *Submission 113*, p. 7; ACT Government, *Submission 82*, p. 7.

Australian Government on best practice safeguards and priorities for action by government and industry. It comprises representatives from industry, community organisations and Government bodies such as the Australian Communications and Media Authority, the Attorney-General's Department and the Australian Federal Police.[53] The Working Group is required to:

- consider those aspects of cyber-safety faced by Australian children;
- provide information to Government on measures required to operate and maintain world's best practice safeguards for Australian children engaging in the digital economy; and
- advise the Government on priorities for action by government and industry.[54]

1.58 The Consultative Working Group on Cybersafety and the **Youth Advisory Group** are the Government's main vehicles for cyber-safety consultation. The Youth Advisory Group provides the Government with advices about issues such as law enforcement, filtering, education and research initiative from a young person's perspective. The Consultative Working Group on Cybersafety considers that the Youth Advisory Group will continue to be crucial in providing the views of children and young people about:

- the nature of young people's online engagement;
- emerging cyber-safety risks; and
- how best to tackle these risks from the young person's perspective.[55]

1.59 In December 2010, the Minister for Broadband, Communications and the Digital Economy, Senator the Hon Stephen Conroy, launched the Cyber Safety Help Button.

1.60 The **Department of Education, Employment and Workplace Relations** provides national leadership in education and workplace training, transition to work and conditions and values in the workplace. As one of the current initiatives, the Australian Government is providing $2.4 billion over seven years to contribute to teaching and learning in Australian schools, preparing students for further education, training and to live and work in a digital world. Through the Digital Education Revolution, funding has been provided for:

53 For its membership and terms of reference, see Consultative Working Group on Cybersafety, *Submission 113*, Attachments A and B.

54 Consultative Working Group on Cybersafety, *Submission 113,* p. 1.

55 Consultative Working Group on Cybersafety, *Submission 113*, p. 2.

- New information and communications technology equipment for all secondary schools, for students in Years 9 to 12, through the National Secondary Schools Computer Fund;
- Deployment of high speed broadband connections to schools;
- Collaboration with States/Territories and Deans of Education to ensure new and continuing teachers have access to training in the use of ICT that enables them to enrich student learning;
- Online curriculum tools and resources supporting the national curriculum and specialist subjects such as languages;
- Parents to participate in their children's education through online learning; and
- Supporting mechanisms to provide vital assistance for schools in the deployment of ICT.

1.61 The **Attorney-General's Department** is responsible for administering Government policy on criminal law and law enforcement, including cyber-crime, cyber security and anti-discrimination. This includes such issues as cyber-racism, identity security and classification, grooming and procuring offences by targeting predatory behaviour occurring through carriage services.[56]

1.62 The **Australian Federal Police** (AFP) is the principal law enforcement agency through which the Australian Government pursues its law enforcement interests. The AFP is unique in Australian law enforcement in that its functions relate both to community policing and to investigations of offences against Commonwealth law enforcement in Australia and overseas. It has responsibilities for child protection matters.

1.63 The **Australian Institute of Criminology** is Australia's national research and knowledge centre on crime and justice. It seeks to promote justice and reduce crime by undertaking and communicating evidence-based research to inform policy and practice. Its functions include conducting criminological research; communicating the results of research; conducting or arranging conferences/seminars; and publishing material arising from its work.[57]

1.64 It has worked closely with the Attorney-General's Department, the AFP and other agencies to undertake research into technology-enabled crime.

56 Attorney-General's Department, *Submission 58*, p. 2. Consultative Working Group on Cybersafety, *Submission 113*, p. 7.

57 Australian Institute of Criminology Home page: www.aic.gov.au

In 2007, the Institute was commissioned to report on existing literature concerning the use of social networking sites for sexual grooming, the extent and nature of the problem, and effective ways in which to address it. The resulting publications have been cited many times in this Report.[58]

1.65 The **Office of the Privacy Commissioner** is an independent statutory body whose purpose is to promote and protect privacy in Australia. Established under the *Privacy Act 1988* (Cth), it has responsibilities for the protection of individuals' personal information handled by Australian and Australian Capital Territory Government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses.[59]

1.66 The **Commonwealth Director of Public Prosecutions** is responsible for the prosecution of criminal offences against the laws of the Commonwealth, and to conduct proceedings for the confiscation of the proceeds of crimes committed against the Commonwealth.[60]

1.67 In the context of this Inquiry, the role of the **Australian Customs and Border Protection Service** is to regulate the movement of prohibited and restricted goods across Australia's borders, including goods purchased on the Internet.[61]

1.68 The **Commonwealth Ombudsman** safeguards the community in its dealings with Australian Government agencies. It handles complaints, conducts investigations, performs audits and inspections, encourages good administration, and carries out specialist oversight tasks.[62]

State and Territory responsibilities

1.69 School education, policing and legal matters within each jurisdiction are primarily responsibilities of State/Territory governments. These matters will be addressed in relevant parts of this Report.

58 Australian Institute of Criminology, *Submission 56*, pp. 1-2.

59 Office of Privacy Commissioner, *Submission 92*, p. 3.

60 Commonwealth Director of Public Prosecutions, *Submission 49*, p. 1.

61 Australian Customs and Border Protection Service, *Submission 109*, p. 2.

62 Australian and New Zealand Ombudsman Association, *Submission 53*, p. 4. This position has been included because of sub-paragraph viii of the Inquiry's Terms of Reference.

Current Parliamentary inquiries

1.70 In March 2011, the Joint Standing Committee on the National Broadband Network was formed to inquire into and report on the rollout of the Network. It will provide progress reports every six months, from 31 August 2011, to both Houses of Parliament and shareholder Ministers on a range of matters related to the Network until completion and it is operational.

1.71 The House of Representatives Standing Committee on Infrastructure and Communications is inquiring into the role and potential of the National Broadband Network. The Committee is due to report its findings by the end of August 2011.

Previous Parliamentary reports

1.72 On 7 April 2011, the Senate Environment and Communications References Committee tabled a report titled *The adequacy of protections for the privacy of Australians online*. It made several recommendations that are relevant to this Inquiry, and these will be addressed in Chapter 5.

1.73 The 2010 Report by the House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime,* addressed 'the incidence of cybercrime on consumers'. This Report examines different but related issues. It seeks to make its contribution to knowledge of the benefits of, and the potential perils created by, the online environment. These perils are especially important for users who are less than 18 years old.[63]

1.74 Other relevant reports include:

- House of Representatives Standing Committee on Employment, Education and Training: *Sticks and Stones: Report on Violence in Australian Schools* (1994);
- House of Representatives Standing Committee on Communications, Information Technology and the Arts: *From Reel to Unreal: Future opportunities for Australia's film, animation, special effects and electronic games industries* (2004);

63 House of Representatives Standing Committee on Communications, Terms of Reference, p. xv.

- Senate Standing Committee on the Environment, Communications and the Arts: *Sexualisation of children in the contemporary media environment* (2008); and
- House of Representatives Standing Committee on Family, Community, Housing and Youth: *Avoid the Harm - Stay Calm. Report on the Inquiry into the impact of violence on young Australians* (2010).

1.75 In 2009, the NSW Legislative Council's General Purpose Standing Committee (No 2) released a report *Inquiry into Bullying of Children and Young People*. A number of its recommendations concerned cyber-bullying.

Australian Law Reform Commission Inquiry

1.76 The Government has asked the Australian Law Reform Commission to review the definition of 'Refused Classification' material, as part of a wider review of the National Classification System.

Joint Select Committee on Cyber-Safety

Conduct of the Inquiry

1.77 In the last Parliament, the House of Representatives agreed to establish the Committee on 25 February 2010. On 11 March 2010, the Senate agreed to this proposal. As the Inquiry was incomplete at the prorogation of that Parliament, it lapsed.

1.78 In the 43rd Parliament, the House of Representatives agreed on 16 November 2010 to the re-establishment of the Committee, with slightly different terms of reference. The Senate agreed on 17 November 2010. The revised terms of reference can be found at p. xxi.

1.79 The Committee wrote to all Ministers, State Premiers/Chief Ministers, organisations and individuals who had forwarded submissions to the original Inquiry seeking additional submissions.

1.80 The Inquiry was advertised in *The Australian* at fortnightly intervals, and featured on a number of occasions in *About the House* and Sky News, House of Representatives Alert Services, Facebook, Google and Twitter.

1.81 In all, 152 submissions and 16 supplementary submissions were received in response to the invitations to contribute to the Inquiry. A list of submissions is at Appendix A.

1.82 A list of other documents of relevance to the Inquiry that were formally received by the Committee as Exhibits is at Appendix B.

1.83 Three roundtable discussions were held in Melbourne and Sydney in June and July 2010. Evidence was given by:

- The information and communications technology industry;
- Academics;
- The Australian Federal Police;
- Non-government organisations working with young people;
- Facebook;
- Professional bodies and unions;
- Representatives of parents/carers;
- Corporations such as Telstra and Symantec; and
- Content providers such as Yahoo!7.

1.84 The Committee also took evidence at public hearings in Adelaide, Brisbane, Canberra, Hobart and Melbourne. A list of organisations and individuals who gave evidence to the Inquiry at the roundtables and public hearings is at Appendix C.

1.85 In addition, the Committee conducted two school forums, one at McGregor State School in Brisbane for Grade 7 students, and the other for Years 9 to 12 in Hobart with students attending from Calvin Secondary School; Cosgrove High School; Elizabeth College; Tasmanian Academy; Guilford Young College; MacKillop Catholic School; New Town High; Ogilvie High School; and St Michael's Collegiate School

1.86 The Committee also conducted two online surveys of young people in relation to cyber-safety issues. A total of 33,751 young people completed: 18,159 for those less than 12 years old and 15,592 for 13 to 18 year olds. Additional information and the methodology used in the survey is at Appendix D.

Table 1.1 Number of survey respondents by gender and age

Age	Female	Male	Not Stated	Total
5	82	75		157
6	64	48		112
7	97	110		207
8	493	424		917
9	1078	1004		2082
10	1798	1701		3499
11	2502	2305		4807
12	2263	2239		4502
13	2456	1890		4346
14	1982	1612		3594
15	1374	1191		2565
16	998	807		1805
17	568	395		963
18	259	312		571
Not stated			3624	3624
Grand Total	16 014	14 113	3624	33 751

Figure 1.1 Number of survey respondents by *gender and age*

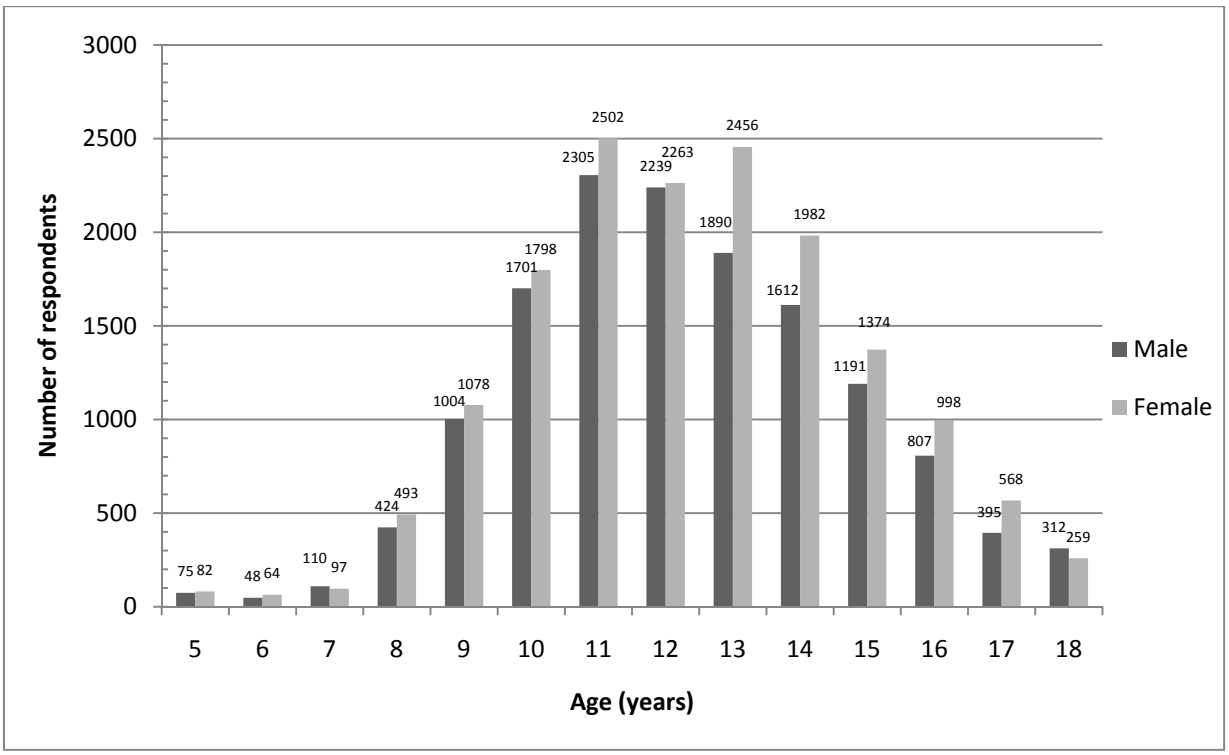

Figure 1.2 Committee Chair, Senator Dana Wortley, during a small group discussion with students at McGregor State School.

Figure 1.3 The Committee during discussions with students and teachers at McGregor State School.

1.87 Copies of all submissions and transcripts that were authorised for publication are available electronically from the Committee's website, at www.aph.gov.au/jscc.

Overview of this Report

1.88 The structure of this Report is based on the Inquiry's Terms of Reference.

Part 1: Introduction

1.89 Part 1 provides the necessary background material to the Inquiry. This section defines and describes the online environment, and defines 'cyber-safety'. It outlines the roles of Commonwealth, State and Territory Government departments and agencies with policy and regulatory responsibilities, in general terms, in the online environment. It then describes legal responsibilities for combating online crime in Australia.

1.90 Chapter 2 outlines the environment in which young people find themselves, including the major stakeholders. It describes two potential problem areas for young people: 'real' and 'online' worlds and privacy. There are at least four groups of young adults who are disadvantaged in the online environment. While they may have access via school libraries, their entry to it can be problematic. Some of the negative features of that environment, for adults and parents/carers particularly, is then outlined.

Part 2: Cyber-safety

1.91 The four Chapters of Part 2 should be regarded as a unit. Chapters 4 to 6 deal with specific abuses of cyber-safety; cyber-bullying, cyber-stalking, online grooming , sexting, privacy and identity theft, and other cybersafety complexities such as fraud, 'technology addictions', online gambling and illegal and inappropriate content. Chapter 7 outlines the responses of young people to the Committee's online survey in relation to how young people make the decision on whether or not to post.

Part 3: Educational strategies

1.92 Part 3 covers the measures necessary to support schools, teacher and the wider school community. Chapter 8 explores a range of ways to support schools to increase cyber-safety and, in particular, to reduce cyber-

bullying. Chapter 9 focuses on support for teachers and chapter 10 looks at the broader school community.

Part 4: Enforcement

1.93 This part of the report outlines the various legal and policing aspects of these abuses, including existing Commonwealth and State/Territory sanctions against them. Chapter 11 outlines legislative approaches. Chapter 12 addresses policing. Chapter 13 focuses on the proposal to establish an online ombudsman to act on cyber-safety issues.

Part 5: Australian and international responses

1.94 Chapter 14 deals with achieving best practice in Australia by government initiatives, industry and non-government organisations. Similarly Chapter 15 examines various international responses to cyber-safety issues.

1.95 Chapter 16 examine the likely benefits of new and existing technologies. Chapter 17 focuses specifically on the mandatory national filtering system proposal.

Part 6: Conclusions

1.96 Chapter 18 summarises the views of students, and report's conclusions are in Chapter 19.

Results of the Inquiry

1.97 To involve young people, and hear what they have to say, an online survey was undertaken. As noted above, 33,751 responses were received, and the results are used throughout this Report. It gains depth from some very informative and sometimes distressing, anonymous contributions.

1.98 The most significant, general points to emerge from the range of material received by this Inquiry included:

- the need for children and young people to be in control of their own experiences in the online environment through better education, knowledge and skills;
- the need for enhanced privacy provisions in the online environment;

- the short-term need for more detailed and longitudinal Australian research on how young people are interacting with the online environment, and emerging technologies in particular. Then based on that research, there is a requirement for a cooperative national response, based on a range of educational programs. To be effective, a combination of carefully designed and targeted programs is needed for the use of parents/carers and teachers, and the varied needs of the different developmental stages of Australian young people; and
- the need for parents/carers, teachers and all those who engage with young people to become more informed, and gain an understanding of online technology and its many uses.