19

Conclusions

19.1 Most users of technology find their experiences in the online environment are useful, pleasurable and trouble-free. Technology is now so central and so valuable that our lives would be incomprehensible without it. Although there have been problems and even tragedies for some users, it would be unrealistic not to acknowledge these facts about use by the majority.

19.2 While it is clear that existing cyber-safety programs are very useful, their range and variety can cause difficulties for those who are not confident in the online environment. A cross jurisdiction, coherent approach has been muted:

> A national coordinated approach is essential. There are many initiatives and sources of information available from a large variety of bodies including universities, all three levels of government – local, state and federal, schools and education departments, and not for profit associations. It is becoming overwhelming for parents, teachers, children and other users to navigate all the information and advice, and to find applicable and practical information quickly when necessary.[1]

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

Centralised system

19.3 One of the issues for young people seeking assistance is that they have to determine which organisation to contact. A central point of contact would be beneficial.[2] The Alannah and Madeline Foundation commented that:

> We, as a foundation, would be approached weekly by someone with a new whizzbang resource that is going to solve cybersafety, whether it is targeted at a parent or a child. With our eSmart project, we are triaging those and pointing to the ones that we know are evidence based. There does need to be a sorting mechanism and there needs to be an awareness of what is already out there so we do not duplicate. Duplication is a huge problem.[3]

19.4 Current programs to reduce online risks are developed by many organisations: particularly the educational and commercial sectors, and the information and technology industry. It is clear that these risks are not being fully addressed, especially for young people.

19.5 The Office of the Privacy Commissioner stated:

> Cyber safety is a national problem and an important way to minimise cyber safety risks is to adopt a coordinated approach across portfolios and jurisdictions. Cross-portfolio co-operation enables agencies specialised in particular areas to collectively consider different aspects of information communications technology initiatives and their associated privacy and security risks, and to develop an appropriate responses. Ensuring that various education and awareness programs are complementary and co-ordinated is key to promoting an empowered community.[4]

19.6 The Association of Independent Schools of South Australia suggested:

> exploration of the formation of a national an advisory group to guide policy development and keeping a watching brief on the 'bigger picture', particularly in regards to international research and policies.[5]

---

2 Mrs Sandy Dawkins, Manager, Engagement and Wellbeing, Office of Youth, SA, *Transcript of Evidence*, 3 February 2011, p. CS22.

3 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. CS37.

4 Office of the Privacy Commissioner, *Submission 92*, p. 7.

5 Association of Independent Schools of SA, *Submission 19*, p. 15.

19.7 The Australian Direct Marketing Association supported the establishment of a single office:

> an Office of Online Security be established to provide industry, consumers and all relevant stakeholders with a single point of contact for this vitally important issue.[6]

19.8 The Safer Internet Group endorsed this view:

> a more coordinated approach across the departments and across the programs [should] be undertaken. Within the Department of Broadband, Communications and the Digital Economy and also the Attorney-General's Department there could be some better collaboration across cybersecurity and cybersafety.[7]

19.9 The Independent Education Union of Australia believed that the range of programs available needs to be brought together, identify what is best practice and decide how and where schools can be involved.[8]

19.10 The Australian Institute of Criminology believed that there is too much material already available, and that this should be coordinated into information sites managed by a central agency.[9]

19.11 The United Kingdom Council of Child Internet Safety is an example of such a body, as it:

> brings together over 140 organisations and individuals to help children and young people stay safe on the internet. It is made up of companies, government departments and agencies, law enforcement, charities, parent groups, academic experts and others.[10]

19.12 The United Kingdom's Home Office Task Force on Child Protection on the Internet has developed a series of good practice guides:

> These documents were intended primarily as a guide to commercial or other organisations, or individuals, providing online services or considering doing so in the future, but as public documents, are also of interest to internet users. The guidance

6 Australian Direct Marketing Association, *Submission 36*, p. 6.

7 Ms Sue Hutley, Executive Director, Australian Library and Information Association, representing the Safer Internet Group, *Transcript of Evidence*, 8 July 2010, pp. CS16.

8 Mr Chris Watt, Federal Secretary, Independent Education Union of Australia, *Transcript of Evidence*, 30 June 2010, p. CS3.

9 Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS19.

10 Childnet International, *Submission 18*, p. 4.

> covered includes advice on chat, search, moderation and social networking services. ACMA submitted a statement of support for the Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services 2007, as well as participating in the drafting of the guidance. Best practice documents have also been drafted and promoted by industry groups, such as the UK code of practice for the self-regulation of new forms of content on mobiles and the European Commission including Safer Social Networking Principles for the EU20 and the European Framework on Safer Mobile Use by Younger Teenagers and Children.[11]

19.13 Singtel Optus also raised the point that there is a need for greater collaboration to ensure resources are 'pooled and used effectively, and to ensure that there is a consistent message'.[12] Childnet International stated:

> It is key to make sure that all actors in this space – parents, schools, children and young people but also law enforcement, industry and governments are playing their part in making the internet a great and safe place and are supported in this.[13]

19.14 The Australian Communications and Media Authority (ACMA) has a range of regulatory and educational roles. Its personnel are knowledgeable and experienced, and the resources they provide are highly valued. It is in an ideal position to take on a greater role in coordinating cyber-safety in the online environment. As a result of its research, it has a range of programs to increase cyber-safety and educate users of technology. For example , the Cyber Safety Help Button was developed in response to advice from the Youth Advisory Group, set up to provide a forum where young Australians can talk directly to government about cyber-safety.

19.15 The Consultative Working Group on Cybersafety exists to advise the Government on priorities for action by government and industry about cyber-safety, especially for Australian children. It includes representatives from industry, community organisations and Australian Government agencies. It would be, therefore, the appropriate body to recommend an appropriate, revised role and structure for ACMA.

---

11 Childnet International, *Submission 18*, pp. 4-5.

12 Singtel Optus Pty Ltd, *Submission 42*, p. 2.

13 Childnet International, *Submission 18*, p. 8.

19.16 The importance of clear definitions was emphasised throughout the Inquiry. One of the first tasks for a centralised body should be to develop appropriate definitions, especially for cyber-bullying:

> The most frustrating thing about Australia in the way that we do things is this lack of consistency...We have different laws right across the country. We cannot agree on the definitions of what a child is. We cannot agree on an age of consent, and here we are talking about cybersafety and all of these other elements. I think trying to get people around the same table from the states and territories is notoriously hard and trying to get them to agree on anything is even harder. Starting to work collaboratively at the top level, by taking on an issue, particularly as this is a new one relatively speaking, might help us as a nation to pull together and understand that we are all dealing with the same people. This lack of consistency and the unwillingness for the states to engage and do the same things everywhere is very frustrating from the child protection point of view. I am happy to say that the framework appears to be tearing that down a little bit, which is great.[14]

19.17 A statement from young people from the Australian/European Training School on cyberbullying included the following list of priorities:

- A clear definition of what cyberbullying is, including the effects and consequences;
- Clarity around policy i.e. what inappropriate behaviours we are talking about;
- Education and education for parents and peers in cyber-safety; how to use Facebook, e.g. privacy settings and what they really mean;
- Adults to acknowledge the importance of how children cope with cyber-bullying;
- Research in every country to figure out the nature of the problem which feeds into addressing the issues;
- Increase communication between students and teachers;
- To promote the notion that it is acceptable to talk about experiences of cyber-bullying to help those who are victimized in the future; and
- Researchers to identify strategies for parents to give support/advice to their children.[15]

---

14 Ms Hetty Johnston, Founder and Executive Director, BraveHearts, *Transcript of Evidence*, 17 March 2011, p. CS42.

15 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 23.

Central portal

19.18 The Australian Toy Association would like to see current information on cyber-safety made available in a central portal:

> A range of government and nongovernment online material was released and promoted. These were seemingly unrelated to one another. There needs to be more co-ordination.[16]

National cyber-safety education program

19.19 A national cyber-safety education program, devised and implemented with the cooperation of all Australian jurisdictions is central to addressing risks in the online environment.

19.20 Schools are the best places to do this, however, any programs that are adopted must be more than a series of 'bolted-on' classes added to already crowded curricula. Continuing to provide ad hoc classes on cyber-safety will not address or resolve effectively cyber-safety problems experienced by young Australians.

19.21 Cyber-safety is essential for all Australian students and therefore needs to be taught within curriculums. As already noted, the Australian Curriculum, Assessment and Reporting Authority is developing the Australian Curriculum. One of its seven general capabilities is competence in information and communications technology. The opportunity exists, therefore, to recognise and fulfil the need for a national approach to cyber-safety education at schools, one that is embedded in curricula.

19.22 The South Australian Commission for Catholic Schools supported the revised National Safe School Framework as a 'well accepted national framework to develop specific school initiatives focused around student safety, addressing bullying and harassment and positive student behaviours'.[17]

19.23 To be effective and increase cyber-safety for young people in particular, such a national program must be:

- thoroughly researched;
- broad and deep in its concepts and approach;
- well funded; and

16 Australian Toy Association, *Submission 45*, p. 1.

17 South Australian Commission for Catholic Schools, *Submission 9*, p. 6.

- long term.

19.24 Above all, an effective program must be the fruit of a cooperative approach so that it can be introduced across all Australian jurisdictions. All users, regardless of their locations, face similar online risks. Without a cooperative approach, many young Australians will continue to face risks in the online environment with inadequate guidance on how to deal with them.

19.25 Netbox Blue outlined the benefits of this approach:

> - Schools will embrace the program as it offers them reassurance of a centrally provided and thoroughly researched set of Standards that offer them a Certification that they will be proud of;
> - Schools will be able to spend less time pursuing individual research into how to solve the same issues that face every school in the country;
> - Schools can be advised as to where the boundaries of their "liabilities" are with relation to their duty of care (specifically relating to laptop provision and what their responsibilities are in managing these outside of the school's network);
> - Less money will be wasted on a "trial and error" approach of individual States and school bodies / schools tackling the issue in different ways;
> - Standards can be set to ensure that the rush of advisors, consultants and technology suppliers meet a set of pre-determined standards and deliver advice or solutions within the framework that may be agreed;
> - Specifically technology suppliers should be required to demonstrate referenceable capabilities in tackling Cyber Safety for children (see further recommendations below); and
> - Federal Government can provide common frameworks and support to State based and Independent and Catholic school bodies. This can include legal frameworks and communications tools to ensure adherence to the standards.[18]

19.26 Symantec Corporation emphasised that schools need 'qualified, independent advice and a blueprint to show best to address the issues'.[19] The importance of appropriate support in schools was discussed by the Australian Psychological Society:

---

18 Netbox Blue, *Submission 17*, p. 5.

19 Mr Craig Scroggie, Vice President and Managing Director, Asia Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, p. CS2.

> teachers are less confident in addressing cyber-bullying compared to other forms of bullying, and that "young people reported losing faith in reporting bullying behaviour because some teachers and other adults are not taking action or not recognising covert bullying as bullying when they see it or when it is reported, especially via cyber means". Staff training, positive classroom management, resources and support for development of appropriate strategies, principal commitment, and reconciliation/restorative techniques are all important as part of teacher engagement in cyber-safety.[20]

19.27 Schools could be encouraged to more easily adopt available solutions if there was a central body to:

- Provide advice and online collateral, papers, policies and best practice examples to schools;
- Research and establish a clear set of standards to be achieved by school to demonstrated their fulfilment of their duty of care and to provide reassurance to all stakeholders that the school is 'certified';
- Establish a national certification standard for schools (K to Year 12) across all sectors (Independent, Catholic and Public) in providing a cyber-safe environment for students;
- Promote the program to all schools and encourage them via grants or other appropriate incentives to benefit from adherence to the Standards;
- Then promote the program to all other stakeholders to provide reassurance that a National Standard is in place and that their school has (ideally) met the criteria; and
- Establish an ongoing review of the Standards and an annual re-accreditation to ensure ongoing compliance and communications to each new student intake.[21]

Effectiveness of education programs

19.28 Research into bullying and cyber-bullying appears to show that, although it is prevalent, it is not the behavioural 'norm'. Promoting socially

20 Australian Psychological Society, *Submission 90*, p. 18.

21 Netbox Blue, *Submission 17*, pp. 4-5.

acceptable behaviour is a more effective strategy than using scare tactics.[22] Quite often:

> presentations about cybersafety are quite scary and are very didactic, saying: 'This is what you shouldn't do; these are the risks.' It scares the parents and it scares the children. Engage parents about all the positive, wonderful things that their children can learn from technology but tell them about the normal things that you should do to keep yourself safe. It is really important how you engage children and parents.[23]

19.29 It was argued that there has been too much of a focus on technology and not enough on the decisions being made to enhance lives. A study in 2007 indicated that cyber-bullying is a behavioural problem, not a technological problem. Therefore, the Alannah and Madeline Foundation and other participants support the view that responses are best focused on behavioural change in the school and beyond.[24]

19.30 Inspire Foundation commented that:

> peer education and discussion oriented approach was particularly effective in engaging young people during the workshops. During formative/consultative discussions, young people expressed feeling that existing Internet Safety programs and resources were unrealistic, boring or 'talked down' to young people about risks that they were already very aware of ... One young person remarked that hearing their peers challenge attitudes and beliefs about online risks was much more credible than hearing about it from adults who she exclaimed 'don't know anything about what we do on the net'. The role of peer education in addressing cyber safety is therefore important in ensuring the measures advocated appear credible and reasonable in light of the integral role technology plays in young people's lives.[25]

Educational resources

19.31 Ms Robyn Treyvaud made the point that, in a web search for teacher resources for cyber-safety, there will be 3 million hits which makes it

22 Australian Parents' Council, *Submission 10*, p. 3.

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

24 Dr Julian Dooley, *Transcript of Evidence* 11 June 2010, p. CS5; Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS35; Alannah and Madeline Foundation, *Submission* 22, p. 19.

25 Inspire Foundation, *Submission 3*, pp. 9-10.

difficult to determine the most appropriate resource.[26] The Stride Foundation added that:

> We need to work with schools, young people, parents and industry. We need to get to everyone and we need to pull that together. We need to make it simple. Sometimes, particularly dealing with parents and teachers, it has become very complicated. If we create a simple message that everyone is following and endorsing then I really believe that we will get cultural change and we will reduce the incidence of the harmful effects of cybersafety in our schools and on young people.[27]

19.32 The Association of Principals of Catholic Secondary Schools highlighted the need for 'relevant authorities to develop high quality online updated educational resources for parents and teachers to access, so to keep pace with the ongoing rapid changes that are part of the online environment'.[28]

19.33 Ms Candice Jansz commented:

> The ability to access detailed resources on cyber-safety and any related Australian helplines or regulatory bodies via one comprehensive government-hosted online portal is strongly advisable, particularly for individuals who are not familiar with the internet and online social networks. A simple, well publicised web address, (i.e. Cybersafety.gov.au) would ensure it is easily remembered, and as such is accessed without difficulty when required.[29]

19.34 Dr Helen McGrath suggested that:

> it would be really good for the institutes of teaching, which set the criteria and standards for the teaching profession, to get together to discuss at some point whether or not cybersafety should be a mandatory aspect of preservice education.[30]

19.35 The *Australian Covert Bullying Prevalence Study* suggested the establishment of an Australian Council for Bullying Prevention, reporting to the Prime Minister and chaired by the Department of Education,

---

26 Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS32.

27 Miss Kelly Vennus, Program and Training Manager, Stride Foundation Ltd, *Transcript of Evidence*, 9 December 2011, p. CS18.

28 Association of Principals of Catholic Secondary Schools, *Submission 27*, p. 1.

29 Ms Candice Jansz, S*ubmission 44*, p. 7.

30 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS33.

Employment and Workplace Relations, to lead the review of the National Safe Schools Framework and the concurrent development of a strategy. Such a council could facilitate a 'sustainable joined-up-Government structures (including education, health, community development, and justice) and approaches to deliver key reforms'. It is more appropriate to utilise and existing governmental structure rather than to add another body to seek to improve cyber-safety in the online environment. In part, the proposal to create an online ombudsman was not supported for this reason, and because of concerns about jurisdictional issues.[31]

19.36 Roar Educate made the point that there needed to be a central repository of resources for teachers to address the current 'turf warfare'.[32]

Recommendation 29

That the Minister for Broadband, Communications and the Digital Economy facilitate a cooperative approach to ensure all material provided on cyber-safety programs is accessible through a central portal, and that a national education campaign be designed and implemented to publicise this portal, especially to young people.

Research

19.37 The need for more research-based evidence to improve cyber-safety for young people was repeated constantly during this Inquiry. It is 'imperative' that research be undertaken to provide a credible base for future policy, derived from Australian evidence rather than relying on international studies. There was 'a central role' for Government support for such research.[33] The Queensland Catholic Education Commission also considered that 'some sort of a clearing house would be very useful'.[34] The Australian Institute of Criminology argued that:

> there is a continuing need for national prevalence level research in Australia to determine the scope of the problem and, in particular, the impact on individual victims. Often the research does not

31 D Cross *et al*, 2009, *Australian Covert Bullying Prevalence Study*, May 2009, Child Health Promotion Research Centre, Edith Cowan University.

32 Mr Craig Dow Sainter, Managing Director, Roar Educate, *Transcript of Evidence*, 20 April 2011, p. CS26.

33 Internet Industry Association, *Submission 88*, p. 6.

34 Mr Michael Wilkinson, Executive Secretary, Queensland Catholic Education Commission, *Transcript of Evidence*, 17 March 2011, p. CS29.

> really investigate in a qualitative way the experience of the victims.[35]

19.38 The Australian University Cyberbullying Research Alliance suggested the:

> establishment of a national and international university cyberbullying research alliance for informing policy and sustainability in cyberbullying intervention.[36]

19.39 A concern was raised about current cyber-safety programs and initiatives, but that it is not clear how many of them have been appropriately evaluated and accredited.[37] Dr Julian Dooley believed that many existing cyber-safety programs are based on uncertain research.[38] The Australian Federal Police (AFP) added that:

> a number of issues that go to overall effectiveness. The fact is that many of the programs that do exist were developed quite quickly and although coordination and consultation was a consideration at the time there is perhaps more that can be done in relation to those aspects, and this should include scanning for best and better practices that would enable optimal use of finite resources and commitment. The AFP questions whether there is a sound base for determining longitudinal effectiveness and evidence of actual behavioural change. The AFP questions whether governments, law enforcement agencies and other stakeholder organisations and communities generally are making the necessary linkages between cybersafety and the wider suite of antisocial behaviours that confront society.[39]

19.40 Yahoo!7 also saw research as vital and a number one priority:

> We have a paucity of research in Australia about what risks Australian children are facing online and what measures Australian parents are taking to help manage those risks today. I actually believe that that research should be the foundation upon which an education program is developed, and I support Mr Scroggie's call for a mandatory curriculum around cybersafety. I think that that research would also inform the technological tools

35 Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS24.

36 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 22.

37 Australian Secondary Principal's Association, *Submission 33*, p. 3.

38 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS6.

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

> that are available and that are developed in response to that research.[40]

19.41 Internode also called for some perspective:

> There is really no sense of perspective on the challenge: a whole pile of threats are lumped on one end of the table with an equal rating or weighting and a whole pile of potential solutions are dumped on the other end of the table with no real assessment of whether they are going to be effective.[41]

19.42 It is inadequate only to address cyber-bullying, as any initiative must attack the overall issue of cyber-safety. To be effective, there must be global, long term, researched, funded national cyber-safety program, following from appropriate research. beyondblue suggested that research is needed to identify effective intervention strategies in relation to prevention and raising of awareness.[42] The Australian Secondary Principals' Association commented:

> There is currently an absence of systemic and ongoing survey data from this context, showing trends, successfulness of intervention programs, victim restoration and perpetrator rehabilitation. A shift in approach is needed to uncover the size and dimensions of the problem and how it changes over time. Such research will inform and direct prevention strategies.[43]

19.43 The *Australian Covert Bullying Prevalence Study* also called for the facilitation of:

> sustainable longitudinal research to investigate the developmental trajectory, causes, protective factors, social and economic costs, societal and cultural influences, and identify the windows of opportunity for bullying prevention and intervention.[44]

19.44 The Australian University Cyberbullying Research Alliance supported the need for:

> longitudinal, multi-disciplinary, cross cultural research into cyberbullying and cyber-safety practices be initiated and be

40 Ms Samantha Yorke, Legal Director, Yahoo!7 Australian and New Zealand, *Transcript of Evidence*, 8 July 2010, p. CS23.

41 Mr John Lindsay, General Manager, Regulatory and Corporate Affairs, Internode, *Transcript of Evidence*, 8 July 2010, p. CS6.

42 beyondblue, *Submission 5*, p. 3.

43 Australian Secondary Principal's Association, *Submission 33*, p. 3.

44 D Cross *et al*, 2009, *Australian Covert Bullying Prevalence Study*, May 2009, Child Health Promotion Research Centre, Edith Cowan University.

> ongoing to register changes in nature and prevalence across time, technological environments and location[45]

19.45 The *Australian Covert Bullying Prevalence Study* supported:

> applied intervention research to determine the impact of promising strategies to reduce bullying, including cyber bullying, that protect and support those involved, promote healthy relationships, reduce perpetration of bullying, and change the circumstances and conditions (individual, relationship, society, structural) that give rise to bullying.[46]

19.46 Further, beyondblue emphasised that there needs to be a system to:

> Develop, promote and share "what works" protective mechanisms and information for young people in easy to understand language and relevant mediums broad based and free to access, including through IT / social media i.e. via facebook, twitter, YouTube.[47]

19.47 Sexting is another area where further research is needed to understand motives behind this behaviour, and to develop effective intervention strategies to ensure that young people are aware of the potential legal sanctions.[48]

19.48 BoysTown raised the issue of research needed in relation to the lack of knowledge about the extent to which young people are targeted because of their religious or cultural backgrounds;

> how do Indigenous children and young people use this technology? We know they do use that; we know they use that for traditional purposes and cultural purposes. We want to look at the whole issue around help-seeking by Indigenous young people and how they use technology to do that. Again, it is an area that has not been studied much in Australia.[49]

19.49 These submission have highlight a broad range of research areas requiring further work, Further, the Australian Secondary Principals' Association called for a national centre for cybersafety:

---

45 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 11.

46 D Cross *et al*, *Australian Covert Bullying Prevalence Study*, May 2009, Child Health Promotion Research Centre, Edith Cowan University.

47 beyondblue, *Submission 5*, p. 3.

48 Ms Megan Price, Senior Research Officer, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS19.

49 Mr John Dalgleish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS19.

> there needs to be something where all this research is brought together. At the moment, for us in schools, when we want to teach students about cybersafety, we go to our local state department—state jurisdiction—or we go searching on the net ourselves or researching. For teachers that is very time consuming, and we find it very frustrating. If there was a one-stop shop, you might want to call it, for us to be able to go to where the research has been done, the data has been collated, there have been educational people involved in developing programs and lessons and things like that, that teachers could download and use as an integrated part of their curriculum that would be an enormous benefit for teachers, because we just simply do not have time.[50]

The role of the media

19.50 It has been suggested that some cyber-safety issues have been created and sustained by the media. The consequences of ignorance or lapses of security online can be devastating, and therefore newsworthy. In some cases, they can include loss of life, with all the tragedy that this means and the heartbreak that it causes to those close to victims.

19.51 Roar Educate believed that if bullying is still a problem, it is hardly surprising that cyber-bullying is an issue, but asserts that bullying of this kind is at least partly media-driven.[51] Cyber-bullying is one of the risks in the online environment that has received considerable publicity.

19.52 Ms Candice Jansz also referred to a 'most prominently, extensive and pervasive media coverage concentrating solely on the negative effects of the internet as a whole, and more recently, online social networks in particular.'[52]

19.53 The Youth Affairs Council of South Australia commented that:

> YACSA is also concerned with the often-hysterical tone taken by the media when reporting on cyber-safety issues. Such reporting can perpetuate the stereotype that young people are passive victims in the online environment, whereas anecdotal evidence

50 Mr Norm Fuller, President, Queensland Secondary Principals Association, *Transcript of Evidence*, 17 March 2011, p. CS71.

51 Roar Educate *Submission 100*, p. 6.

52 Ms Candice Jansz, S*ubmission 44*, p. 5

> suggests many young people are more technologically literate than their parents and other decision-makers.[53]

19.54 One young person expressed the view that:

> i believe cyber safety is getting worse when talked about it. Do you think it could stop being talked about on the news and advertised. Please many regards to make health and safety at ease. To stop this talk and make the world have better uses then cyber bullying and health and safety.[54]

19.55 The approach taken by media outlets can significantly affect the impact of these events on public attitudes and it is important that a knowledgeable and responsible approach is taken. An approach that may assist young people would be to advertise ACMA's *Cybersmart* website during news items relevant to cyber-safety, to enable young people experiencing difficulties to seek for the assistance they need. The Youth Affairs Council of South Australia suggested that while:

> it is difficult to say that there is scope for working with 'the media', but there is certainly scope to work with sympathetic media organisations to try to put across a view about these sorts of issues that is not hysterical and overly dramatic.[55]

19.56 Development of a kit informing media outlets of cyber-safety risks and general issues would provide authoritative information and, perhaps, go some way to reducing sensational reporting.

19.57 When cyber-safety stories are shown on television, it would be useful if a ribbon was added displaying the web address for the central portal containing information on cybersafety.

Media advertising campaign

19.58 Dr Helen McGrath suggested a campaign similar to the Quit anti-smoking campaign to reach parents/carers about cyber-safety[56]. ninemsn

53 Youth Affairs Council of South Australia, *Submission 25*, p. 2.

54 Tiger, *Submission 144*, p. 1.

55 Ms Anne Bainbridge, Executive Director, Youth Affairs Council of South Australia, *Transcript of Evidence*, 3 February 2011, p. CS30.

56 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS33.

suggested a campaign similar to 'Slip, Slop, Slap' on the importance of parental engagement with this issue.[57]

> The slip slap slop campaign was not saying that the sun is bad; slip slap slop was saying, 'When you are in the sun, you need to do this too.' It was a positive message. That, I think, is what the slip slap slop argument was: trying to reach at either level—parents or children—and spread a positive message in a catchy way for the target group.[58]

19.59 The Australian Secondary Principals' Association also supported:

> a major public campaign like we saw around some of the major public campaigns that we have had from the national government around things to do with sun safety and bits and pieces like that, would be of significant benefit in this.[59]

19.60 The ACT Council of P&C Associations recommended that:

> the government introduces effective advertisement that increases awareness among children of online risks. Parents have advised Council that they would like to see advertising used in a similar fashion as the current drink responsibly and speeding ads on television. In addition, schools and the government should use case studies to effectively illustrate what can happen if a young person does not effectively protect themselves online.[60]

19.61 The NSW Primary Principals' Association stated that the Australian Government:

> needs to address current cyber-safety threats through the media to ensure all citizens are informed about the dangers. Citizens also need to be made aware of the punishments associated with committing such offences.[61]

19.62 BraveHearts also called for a national television and radio campaign to raise awareness of Internet risks because there are now 45 percent of children accessing the Internet outside their homes.

---

57 Ms Jennifer Duxbury, Director, Compliance, Regulatory and Corporate Affairs, ninemsn, *Transcript of Evidence*, 21 March 2011, p. CS15.

58 Dr Roger Clarke, *Transcript of Evidence*, 21 March 2011, p. CS27.

59 Mr Norm Fuller, President, Queensland Secondary Principals Association, *Transcript of Evidence*, 17 March 2011, p. CS75.

60 ACT Council of P&C Associations, *Submission 41*, p. 10.

61 NSW Primary Principals' Association Inc, *Submission 69*, p. 3.

> We are confident that through quick infomercials, aimed at kids and adults, accurate and useful information delivered in a simple, easy to understand, engaging and informative way will work.[62]

19.63 BraveHearts drew a parallel with Mr John Schluter's environmental minutes, explaining that:

> where you get these great bits of information and this tiny little window that is 30 seconds or so where you go, 'Wow! I didn't know that.' If we could start feeding the general community little bits of information, just bite-sized chunks that they can consume without exposing how little they know, then we could start to empower both the parents and the kids, the general community, about an issue that they can discuss. I could see that absolutely starting a discussion around the lounge room between the parents and children saying, 'I didn't know that. Did you know that?'[63]

19.64 The Committee has already recommended the establishment of a central portal on which a range of cyber-safety material should be displayed. Once this is established, it will be a reference point, not least in media campaigns.

Industry cooperation

Reporting mechanisms

19.65 When problems occur, many users are not able to discover how problems can be resolved, or to whom they can complain. It is difficult to contact Facebook, although this may improve with the appointment of a representative in this country.

19.66 Simple measures can be taken which would assist users in the online environment, especially when they are seeking help or information.

62 BraveHearts, *Submission 34*, pp. 4-5.

63 Ms Hetty Johnston, Founder and Executive Director, BraveHearts, *Transcript of Evidence*, 17 March 2011, p. CS40.

Recommendation 30

That the Minister for Broadband, Communications and the Digital Economy encourages industry including the Internet Industry Association, to enhance the accessibility to assistance or complaints mechanisms on social networking sites; and develop a process that will allow people who have made complaints to receive prompt advice about actions that have been taken to resolve the matter, including the reasons why no action was taken.

Take down notices

19.67 The ACT Council of P&C Associations added that 'owners of websites' should be urged:

> to introduce additional safety measures to protect children. For example, while only the page creators on facebook can delete a post made by a member of a group, the government should pressure sites like facebook to automatically hide comments by users if there are a number of "dislikes". The government has limited power in relation to patrolling the internet and therefore it should take a moral stance rather than using funds to establish an online ombudsman whose role will be mostly ineffective.[64]

19.68 Dr Helen McGrath emphasised that:

> I would like to see some kind of seriously strong recommendation made that all of those service providers respond more rapidly to requests that are demonstrably genuine to remove content which is extremely distressing. They are very slow at the moment. If you are lucky, you might get it down in four weeks. [65]

19.69 The Australian Institute of Criminology commented that:

> Australia could seek to play a greater role in international co-operation on take down notices for child sexual abuse sites. A study by Cambridge University compared times taken to take down different forms of content. It was found that Phishing sites and sites which threaten banks' commercial interests are taken down very quickly. The child abuse sites are by contrast likely to stay up for many weeks due to the complexities of the fact that

64 ACT Council of P&C Associations, *Submission 41*, p. 12.

65 Dr Helen McGrath, Senior Lecturer, Faculty of Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS33.

> different jurisdictions do not work together effectively, and reports are routed via local law enforcement which may not prioritise the issue or be properly trained to deal with it.[66]

19.70 Evidence suggested that another area of concern was that, after lodging a request to have information taken down, all a complainant could do was to wait to see if the offending material disappeared. It is by no means certain that any notice will be taken of complaints. Once a page was removed, it was common that another page was quickly created containing similar material.

Recommendation 31

That the Minister for Broadband, Communications and the Digital Economy invite the Consultative Working Group on Cybersafety to negotiate protocols with overseas social networking sites to ensure that offensive material is taken down as soon as possible.

19.71 The complaints-based process of ACMA has received increased reports about online child abuse and child sexual abuse material hosted overseas. A more central focused approach would enhance the operation of current and future structures.

19.72 Because many of the offending sites are hosted overseas, they are not subject to Australian legislation. Thus, although it is not appropriate to make a recommendation in this area, the Committee believes that the sponsors of such sites should take note of and adhere to guidelines promulgated by ACMA.

Point of sale

19.73 It is important that adequate information is available to all those purchasing computers or mobile phones. The ACT Council of P&C Associations would like to see better service provision at the point of sale.

> The government should legislate for mobile phone providers to make it explicit for parents when signing new mobile phone contracts or allowing access to the iTunes store on a child's iPod that their child will have access to the internet on these devices.

66 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 93*, p. 5.

> Parents have indicated to Council that at times they have been unaware that their child was provided access to the internet on their mobile phone or iPod. While they may have signed a contract with service providers, the provision of internet was not made explicit. Council recommends that the government legislates that providers have an explicit, opt-in system, rather than opt-out for providing the internet on mobile phones for children 18 years or younger and that internet access for minors on mobile phones and iPods only be allowed with parental approval.[67]

19.74 In complaints to the Telecommunications Industry Ombudsman, some people referred to inadequate advice at the point of sale.[68]

Health and wellbeing

19.75 The Centre for Adolescent Health emphasised the positive impact of new technologies enabling young people to access advice on health and wellbeing:

> young people can be a bit wary of approaching professionals if they need help; however, the internet opens up a whole range of possibilities for them in terms of actually seeking help.[69]

19.76 The Australian Psychological Society agreed:

> They are also useful tools for specific kinds of young people. For example, young people with Asperger's syndrome or with social phobia, whose social lives face to face are perhaps a little more limited or more challenging, can use these tools to enhance their social connections.[70]

19.77 BoysTown noted that in situations where young people are in crisis the mobile phone may be the only avenue they have to seek assistance. It would like to see assistance with the cost of these calls to ensure that a lack of credit will not prevent a young person getting the assistance they seek.[71]

---

67 ACT Council of P&C Associations, *Submission 41*, p. 13.

68 Telecommunications Industry Ombudsman, *Submission 46*, p. 4.

69 Associate Professor Sheryl Hemphill, Senior Research Fellow, Murdoch Children's Research Institute, *Transcript of Evidence*, 9 December 2011, p. CS23.

70 Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS58.

71 Ms Tracy Adams, Chief Executive, BoysTown; Mr John Dalgleish, Manager, Strategy and Research BoysTown, *Transcript of Evidence*, 17 March 2011, pp. 11-12.

Prevention strategies

19.78 The appropriateness of educational strategies was often raised during this Inquiry:

> Indeed, Murray-Harvey and Slee (in preparation) found that strategies rated as effective by adults are not generally used by young people e.g. talk to a professional at school; use the school anti-bullying policy. Instead, young people prefer to use strategies rated as ineffective by experts: e.g. wishing for a miracle; hoping it will stop; taking it out on others; using drugs to feel better; pretend to be cheerful. Pre-service teachers in this study were advocating advice and strategies which young people do not use. This discrepancy is a problem that needs addressing.[72]

19.79 Roar Educate commented that:

> Technology is now available where students can be assessed against benchmarks for cyber-safety and the data base can be interrogated on a single student basis, an issue basis or professional development. This enable students who are not getting the message to be identified earlier ... The students are assessed against benchmarks. Their progress and results are reported to teachers, either in individual or aggregated format. It is reported to the parents to stimulate parent engagement about where their children are at and whether they are actually understanding the issues and responsible use. It also can be used by the principal to gauge not just where their school is at in terms of becoming the eSmart school, but also how many of their teachers and students have actually gone through this development.[73]

19.80 The assessment against benchmarks can also be reported to parents/carers:

> The holy grail that we are noticing in the UK is where the head teacher or principal in the UK of a government school is the legal entity; it is actually getting parents to take some responsibility. The vast majority of cyberincidents that actually take place take place using private or home based technologies, whether they be mobile

72 The Australian University Cyberbullying Research Alliance, *Submission 62*, p. 25.

73 Mr Craig Dow Sainter, Managing Director, Roar Educate, *Transcript of Evidence*, 20 April 2011, pp. CS19- 20.

> phones or the brother's, sister's, their own or their parents', computer in the house, yet the social connections are those made at the school.[74]

19.81 Another area of possible improvement is the acceptable use agreements. Netbox Blue called for:

> the creation of an up-to-date policy for all internet, social media and mobile device use, both inside and outside the school, needs to be implemented by each school. This must include clear consequences for inappropriate actions and it must be kept up to date and regularly communicated to all stakeholders, which obviously includes students, teachers, parents and carers.[75]

19.82 This also provides an opportunity for a nationally consistent approach.

Input from young people

19.83 As discussed in the previous chapter, it is paramount that the voice of young people be heard.

> That students and young people from diverse and inclusive communities be encouraged to actively contribute their voice to inform and shape policies and practices which are age-appropriate, concerning cyberbullying and cyber-safety strategies.[76]

19.84 To encourage input from young people, appropriate strategies need to be developed. One suggestion to learn more about the experience of young people was creation of:

> A practical education campaign where teens can see examples of the consequences that their actions may lead to. This could involve young people who have actually had to handle negative consequences from their actions online. A Facebook page or website could be created where teens describe the worst thing that has happened to them either because of mobile phone photos or social media postings. [77]

19.85 Another suggestions was:

---

74 Mr Craig Dow Sainter, Managing Director, Roar Educate, *Transcript of Evidence*, 20 April 2011, pp. CS21-22.

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

76 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 29.

77 Mr Nick Abrahams and Ms Ju Young Lee, *Submission 66*, p. 3.

> the creation of a list of short and memorable questions that teens should ask when being asked for personal information would also be useful e.g:
>
> - Why do you want it?
> - What are you going to do with it?[78]

19.86 A number of students participating in the Committee's *Are you safe?* survey explained the effect of having a police officer able to locate a young girl's address from the information of her profile in just four clicks. Students can benefit from practical demonstrations of the consequences of placing too much personal information online.

19.87 The Australian Psychological Society added that:

> In the light of young people being aware of emerging technologies (keeping pace with changes), and of their potential roles in witnessing and intervening in cyber-safety threats (such as cyber-bullying) among their peers, peer education and intervention programs should be developed and adequately resourced as a key part of any cyber-safety initiative.[79]

Seeking help online

Young people

19.88 Mr Stewart Healley suggested the establishment of a National Cyberbullying 24 hour/seven days per week Hotline.[80] This would complement the existing Cyber-safety Help Button. Kids Helpline also provides counselling service. One option is a possibility of directing these calls to an existing service such as Kids Helpline, provided that appropriate funding is provided.

19.89 BoysTown suggested that:

> The Australian Government could assist young people to identify credible online information by introducing a national accreditation scheme. Australian websites providing information on health and social issues impacting on children and young people could voluntarily seek accreditation with a National Board. Accredited

78 Mr Nick Abrahams and Ms Ju Young Lee, *Submission 66*, p. 3.

79 Australian Psychological Society, *Submission 90*, p. 3.

80 Mr Stewart Healley, *Submission 136*, p. 20.

> organisations would be recognised by a logo similar to that used by the Heart Foundation and similar organisations.[81]

19.90 It added that:

> following the introduction of a National Accreditation Scheme, the Australian Government instigates a communication and marketing campaign to promote awareness of accredited online services among young people and their parents/carers.[82]

Parents/carers

19.91 Parentline services are available in all Australian States and Territories which could assist in additional awareness promotion if adequately resourced. BoysTown therefore suggested that:

> the Australian Government enter into discussions with Parentlines to develop strategies that will increase their capacity to support parents and carers in relation to online risks that impact children and young people.[83]

Law enforcement

National cyber-crime coordination centre

19.92 Google Australian & New Zealand argued that there was a need for a national body to investigate, advocate and act on cyber-safety issues.

> Cooperation with law enforcement to combat child exploitation. Google cooperates with child safety investigations, and has a legal team devoted to this effort 24 hours a day, 7 days a week. We respond to thousands of law enforcement requests for assistance, and hundreds of subpoenas, each year. We also provide training and technical assistance to law enforcement officials investigating online crimes against children through forums such as the Internet Crimes Against Children National Conference and the Virtual Global Taskforce.[84]

19.93 The South Australian and the Western Australia Police drew attention the need for greater coordination of available resources between agencies to

81 BoysTown, *Submission 29*, p.16.
82 BoysTown, *Submission 29*, p.16.
83 BoysTown, *Submission 29*, p.17.
84 Google Australia & New Zealand, *Submission 13*, p. 3.

deal with cyber-safety issues. The WA Police referred to fragmentation of agencies across Australia, and within agencies themselves.[85]

19.94 The South Australian Police referred to international trends in cyber-crime:

> The United Kingdom, United States of America and New Zealand have implemented centralised cyber crime reporting facilities. The roll out of the National Broadband Network (NBN) and the imminent participation of Australia in the European Convention on Cybercrime provides a timely opportunity for Australia to improve the coordination of all cybercrime security and safety activities through establishing a National Cyber Crime Coordination Centre.[86]

19.95 It listed the possible features of such a cyber-crime centre, with units dealing with reporting, prevention and training, and one focusing on relations with offshore organisations. It would have to be funded by the Commonwealth, and amalgamate some services currently provided by State/Territory law enforcement, the AFP, ACMA, the Australian Crime Commission, the Tax Office and other Federal agencies.[87]

Timeliness of information

19.96 The timeliness of responses can sometimes be a problem. For example, evidence about child exploration needs to be quarantined and Facebook's quick response in taking down inappropriate material can actually impede investigations.[88] The Australian Institute of Criminology called for a review of the mutual legal assistance treaties relevant to transnational police investigations.[89]

19.97 The Committee also received evidence from a number of industry players on the difficulty of getting police assistance when they report significant incidents.[90] There is a need for greater cooperation, therefore, from law enforcement bodies.

85 Western Australia Police, *Supplementary Submission 78.1*, p. 1.

86 South Australia Police, *Supplementary Submission 86.1*, p. 2.

87 South Australia Police, *Supplementary Submission 86.1*, p. 3.

88 Commander Grant Edwards, Acting National Manager, High Tech Crime Operations, Australian Federal Police, *Transcript of Evidence*, 24 March 2011, p. CS7.

89 Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS9.

90 Mr John Lindsay, General Manager, Regulatory and Corporate Affairs, Internode, *Transcript of Evidence*, 8 July 2010, p. CS6; Ms Samantha Yorke, Legal Director, Yahoo!7, *Transcript of Evidence*, 8 July 2010, p. CS10.

Costs for law enforcement agencies

19.98 Costs imposed by service providers on law enforcement agencies requesting information about online accounts can make it difficult for investigations to proceed. Mr Stewart Healley suggested that the Australian Government:

> provide the necessary resources, support and funding to cover AFP and State Police for request of Account Details from Service Providers, who currently charge a substantial fee for requests by Police for Account Details in non life threatening incidents, under current Legislative conditions of "Cost Recovery" [91]

19.99 The AFP also drew attention to the costs involved:

> Legal mechanisms for compelling CSPs to remove content are limited, and are unlikely to succeed due to the costly and lengthy process involved. Even where a legal remedy was successful, it would likely be detrimental to the AFP's future relationships with that CSP where assistance of an even more critical nature is required.[92]

Recommendation 32

That the relevant Ministers in consultation with service providers consider how costs may be reduced for law enforcement agencies collecting evidence against online offenders.

19.100 Throughout this Inquiry, the Committee sought to understand better the views and concerns of young people in the online environment. Recommendations have addressed ways of involving parents/carers more effectively in promoting good cyber-ethics and practices. While industry and not-for-profit organisations have made significant contributions to cyber-safety for the whole community, there needs to be greater coordination of their efforts. Underpinning many Recommendations is the need for a cooperative national approach to all aspects of cyber-safety.

19.101 The Committee is confident that, if its Recommendations are adopted, the safety of young Australians when online can be improved, especially if their knowledge and capacities are harnessed.

---

91 Mr Stewart Healley, *Submission 136*, pp. 20-21.

92 Australian Federal Police, *Submission 64*, p. 19.

Senator Dana Wortley
Chair