
The Parliament of the Commonwealth of Australia

High-Wire Act Cyber-Safety and the Young

Interim Report

June 2011

Joint Select Committee on Cyber-Safety

© Commonwealth of Australia 2011

ISBN 978-0-642-79478-9 (Printed version)

ISBN 978-0-642-79479-6 (HTML version)

Cover image courtesy of Thinkstock



Contents

Foreword	xvii
Membership of the Committee	xx
Terms of reference	xxii
List of abbreviations	xxiv
List of recommendations	xxvi
Acknowledgments	xxxiii
PART 1 Introduction.....	1
1 Introduction	3
The online environment.....	3
Defining the online environment	7
Platforms.....	8
Access to the online environment	10
‘Cyber-safety’	12
Adult responses to cyber-safety issues.....	13
Australian Government responsibilities	15
State and Territory responsibilities	18
Current Parliamentary inquiries.....	19
Previous Parliamentary reports.....	19
Australian Law Reform Commission Inquiry.....	20
Joint Select Committee on Cyber-Safety	20

Conduct of the Inquiry	20
Overview of this Report	24
Part 1: Introduction	24
Part 2: Cyber-safety	24
Part 3: Educational strategies	24
Part 4: Enforcement	25
Part 5: Australian and international responses	25
Part 6: Conclusions	25
Results of the Inquiry	25
2 Young people in the online environment.....	27
Stakeholders.....	27
Real and virtual worlds.....	30
Entry to the online environment	31
Disadvantaged young people	36
Vulnerable young people	38
Young people with disabilities	39
Young Indigenous people in remote communities.....	39
Young people in regional areas.....	39
Privacy	40
Schools	40
Libraries.....	41
School libraries.....	42
Public libraries.....	44
Public libraries in NSW.....	45
Public libraries in the ACT	45
Consultation with young people.....	46
Youth Advisory Group	46
Committee’s consultations	48
Comments	50

PART 2 Cyber-Safety	55
3 Cyber-bullying	57
Definitions	57
Nexus with 'traditional' bullying	63
Some experiences	65
Causes and means	73
Prevalence	86
Impacts and implications	96
Coping strategies	100
Committee comments.....	117
4 Cyber-stalking, online grooming and sexting	119
Cyber-stalking	119
Genuineness of others online.....	122
Prevalence	123
Impact	127
Sanctions against cyber-stalking.....	129
Sexual grooming	129
Prevalence	132
Impact	134
Sanctions against sexual grooming.....	135
Research.....	135
Sexting	136
Prevalence	137
Impact	141
Sanctions against sexting	145
Research.....	145
Illegal and inappropriate content.....	146

5	Breaches of privacy and identity theft	149
	Introduction	149
	<i>Privacy Act 1988 (Cth)</i>	149
	Privacy and young people	151
	Identity theft	163
	Collection of unnecessary information	166
6	Other significant cyber-safety complexities	177
	'Technology addictions'	177
	Online gambling	180
	Violence	181
	Online promotion of inappropriate behaviours	182
	Online availability of alcohol	182
	Online availability of drugs	183
	Suicide	183
	Anorexia	184
	Committee views	185
7	The decision to post	187
	Information sharing, assessment of risk and the privacy of young people	187
	The Internet and identity	188
	Creating authentic identities online and offline	189
	Exploring identity	190
	What information do young people share?	192
	Types of information shared	192
	Are young people aware of online risks?	214
	How and why do young people decide what content to share online?	222
	Personality, identity and appreciation of risk	223
	Critical thinking and rational deduction	224
	Informal learning	225
	Formal learning	230
	Limiting online networks	231

Digital footprints	234
When fun isn't fun anymore: examining the complexities of photo sharing	238
Requesting the removal of photos.....	240
Conclusion	243
PART 3 Educational Strategies.....	245
8 Schools	247
Early cyber-safety education	247
Roles of schools	249
Duty of care.....	249
National Safe Schools Framework	252
Curriculums and programs	253
Partnerships with the Australian Communications and Media Authority.....	255
Technological approaches	256
Coordination.....	259
Committee views.....	261
9 Teachers.....	265
Professional development of teachers.....	265
Pre-service teacher education.....	267
Cyber-bullying of teachers	269
Mandatory reporting	273
Training accreditation.....	273
10 Whole-of-school community.....	275
Parents/carers	276
Information for parents/carers	281
Available technologies	286
Household media rules	290
Involving parents/carers	293
Conditions of use agreements.....	297
Parent advisory body	298

Peers	299
Concluding comments	300
PART 4 Enforcement.....	303
11 Legislative basis	305
Australian law and the online environment	305
Australian Government responsibilities	305
Attorney-General's Department.....	305
Australian Federal Police	308
State and Territory responsibilities	313
New South Wales.....	313
Victoria.....	313
South Australia.....	314
Western Australia.....	315
Tasmania	316
Sanctions against cyber-bullying	317
Sanctions against cyber-stalking	319
Sanctions against sexual grooming.....	321
Sanctions against sexting.....	322
Sanctions against illegal or inappropriate content	323
Promotion of suicide.....	323
Breaches of privacy and identity theft	324
Information requests	325
National accredited training	329
Role of industry.....	333
Concluding comments	334
12 Policing	339
Policing and justice	339
Criminalisation of online behaviour	339
Restorative justice programs.....	345
Intervention orders	347
Coordination.....	350

Legal risks	351
Feedback from young people	352
Concluding comments	354
13 An online ombudsman?	355
Role of an ombudsman	355
Support for an online ombudsman.....	358
Those opposing the establishment of an ombudsman	362
Other options.....	370
Those undecided.....	372
Conclusion	373
PART 5 Australian and International Responses.....	375
14 Australian responses to cyber-safety issues.....	377
Australian Government responses.....	377
Australian Communications and Media Authority.....	377
Department of Education, Employment and Workplace Relations	383
Attorney-General's Department.....	385
State and Territory Government responsibilities	385
New South Wales.....	386
Victoria	388
Queensland.....	390
South Australia.....	392
Western Australia.....	395
Tasmania	397
Northern Territory.....	399
The Australian Capital Territory.....	400
Non-government and industry responses	403
Australian organisations.....	403
Aboriginal initiatives	407
Australian ICT industry bodies	408
Marketing	413

15 International Responses to Cyber-Threats.....	415
United Kingdom	415
Task Force on Child Protection on the Internet	415
Child Exploitation and Online Protection Centre and <i>ThinkUKnow</i>	416
United Kingdom Council for Child Internet Safety	417
Education programs	417
Childnet International	418
United States	418
Online Safety and Technology Working Group	418
<i>NetCetera: Chatting with Kids About Being Online</i>	419
<i>Children's Agenda for Digital Opportunity</i>	420
<i>OnGuard Online</i>	420
Centre for Safe and Responsible Internet Use	420
Wired Safety resources	420
National Center for Missing and Exploited Children	421
<i>Cyber-safety.com</i>	421
Cybercitizen Awareness Program	422
Cybersmart!	422
Canada	422
Definetheline.ca	422
Internet 101	422
New Zealand	423
Netsafe	423
Leading international collaborations	423
Virtual Global Taskforce	424
<i>Council of Europe Convention on Cyber-Crime</i>	424
United Nations Crime Prevention and Criminal Justice Commission	425
The Australian/European Research Training School	425
Australia New Zealand Policing Advisory Agency	426
Australia's contributions	427

16	New technologies	429
	Safeguards	430
	Some solutions	431
	Family Friendly Filter	431
	Throttling bandwidth.....	432
	Central monitoring of access.....	432
	Australian Protected Network.....	432
	Industry advances	434
	Mobile phones.....	435
17	Proposal for a mandatory filtering system	441
	Background	441
	Support for the proposal	444
	Concerns about the proposal	446
	Other views.....	447
	Feedback from young Australians	449
	PART 6 Concluding Comments	451
18	Input from young people	453
	Getting the message right.....	459
	Appropriate educational materials	461
	Empower young people to better assist each other	464
	Peer education.....	466
	Crossing the inter-generational divide.....	467
	Inverting the teaching relationship.....	469
	Other suggestions	474
	Industry	474
	Site Administrators and Developers	475
	Technology	478
	Community.....	479
	Legislation and law enforcement.....	480

Tackling cyber-bullying	480
Education programs and awareness campaigns.....	480
Greater support networks.....	483
More actions by site administrators.....	484
Innovative suggestions.....	485
General comments.....	486
Conclusion	488
19 Conclusions	489
Centralised system	490
National cyber-safety education program.....	494
Effectiveness of education programs	496
The role of the media	503
Media advertising campaign.....	504
Industry cooperation	506
Point of sale	508
Prevention strategies	510
Seeking help online	512
Law enforcement.....	513

APPENDICES

Appendix A — Submissions	519
Appendix B — Exhibits	527
Appendix C — Witnesses	531
Appendix D — Survey Methodology	539
Sample	540
Content	540
Data analysis	541
Online Survey for 12 years and younger.....	541
Questions for 12 years and younger	542
Message on completed page	547
Online Survey for 13 years and older	548
Questions for 13 years and older	548
Message on completed page	555
Appendix E — Online Offences	557

LIST OF TABLES

Table 1.1	Number of survey respondents by gender and age	22
Table 3.1	In the last 12 months have you been directly involved in cyber-bullying?.....	81
Table 3.2	Of those that cyber-bullied another, have they also been targets of cyber-bullying by others?	82
Table 3.3	What are the main reasons why people cyber-bully?	84
Table 3.4	Is cyber-bullying increasing?	95
Table 3.5	If you were cyber-bullied in the last 12 months, what did you do?	102
Table 3.6a	If you were cyber-bullied, did you tell someone? <i>Aged 5-12 years</i>	105
Table 3.6b	If you were cyber-bullied in the last 12 months, who did you tell? (<i>Aged 13-18 years</i>).....	107
Table 4.1	Is repeatedly accessing someone's Facebook page stalking?	121
Table 4.2	Do you feel unsafe online?	124
Table 4.3	Do you send nude or semi-nude pictures?	140
Table 5.1	Have you explored the privacy settings on your social networking pages?	158
Table 7.1	Do you share your name online?	194
Table 7.2	Do you share your age or birthday online?	198
Table 7.3	Do you share your address online?	200
Table 7.4	Do you share your telephone number online?	201
Table 7.5	Do you post the name of your school online?	204
Table 7.6	Do you share your or your family's bank account details online?	205
Table 7.7	Do you share your holiday plans online?	208
Table 7.8	Do you share your email and passwords online?	210
Table 7.9	Do you post photos of others online?	212
Table 7.10	Do you think you are anonymous on line?.....	218
Table 10.1	How frequently does your family talk about cyber-safety?	279
Table 12.1	Proven Offences to 22 June 2010 of offences under the Code	340
Table 18.1	What can be done to make the online environment safer?	457

LIST OF FIGURES

Figure 1.1	Number of survey respondents by <i>gender and age</i>	22
Figure 1.2	Committee Chair, Senator Dana Wortley, during a small group discussion with students at McGregor State School.....	23
Figure 1.3	The Committee during discussions with students and teachers at McGregor State School.	23
Figure 3.1	Proportion (%) of those directly involved in cyber-bullying aged 13 years and over	82
Figure 3.2	Proportion (%) of those that cyber-bullied who have also been targets of cyber-bullying by others aged 13 years and over	83
Figure 3.3	Proportion (%) of those that have been the targets of cyber-bullying the past 12 months by age and gender.....	87
Figure 3.4	Proportion (%) witnessing cyber-bullying in the last 12 months by age and gender	88
Figure 3.5	If you were cyber-bullied, what did you do?	101
Figure 3.6a	Of those cyber-bullied, did they tell someone (<i>Female, aged 12 years and younger</i>).....	104
Figure 3.6b	Of those cyber-bullied, did they tell someone (<i>Male, aged 12 years and younger</i>)	104
Figure 3.7	If you were cyber-bullied in the last 12 months, who did you tell? (<i>Aged 13-18 years</i>).....	106
Figure 4.1	Is repeatedly accessing someone's Facebook page stalking? (<i>Aged 13 years and older</i>).....	120
Figure 4.2	Proportion (%) of those who have felt unsafe online (<i>Age and gender</i>)	124
Figure 4.3	Do you send nude or semi-nude photos? (<i>Age</i>).....	139
Figure 5.1	Have you explored the privacy settings of your social networking pages?	155
Figure 5.2a	Have you explored the privacy settings on your social networking pages? (<i>Female</i>).....	156
Figure 5.2b	Have you explored the privacy settings on your social networking pages? (<i>Male</i>).....	157
Figure 5.3a	Of those with privacy settings left at default, are they worried about their safety online? (<i>Female</i>)	159

Figure 5.3b	Of those with privacy settings left at default, are they worried about their safety online? (<i>Male</i>)	159
Figure 5.4	Of those with no privacy settings, have they felt unsafe online?	160
Figure 7.1	Do you share your name online? (<i>Age</i>).....	193
Figure 7.2	Do you share your age or birthday online? (<i>Age</i>).....	197
Figure 7.3	Do you share your address online? (<i>Age</i>).....	199
Figure 7.4	Do you share your telephone number online? (<i>Age</i>).....	201
Figure 7.5	Do you post the name of your school online? (<i>Age</i>).....	203
Figure 7.6	Do you share your or your family's bank details online? (<i>Age</i>).....	205
Figure 7.7	Do you share your holiday plans online? (<i>Age</i>).....	207
Figure 7.8	Do you share your email or passwords online? (<i>Age</i>).....	210
Figure 7.9	Do you post photos of others online? (<i>Age</i>).....	212
Figure 7.10	Do you think you are anonymous on line? (<i>Age and gender</i>).....	217
Figure 7.11a	Of those who believe they are anonymous online, do they feel safe? (<i>Female</i>)....	219
Figure 7.11b	Of those who believe they are anonymous online, do they feel safe? (<i>Male</i>).....	220
Figure 7.12a	Of those who believe they are anonymous, what is their level of concern about online risks? (<i>Aged 12 years and younger</i>).....	220
Figure 7.12b	Of those who believe they are anonymous, what is their level of concern about online risks? (<i>Aged 13 years and older</i>).....	221
Figure 7.13	Where did you learn about cyber-safety?	227
Figure 10.1	Where did you learn about cyber-safety?	277
Figure 10.2a	Do you talk about cyber-safety with your parents? (<i>Female aged 12 years and younger</i>).....	278
Figure 10.2b	Do you talk about cyber-safety with your parents? (<i>Male aged 12 years and younger</i>).....	278
Figure 10.3a	How frequently does your family talk about cyber-safety? (<i>Female aged 13 years and over</i>)	280
Figure 10.3b	How frequently does your family talk about cyber-safety? (<i>Male aged 13 years and over</i>).....	280
Figure 18.1	Can more be done to make the internet safer? (<i>Aged 13 and over</i>).....	456
Figure 18.2	What can be done to make the online environment safer?	457



Foreword

The online environment is an integral part of modern economic and social activities, and a vast resource of education, information, communication and entertainment. Further, the evolution of new technologies is diversifying the ways in which Australians connect with each other and the world.

As part of the Government's comprehensive commitment to cyber-safety, the Australian Parliament established this Committee in March 2010. This report focuses on how young people can be empowered and connect to the Internet, and use new technologies with confidence, knowing that they can use them safely, ethically and with full awareness of risks and benefits. The facilitation of safer online environments requires government, industry and the broader community to work together to realise the benefits of the online environment while also protecting Australians from dangers and enabling them to use existing and emerging tools to mitigate risks.

The Australian Government's ongoing commitment to consulting with the broad community on this issue is also demonstrated by the creation of the Youth Advisory Group and the more recent Teachers and Parents Advisory Group.

The Committee conducted three roundtables with industry, academics, law enforcement agencies, non-government organisations, parents and professional bodies and unions. Seven public hearings also contributed to the evidence received.

Consulting with young Australians was a key priority: understanding how they use technology, their awareness of risks, the strategies they use to alleviate dangers, and what they believe can be done to enhance safe and ethical engagement with new technologies.

Two online surveys of young Australians were also conducted by the committee: the first for young people up to the age of 12 and the second for 13-18 year olds. The surveys were completed by 33,751 young people. In addition, two school

forums were hosted so as to engage in a direct dialogue with these highly-connected young Australians.

The results of this consultation highlight the fact that younger generations not only hold the key to their own safety, but also that their knowledge and risk-management strategies are frequently undervalued. Young Australians have a wealth of experience with new technologies and are often more equipped to respond appropriately to online risks than is assumed.

Overwhelmingly, young people told us that the cyber-safety message needs to be age appropriate and suggested better ways to deliver the message and how it might be adapted. It is important that positive initiatives encourage young people to promote their own safety, and that of their peers.

There was also a clear message from young people that programs should seek to value existing knowledge and build upon this with appropriate and resourceful strategies.

The most significant points to emerge from the range of material received by this Inquiry include 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 need for research in many areas and, importantly, the need to assist parents/carers, teachers and all those who deal with young people to become more informed.

The myriad of stakeholders involved in promoting safer online environments requires innovative, collaborative solutions. Governments, industry, organisations, schools and parents all play crucial roles but they cannot operate in isolation from each other. Governments can play a leadership role and support the development of resources that are suitable for a diverse citizenry. Industry can ensure the safety of consumers, advance technological solutions and protections, and further drive their corporate social responsibilities. Schools are the key places to encourage young people to improve their own safety and online ethics.

The role that parents play in the cyber-safety education of their children also cannot be understated. Not only does the family play an important educative role, it plays an essential supportive role when young people face cyber-safety risks and dangers. In order to keep the lines of communication open with their children, it is vital that parents can assist their children with cyber-safety and cyber-ethics messages. To make this possible, parents need a strong awareness of the excellent resources available to them.


In concluding, I express appreciation to the Deputy Chair and my colleagues on the Committee. On behalf of the Committee, I also thank the Secretariat for their

dedication. I am grateful to all who provided submissions or appeared as witnesses, in particular the young people who took part in the forums and completed the online surveys. My thanks also to principals and teachers throughout Australia who encouraged widespread participation in the surveys.

Senator Dana Wortley
Chair

Committee Secretariat

Secretary	Mr James Catchpole
Inquiry Secretary	Ms Cheryl Scarlett
Research Officers	Mr Patrick Regan (from 10 January 2011) Mr Geoff Wells (to 23 December 2010) Ms Lauren Wilson
Administrative Officers	Ms Heidi Lushtinetz Ms Dorota Cooley (to 27 April 2011) Ms Michaela Whyte (from 28 April 2011)



Terms of reference

- (a) That a Joint Select Committee on Cyber-Safety be appointed to inquire into and report on:
 - (i) the online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles) and stakeholders controlling or able to influence that engagement (governments, parents, teachers, traders, internet service providers, content service providers);
 - (ii) the nature, prevalence, implications of and level of risk associated with cyber-safety threats, such as:
 - abuse of children online (cyber-bullying, cyber-stalking and sexual grooming);
 - exposure to illegal and inappropriate content;
 - inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking);
 - identity theft; and
 - breaches of privacy;
 - (iii) Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders, including business;
 - (iv) opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues;
 - (v) examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised;

- (vi) ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying including by:
 - increasing awareness of cyber-safety good practice;
 - encouraging schools to work with the broader school community, especially parents, to develop consistent, whole school approaches; and
 - analysing best practice approaches to training and professional development programs and resources that are available to enable school staff to effectively respond to cyber-bullying;
 - (vii) analysing information on achieving and continuing world’s best practice safeguards;
 - (viii) the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues; and
- (b) such other matters relating to cyber-safety referred by the Minister for Broadband, Communications and the Digital Economy or either House.



List of abbreviations

ABS	Australian Bureau of Statistics
ACARA	Australian Curriculum, Assessment and Reporting Authority
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ACPC	ANZPAA Child Protection Committee
AFP	Australian Federal Police
AISSA	Association of Independent Schools of South Australia
ANZPAA	Australian New Zealand Policing Advisory Agency
APN	Australian Protected Network
AYAC	Australian Youth Affairs Coalition
CDPP	Commonwealth Director of Public Prosecutions
CEOP	Child Exploitation and Online Protection
CPS	Content Service Provider
Cth	Commonwealth
CWG	Consultative Working Group on Cybersafety
DBCDE	Department of Broadband, Communication and the Digital Economy
DECS	(South Australian) Department of Education and Children's Services
DEEWR	(Commonwealth) Department of Education, Employment and Workplace Relations

EU20	European Social Networking Principles
FCC	Federal Communications Commission
FTC	Federal Trade Commission
ICT	Information and Communications Technology
IIA	Internet Industry Association
IP	Internet Profile
ISP(s)	Internet Service Provider(s)
JSSC	Joint Select Committee on Cyber-safety
MCEETYA	Ministerial Council for Employment, Education, Training and Youth Affairs
MCEECDYA	Ministerial Council of Education, Early Childhood Development and Youth Affairs ¹
NCS	National Classification Scheme
NTIA	National Telecommunications and Information Administration
NSSF	National Safe Schools Framework
OECD	Organisation for Economic Cooperation and Development
OCSET	Online Child Sexual Exploitation Taskforce
OSTWG	Online Safety and Technology Working Group
PIU	'Problematic Internet use'
SAGE-AU	System Administrators Guild of Australia
URL	Uniform Resource Locator
VGT	Virtual Global Taskforce
WWW	World wide web
YACSA	Youth Affairs Council South Australia
YAG	Youth Advisory Group
YAW-CRC	Cooperative Research Centre for Young People Technology and Wellbeing

1 This body has replaced MYCEETYA.



List of recommendations

PART 1 Introduction

1 Introduction

2 Young people in the online environment

Recommendation 1

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

PART 2 Cyber-Safety

3 Cyber-bullying

Recommendation 2

That the Minister for Broadband, Communications and the Digital Economy invite the Consultative Working Group on Cybersafety, in consultation with the Youth Advisory Group, to develop an agreed definition of cyber-bullying to be used by all Australian Government departments and agencies, and encourage its use nationally.

Recommendation 3

That the Minister for Broadband, Communications and the Digital Economy and the Minister for School Education, Early Childhood and Youth work with the Ministerial Council for Education, Early Childhood Development and Youth and the Australian Communications and Media Authority to investigate the feasibility of developing and introducing a cyber-safety student mentoring program in Australian schools.

5 Breaches of privacy and identity theft

Recommendation 4

That the Australian Government consider amending small business exemptions of the *Privacy Act 1988* (Cth) to ensure that small businesses which hold substantial quantities of personal information, or which transfer personal information offshore, are subject to the requirements of that Act.

Recommendation 5

That the Australian Privacy Commissioner undertake a review of those categories of small business with significant personal data holdings, and make recommendations to Government about expanding the categories of small business operators prescribed in regulations as subject to the *Privacy Act 1988* (Cth).

Recommendation 6

That the Office of the Privacy Commissioner examine the issue of consent in the online context and develop guidelines on the appropriate use of privacy consent forms for online services and the Australian Government seek their adoption by industry.

Recommendation 7

That the Australian Government amend the *Privacy Act 1988* (Cth) to provide that all Australian organisations which transfer personal information overseas, including small businesses, ensure that the information will be protected in a manner at least equivalent to the protections provided under Australia's privacy framework.

Recommendation 8

That the Office of Privacy Commissioner, in consultation with web browser developers, Internet service providers and the advertising industry, and in accordance with proposed amendments to the *Privacy Act 1988* (Cth), develop and impose a code which includes a 'Do Not Track' model following consultation with stakeholders.

Recommendation 9

That the Australian Government amend the *Privacy Act 1988* (Cth) to provide that an organisation has an Australian link if it collects information *from* Australia, thereby ensuring that information collected from Australia in the online context is protected by the *Privacy Act 1988* (Cth).

Recommendation 10

That the Australian Government amend the *Privacy Act 1988* (Cth) to require all Australian organisations that transfer personal information offshore are fully accountable for protecting the privacy of that information.

Recommendation 11

That the Australian Government consider the enforceability of provisions relating to the transfer of personal information offshore and, if necessary, strengthen the powers of the Australian Privacy Commissioner to enforce adequate protection of offshore data transfers.

Recommendation 12

That the Australian Government continue to work internationally, and particularly within our region, to develop strong privacy protections for Australians in the online context.

PART 3 Educational Strategies**8 Schools****Recommendation 13**

That the Attorney-General, as a matter of priority, work with State and Territory counterparts to develop a nationally consistent legislative approach to add certainty to the authority of schools to deal with incidents of inappropriate student behaviour to other students out of school hours.

Recommendation 14

That the Minister for School Education, Early Childhood and Youth propose to the Ministerial Council of Education, Early Childhood Development and Youth Affairs:

- to develop national core standards for cyber-safety education in schools,
- to adopt a national scheme to encourage all Australian schools to introduce 'Acceptable Use' Agreements governing access to the online environment by their students, together with the necessary supporting policies, and
- to encourage all Australian schools to familiarise students, teachers, and parents with the ThinkUknow program, and the Cyber-

Safety Help Button and other resources of the Australian Communications and Media Authority to promote the cyber-safety message.

Recommendation 15

That the Minister for School Education, Early Childhood and Youth and the Minister for Broadband, Communications and the Digital Economy consider extending the Australian Communications and Media Authority's *Connect-ED* program and other training programs to non-administration staff in Australian schools including school librarians, chaplains and counsellors.

9 Teachers

Recommendation 16

That the Minister for Tertiary Education, Skills, Jobs and Workplace Relations and the Minister for Broadband, Communications and the Digital Economy work together to ensure that sufficient funding is available to ensure the Australian Communications and Media Authority can provide the necessary training for professional development of Australian teachers.

Recommendation 17

That the Minister for Tertiary Education, Skills, Jobs and Workplace Relations and the Minister for Broadband, Communications and the Digital Economy encourage all Australian universities providing teacher training courses to ensure that cyber-safety material is incorporated in the core units in their curriculums.

Recommendation 18

That the Minister for School Education, Early Childhood and Youth establish a position similar to Queensland's 'reputation management' position to provide nationally consistent advice to teachers who are being cyber-bullied by students about the role and processes of the Australian Communications and Media Authority, law enforcement agencies and Internet service providers in facilitating the removal of inappropriate material.

Recommendation 19

That the Minister for School Education, Early Childhood and Youth and the Minister for Broadband, Communications and the Digital Economy investigate funding a national, online training program for teachers and students that addresses bullying and cyber-bullying, and is validated by national accreditation.

10 Whole-of-school community**Recommendation 20**

That the Minister for School Education, Early Childhood and Youth invite the Ministerial Council of Education, Early Childhood Development and Youth Affairs to formulate a cooperative national approach to the development of a whole-of-school community approach to cyber-safety, and to provide all schools with the necessary information and strategies to measure the effectiveness of their cyber-safety policies.

PART 4 Enforcement**11 Legislative basis****Recommendation 21**

That the Attorney-General work with State and Territory counterparts to invite all Australian Police Forces to develop a range of online courses to provide training in cyber-safety issues for all ranks, from basic training for recruits and in-service and refresher courses for more senior members.

Recommendation 22

That the Attorney-General work with State and Territory counterparts to initiate a mandatory training program for judicial officers and all relevant court staff addressing cyber-safety issues, to ensure they are aware of these issues, and of emerging technologies.

Recommendation 23

That the Attorney-General in conjunction with the National Working Group on Cybercrime undertake a review of legislation in Australian jurisdictions relating to cyber-safety crimes.

PART 5 Australian and International Responses

16 New technologies

Recommendation 24

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

Recommendation 25

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

Recommendation 26

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

PART 6 Concluding Comments

18 Input from young people

Recommendation 27

That the Minister for Broadband, Communications and the Digital Economy invite the Consultative Working Group on Cybersafety, in conjunction with the Youth Advisory Group, continue to advise Government on enhancing the effectiveness of cyber-safety awareness campaigns including targeted media campaigns and educational programs.

Recommendation 28

That the Minister for School Education, Early Childhood and Youth consult with the Minister for Broadband, Communications and the Digital Economy to develop measures to introduce:

- youth leadership courses enabling students to mentor their school communities about cyber-safety issues, and
- courses on cyber-safety issues for parents/carers and other adults are developed in consultation with young people and delivered by young people.

19 Conclusions

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.

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.

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.

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.



Acknowledgments

The Committee would like to express its appreciation to all those who participated in the inquiry by providing submissions, appearing as witnesses, participating in the survey and in other ways. In particular the Committee would also like to acknowledge the following for their assistance:

Ms Rosalind Bush for technical support for the survey

Ms Lisa McDonald for graphics for survey and cover design

Mr Greg Baker for statistical analysis

Mr Joe Italiano for survey video and advertising

The Principals who encouraged their students to participate in the survey

Ms Susan Phillips, Principal, and staff and students of McGregor State School

Mr Waikay Lau for photos of school forum in Brisbane

Students who participated in the school forum in Hobart from:

Calvin Secondary School

Cosgrove High School

Elizabeth College, Tasmanian Academy

Guilford Young College

MacKillop Catholic School

New Town High

Ogilvie High School

St Michael's Collegiate School

The Committee would also like to thank those organisations who assisted in advertising the youth survey through their newsletters, advertisements on webpages and social networking sites.

PART 1

Introduction

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 and 7 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

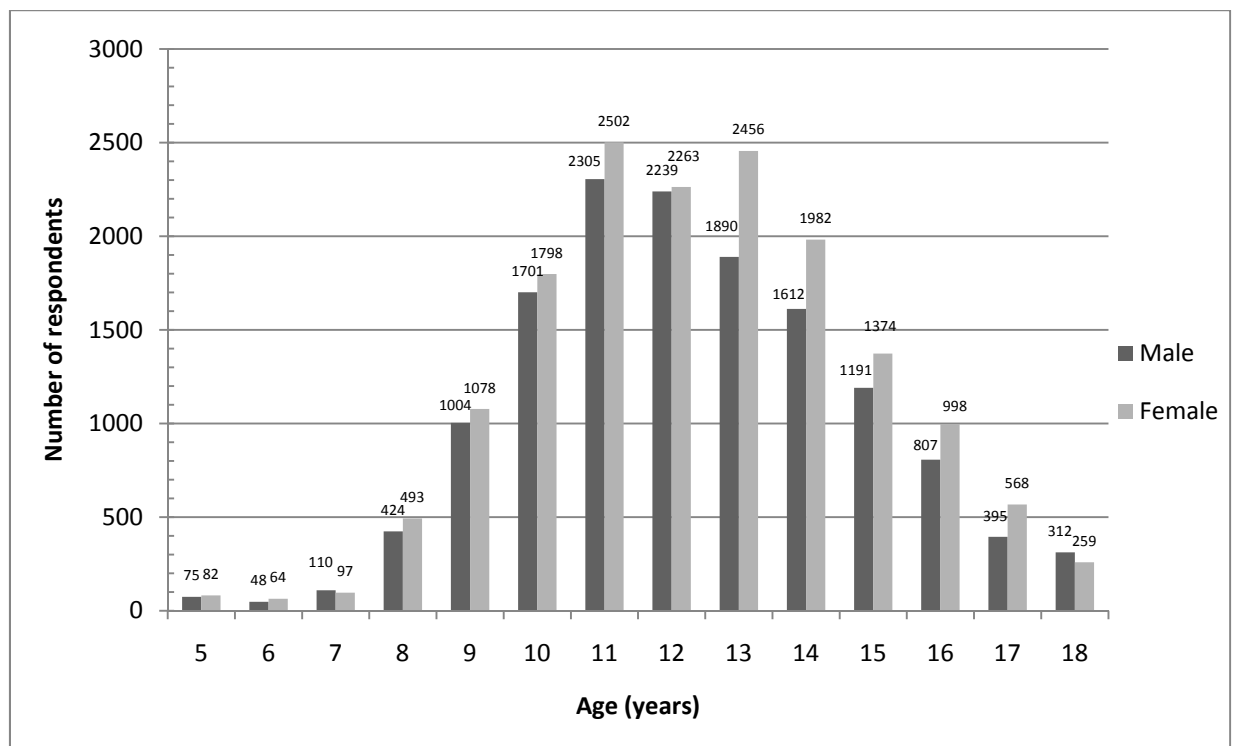


Figure 1.2 Committee Chair, Senator Dana Wortley, during a small group discussion with students at McGregor State School.



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/jsc.

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-

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.

Young people in the online environment

- 2.1 This chapter describes how the online environment impacts on young people in Australia. This will include entry to that environment, and the roles of schools and public libraries within it. It lists the various stakeholders who are able to have an impact on the online engagement of children and young people less than 18 years of age.
- 2.2 Most young people in Australia have regular access to this environment, and it plays an important role in their education, social connections and recreation.
- 2.3 Consulting with young Australians was a key priority for the Committee. It developed specific opportunities to capture the views of young Australians – a group that is otherwise unlikely to make formal submissions to a Parliamentary inquiry. Consultations included an online survey, a primary school visit and a high school forum. Interestingly, as a direct result of the survey and its school visits, the Committee began to receive submissions from young Australians.

Stakeholders

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

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

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

- parents/carers;
- Commonwealth, State and Territory Government agencies, particularly those with regulatory roles;
- schools and teachers;
- Internet service providers;
- content providers;
- public libraries;
- researchers; and
- traders.

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

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

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

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

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

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

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

- Those who are savvy, with the knowledge and skills to make good decisions about their online behaviour and know when to stop and withdraw;
- Those who are naïve with some skills, needing to be educated and 'topped up'; and
- Those who are vulnerable, having trouble at school or home, or both. When teenage angst comes into play and they disengage momentarily, they become vulnerable if they look for communities online with whom to engage. Young people with mental health problems, who are the most vulnerable, seek to belong online but lack the skills to disengage when they encounter inappropriate behaviour.⁶

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

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

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

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

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

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

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

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

- 2.12 Berry Street reported that for vulnerable young people:

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

Real and virtual worlds

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

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

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

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

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

- 2.14 They grew up in the online environment as ‘digital natives’ or ‘online natives’, rather than as the ‘digital immigrants’ of older generations. For such young people, the terms ‘online’ and ‘offline’ are differentiated only by other generations and where they straddle both worlds. Their involvement with that environment is an essential means to and part of their interactions with other people. In many cases, it seems that their parents/carers are unable to assist because they are busy, or not very interested in or knowledgeable about ‘technology’.¹³
- 2.15 In some circumstances, young people who are not able or willing to differentiate between the two worlds can be at even greater risk of harm in the online environment than their peers who are able to absorb warnings about safety and risks. Threats to cyber-safety now extend well beyond school gates to any Wi-Fi connected or home network.¹⁴ These treats can be significant because of the rapid rate of emerging new technologies.
- 2.16 Therefore, as part of their approach in the online environment young people need to exercise reasonable care and responsibility online. The key components of the necessary holistic response to cyber-safety should be based on ‘education, law enforcement, international cooperation, appropriate products and parental supervision’. A smart, ethical and socially aware online experience requires individuals to adopt responsible online behaviour and, to achieve this, it was suggested that effective education programs are needed.¹⁵

Entry to the online environment

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

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

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

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

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

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

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

- Pre-school children begin to learn how computers work. Their online activity may include visiting children's websites and communicating with family and friends through email;
- Primary school children feel more confident using other applications such as chat rooms. Some may search for prohibited material; and
- For high school children, the Internet is a necessity to assist with research for projects and homework. This age group seeks more freedom and independence in their use of the Internet, and they increasingly use the online environment as a social tool. These young people may also want to explore prohibited material.¹⁸

2.19 Research published by ACMA in 2007 indicated that 'first-use' of the Internet is at about five years old, but stated that there was anecdotal evidence suggesting that many children go online at progressively younger ages. Just under half of families are regularly involved with the Internet access of those six to ten years old. Earliest learning about the online environment can be through recreational activity, such as visiting the website associated with a favourite TV show.¹⁹ Cyber-safety education in schools usually does not begin until Year 2.²⁰ Professor Karen Vered added that:

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

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

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

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

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

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

Recommendation 1

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

- 2.20 The Alannah and Madeline Foundation noted that entry to the general online environment had changed considerably in the past few years. There are now approximately 2.2 million Australian children actively engaging online.²² Although ages do vary, it was suggested that Year 5 (ten or eleven years old) is the most common entry point into the social networking environment.²³
- 2.21 After very young children are introduced to computers, the use of mobile phones and other wireless devices follows. Once in this environment, there are many other places where access is available, including schools, public libraries, homes of friends, etc. Some will be unsupervised.²⁴
- 2.22 ACMA's research *Click and Connect: Young Australians' use of online social media* (2009) found that as children age they spend more time online:
- Children eight to nine years old use the Internet for an average of one hour, six minutes every two days;
 - Young people 16 to 17 years old average three hours, 30 minutes on the Internet every day;

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

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

23 Association of Independent Schools of SA, *Submission 19*, p. 8.

24 Childnet International, *Submission 18*, p. 1.

- Younger children are more interested in individual activities online, such as playing games; 83 percent of eight to 11 years old reported online gaming as the most popular use of the Internet; and
- By comparison, young people aged 12 to 17 use the Internet mainly for social interaction—81 percent of 12 to 17 years old nominated social networking services as their main reason for going online.²⁵

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

- Young people, aged 12 to 17, have a very high level of use of social networking services. Approximately 97 percent of 16 to 17 years old surveyed reported using at least one of these services, compared to 51 percent of children aged eight to 11 years.
- Fifty four percent of those 12 to 17 years old claim that ‘chatting to friends from school’ is their main reason for using social networking services. A survey conducted by the Australian Bureau of Statistics, *Children’s Participation* (2009), indicated that younger children used the phone primarily to contact family rather than friends.
- By comparison, only 17 percent of those 12 to 17 years old claim to use the Internet to ‘make new friends’.²⁶

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

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

- Sixty-one percent report accepting ‘friend requests’ from people they do not know offline.
- Seventy-eight percent claim to have personal information, such as a photograph of themselves, on their social networking profile pages, compared to 48 percent of eight to nine year olds.

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

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

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

- Seventeen percent of those 12 to 17 years old claim that one of their top three reasons for using social networking services is to 'make new friends'.
 - Conversely, use of privacy settings on profile pages appears to be greater amongst the older age groups.²⁸
- 2.25 The Australian Youth Affairs Coalition provided the following data:
- Young people use the Internet for an average of one hour and 17 minutes each day which includes:
- Almost 50 minutes of using the internet for messaging, visiting social websites and emailing,
 - 15 minutes for games online against other players, and
 - 13 minutes for homework on the computer and/or Internet.²⁹
- 2.26 Young people access the online environment by a variety of means, and therefore adequate frameworks must be in place to protect them from on-line threats as much as possible. Some of these places may not have the same level of controls as those at home or school. In particular, rules and supervision at friend's homes may be different to those in place at the child's own home.³⁰ Also in places such as Internet cafes or bookstores, restrictions to online access by young people may be vague or not enforced.
- 2.27 Government regulators have a role in providing information and programs about online risks. It seems that few young people or parents/carers go to the appropriate websites, so that they are often ignorant about both the risks and ways of avoiding them.³¹
- 2.28 While there is a great deal of material available about cyber-safety, many parents/carers are often not able to discern what is most valuable or useful. In addition, those who are likely not to engage with schools are likely to be the ones whose children are having problems with cyber-safety. For differing reasons, therefore, parents may not be able to attend sessions on cyber-safety when schools arrange them.³²

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

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

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

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

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

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

Disadvantaged young people

- 2.30 Some young people do not have access to computers in their home, or their access is severely limited. In addition, there are at least four specific groups whose access to the online environment is less than that of the great majority of their age groups. Lack of effective access makes it difficult for such children and adolescents to participate in the activities and social networking that are important to them, and undermines their ability to develop the skills they will need. Effective access is required if they are to develop into responsible, safe and resilient users of the online environment.³⁴
- 2.31 Assistance to such children is vital so that all young people can have the same opportunities online as their peers. There is little if any research about the numbers of young people who are disadvantaged, or degrees of disadvantage, in this environment. It is not clear how 'effective access' should be defined, or how such young people could be supported. It is therefore difficult to prescribe and implement effective plans to correct this situation.³⁵
- 2.32 The Victorian Child Safety Commission referred to effective access to include support for the child while using the technology enabling them to develop the skills to be responsible and resilient users of the technology:
- Lack of effective access to ICT makes it more difficult for children to participate in the activities and social networks that are important to children today and undermines their ability to develop the skills they require when they leave care.³⁶
- 2.33 It is clear, however, that those young people who engage in risky behaviour online often also engaged in risky offline behaviour. There is a pressing need for more research into the cyber-safety needs of the most

33 Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS66.

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

35 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 1.

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

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

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

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

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

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

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

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

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

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

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

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

- 2.37 Many of those responsible for young people in care have low levels of skills and 'extremely low' knowledge of technology, its uses and opportunities. Considerable work has therefore been done by Berry Street to build competence and confidence in those who already carry out complex jobs in looking after young people in care.⁴²
- 2.38 Vulnerable children are often unwittingly at heightened risk in spite of safety programs and extensive messages about unwise behaviour on the basis that most programs are targeted at mainstream audiences. It may therefore be a fundamental, though well-founded, error to approach cyber-safety without considering the wider spectrum of behavioural issues confronting our society. The Victorian Office of the Child Safety Commissioner commented that current cyber-safety strategies had not yet addressed the issue of keeping either group safe online.⁴³
- 2.39 There is 'relatively limited understanding' about the use of the online environment by disadvantaged young people, and growing concern that disparities in access, quality and skills would reinforce existing disparities in health and social outcomes. Of course, for some disadvantaged groups, the Internet has enabled freedom of expression and engagement where face-to-face contact is often difficult. This highlights the potential for new online technologies to create new processes of social inclusion.⁴⁴

Vulnerable young people

- 2.40 The Victorian Office of the Child Safety Commissioner drew attention to two groups of about 5,000 'vulnerable' children in Victoria:
- those who are in out-of-home care, removed from their parents because of abuse or neglect. The factors that make such children more vulnerable to abuse in the 'real' world also make them more vulnerable in the 'virtual' world. The level and type of their access to this environment can vary; and
 - those who have been identified as 'high risk' because of such factors as low satisfaction with their lives, sexual or physical abuse, poor family relationships or parental conflict. Some are living on the

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

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

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

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

Young people with disabilities

- 2.41 The Australian Communications Consumer Action Network noted that the 20 percent of Australians with a disability had particular circumstances requiring specialised tools and support to access the online environment. Such support was vital for disabled young people.⁴⁶
- 2.42 After a roundtable convened in June 2010 to discuss online issues effecting those with disabilities, the Network summarised its concerns:
- vulnerability;
 - barriers to confidence;
 - gaps in awareness, and
 - improved accessibility to websites.⁴⁷

Young Indigenous people in remote communities

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

Young people in regional areas

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

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

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

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

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

Privacy

- 2.45 Little is known about the attitudes of Australian young people to privacy. A recent American report suggested that children can see some online interactions as private, and were concerned about their parents/carers breaching that privacy.⁴⁹ Similar feedback was given during the Committee's High School Forum in Hobart.
- 2.46 Young people may have a limited capacity to assess the implications of divulging their own information, and therefore rely on others to ensure that their interests and safety are protected. The online environment is an area where they can be at risk, so that a breach of their privacy can be substantial, including trauma and identity theft.
- 2.47 The *Privacy Act 1988* (Cth) does not make special reference to young people, on the basis that they have the same rights to privacy as adults. In practice, primary care-givers would usually be responsible for exercising their rights under the Act until individuals reached levels of maturity and understanding to make independent decisions.⁵⁰
- 2.48 The complexity of the issue is highlighted by the argument that children and young people sometimes require protection from themselves.⁵¹
- 2.49 Privacy will be examined in more detail in Chapter 5, as part of the consideration of the threats to cyber-safety.

Schools

- 2.50 Specific cyber-safety programs and measures in some of the States and Territories are outlined in Chapter 14.
- 2.51 Schools are optimally placed to support students to be cyber-safe. Raising the awareness of young people before, or as, computers are introduced
-

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

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

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

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

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

- 2.52 Many schools have in place policies and filters provided by the local education authority. Schools with effective behaviour management systems, and vigilant supervision of student use of computers provide additional layers of support and protection. In many schools however, policies are not consistently followed by teachers, or are not widely known or understood by teachers, students or parents/carers.⁵³
- 2.53 The Alannah and Madeline Foundation suggested that Australian schools had ‘much ground’ to make up in producing ‘robust, acceptable’ policies reaching beyond their gates to include parents and the wider community.⁵⁴
- 2.54 The Australian Government’s provision of laptops for every student in Years 9 to 12 is intended to give unprecedented access, creating borderless classrooms and blurring boundaries between school and home.⁵⁵ The Government’s National Secondary School Computer Fund is helping schools to provide new computers and ensure that all students in these grades have access to facilities.

Libraries

- 2.55 The Australian Library and Information Association noted that libraries, especially school and public libraries, are key access points for the Internet for Australian children. They are an integrated, connected and collaborative network, and are therefore able to impact young people’s engagement online. The responsibilities of libraries to provide safe environments are taken very seriously, to the extent that user behaviour policies and other measures have been developed to increase online safety.⁵⁶
- 2.56 *The ALIA Internet access in public libraries survey 2008* found that there are separate internet terminals for use by children at 33 percent of responding

52 Association of Children’s Welfare Agencies, *Submission 35*, p. 3.

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

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

55 Alannah and Madeline Foundation, *Submission 22*, pp. 7-8.

56 Australian Library and Information Association, *Submission 16*, pp. 5- 6; Mrs Sue Hutley, Executive Director, Australian Library and Information Association, representing the Safer Internet Group, *Transcript of Evidence*, 8 July 2010, p. CS28.

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

School libraries

- 2.57 Outside classrooms, school libraries are the main location for the delivery of messages about the online environment. Library staffs are familiar with Internet-use policy and procedures at their schools, and with current information and research about safe online practices.
- 2.58 Teacher librarians are valuable and crucial partners in delivering important messages about these practices through teaching and learning programs. These focus specifically on digital information literacy development, including being literate across multiple areas within the ever-changing online environment.⁵⁹
- 2.59 These libraries are places of learning and discovery; safe and secure spaces for students that have Internet access. They have constant adult supervision and are only open when there is supervision. Further, school libraries play an important role in teaching students about
- Searching for, selection, analysis and creation of, material;
 - How to develop responsible cyber-safety behaviour;
 - Becoming aware of ethical practice;
 - The impact of their digital footprints; and
 - Good cyber behaviour habits for use after their formal learning finishes.⁶⁰
- 2.60 Teacher librarians are in central positions because they touch the lives of everyone in those school communities. They are therefore well-placed to support and deliver digital information literacy across all curriculum areas and age groups, including parents/carers.

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

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

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

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

- 2.61 While technology has changed them, libraries can also be sanctuaries: for some students, the safest places in their schools.
- 2.62 The Australian School Library Association believed that digital information literacy, of which cyber-safety is an integral part, is not being taught because of lack of training and professional development in either pre- or in-service professional training.
- 2.63 Being a responsible digital citizen requires appropriate, responsive behaviour with regard to the use of technology. A digital information literacy program in a school setting would focus on the following:
- Etiquette;
 - Effective communication;
 - Information literacy taught in the content of teaching and learning programs;
 - Equity of access and participation;
 - Social responsibility and ethical behaviour;
 - Collaboration and creativity in a safe environment;
 - Safe practices (e-safety and health safety);
 - Critical thinking and evaluation; and
 - Cultural and social awareness of the information environment.
- 2.64 The Australian School Library Association believed that the potential of teacher librarians to contribute to better outcomes for students within safe learning environments is untapped. As these personnel support all levels within a school, they are well-placed to integrate cyber-safety into digital information literacy programs and to provide professional learning for all of its teachers.
- 2.65 As a result of Building the Education Revolution, more than 3,000 new libraries have been built in primary schools. Most have been designed so that there is a movement away from the 'traditional' library environment. In many of them, there are trolleys allowing Netbooks to be moved around the library and connect to a wireless network, or plugged in to a direct connection. Such spaces are learning and information environments where students can use tools provided by the school or ones that they bring from their homes.
- 2.66 Where there are 'Acceptable Use' policies at schools, both students and their parents/carers are required to sign acknowledgement agreements.

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

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

Public libraries

- 2.68 There is a network of over 1,500 public libraries in Australia and they are community hubs, the hearts of their communities. This network is the key provider of safe and free access to information and services. These libraries are recognised as trusted, neutral and non-threatening spaces for individual or group social inclusion.⁶¹
- 2.69 While cyber-safety training is already being delivered at libraries around the country, for seniors as well as young people, the Australian Library and Information Association noted the need for more support to provide more training for staff in the use of the Internet and cyber-safety.⁶²
- 2.70 Since 2002, public libraries have continued to develop and improve Internet services for children. A survey in 2008 showed there were separate terminals for use by children at 33 percent of responding libraries, compared with 20 percent in 2005 and 16 percent in 2002. Websites linked to material especially recommended for young people increased to 56 percent (up from 52 and 47 percent respectively).⁶³
- 2.71 Parental consent is required for children to use the Internet by 77 percent of respondents, an 8 percent increase since 2005. While more than half the responding libraries require this consent to the age of 18, the youngest age where it is not required was eight years. Almost a third of responding libraries required parents to be present when children used the Internet, although the age to which this was required varied widely.

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

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

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

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

Public libraries in NSW

- 2.73 Public libraries across NSW provide free Internet access for the community. They form a critical element in community development, supporting life-long learning, literacy and education.
- 2.74 The *Library Act 1939* (NSW) guarantees everyone in the community access to libraries. All have conditions of use relating to public Internet access, and conditions of vary between local authorities. It is common for parents/carers to be required to give permission for children to use the Internet. The State Library provides free access, including by wireless, for laptops or PDAs. It recognised the privacy of users and did not monitor the information or sites accessed.
- 2.75 While young people are not formally supervised in NSW public libraries, there are guidelines for use of the online environment within them. The responsibility to supervise their young people remained at all times with parents/carers.⁶⁵

Public libraries in the ACT

- 2.76 Libraries ACT, formerly the ACT Library and Information Service, forms part of the network of public libraries in Australia.⁶⁶
- 2.77 The ACT Government provides free Internet access in its libraries, promoting community access to information. Community use is high, and a project has begun to provide wireless facilities in addition to desktop computers.
- 2.78 Users are required to accept an access policy before they use terminals, and an Internet blocking facility has been installed preventing access to sites identified in the Australian Communications and Media Authority's blacklist. Computers are in areas where there is a balance between privacy and supervision.

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

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

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

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

Consultation with young people

- 2.80 Sociologists have described young people as 'having been born into an age where they are unable to rely on anything, yet have incorporated this uncertainty into their lives [and exude] optimism and a sense of confidence.'⁶⁷ The optimism and confidence of young Australians in exploring, utilising and navigating new technologies is often over-looked.
- 2.81 As recent research confirms, young people are the most valuable resource in the development of cyber-safety awareness programs.⁶⁸ It is therefore vital that young people's perspectives are incorporated into the cyber-safety debate in ways that empower them and develop meaningful policies and programs.

Youth Advisory Group

- 2.82 The Youth Advisory Group was formed in 2009. It provides a forum where young people can talk directly to the Government about cyber-safety.⁶⁹
- 2.83 In its first year, it consisted of 304 secondary students from 15 schools across the country and provided advice on cyber-safety issues such as cyber-bullying, mobile phone safety, privacy and online computer games. This advice led to the announcement of two important initiatives: the Cybersafety Help Button and the Teachers' and Parents' Advisory Group on Cybersafety.

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

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

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

- 2.84 The expansion of ACMA's cyber-safety education, awareness-raising and counselling services was also informed by feedback from the Youth Advisory Group. The Authority's *Cybersmart* website and online helpline implemented a number of features consistent with initial advice from the Youth Advisory Group.
- 2.85 In 2010, the Youth Advisory Group was expanded to include 500 primary and secondary students aged from eight to 17 years, from 30 schools nationally. It provided advice through the *y@gonline* site and at face-to-face meetings, dealing with five main areas of concern: cyber-bullying, socialising online, scams and fraud, online games and digital citizenship.⁷⁰
- 2.86 A Consultative Working Group on Cybersafety and Youth Advisory Group summit was held in June 2010, where its members, parents and teachers provided views on a range of Government cyber-safety programs and initiatives. These included the Cybersafety Help Button and the Teachers' and Parents' Advisory Group, the *budd:e* cyber-security educational modules and the *ThinkuKnow* program administered by the Australian Federal Police.
- 2.87 A slightly different format will be used for the Youth Advisory Group in 2011. Ten one week consultation spheres are proposed, representing State/Territories, metropolitan and regional areas, Indigenous communities and National Broadband Network rollout sites. The Consultative Working Group is particularly interested to talk to schools near these rollout sites, to see how their students view the Network.⁷¹
- 2.88 Each sphere will include 100 to 200 primary or secondary students from between ten and 20 schools in a designated area or community. In total, there will be about 1,300 Youth Advisory Group members from about 130 schools.⁷²
- 2.89 The Youth Advisory Group has commented on the array of social networking sites and games, and the associated features and conditions. Before they can join a site or play a game, young people are confronted by long and detailed, usually legalistic material on the terms and conditions

70 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS22.

71 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS22.

72 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS22.

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

- 2.90 The Consultative Working Group on Cybersafety has taken very seriously advice that the Youth Advisory Group has given. It considered that this Group would be critical to further development of cyber-safety policy, and acknowledged that it will be essential that all stakeholders be responsive in considering the Group's advice.⁷⁴
- 2.91 One of the Working Group's members stated that involvement with the Youth Advisory Group had brought 'enormously valuable feedback'. There was a continuing need to analyse what adolescents actually said to each other on the Internet so that inappropriate behaviour could be detected.⁷⁵

Committee's consultations

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

73 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS22-23.

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

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

76 Rachel, *Submission 126*, p. 1

Are you safe? Survey of Australian youth

- 2.92 As noted above, the Committee launched its *Are you safe?* online survey on the National Action Day Against Bullying and Violence, 18 March 2011, at Macgregor State School in Brisbane. This survey closed on 6 May 2011.
- 2.93 It was completed by 33,751 respondents from around Australia, by children and young adults ranging from five years to 18 years of age. 18,159 respondents completed the 12 years and under survey; 15,592 respondents completed the 13 years and older survey.
- 2.94 The results and comments received by the Committee through the survey are discussed throughout this Report.

Primary school visit

- 2.95 On the National Action Day Against Bullying and Violence, Friday 18 March 2011, the Committee visited MacGregor State School in Brisbane to formally launch the *Are you safe?* survey. Its students were the first students to complete the survey.
- 2.96 Members of the Committee also led small group discussions with students. These groups then reported back to the Committee as a whole and in camera evidence was formally taken from these presentations.
- 2.97 Group discussions generated many useful insights, and some groups developed practical recommendations for their peers to protect personal information. Discussions centred on the following key topics:
- Anonymity and disclosure of personal information on the Internet;
 - Concerns about personal safety and avenues to seek help when feeling unsafe;
 - Targets, prevalence and motivations of cyber-bullying and avenues to seek help;
 - The success of current education programs and the degree of parental or guardians knowledge as a source of support and guidance; and
 - Specific recommendations on how Australians can increase their own cyber-safety, and initiatives that can reduce cyber-bullying in our communities.

High school forum

- 2.98 Hosted by the Tasmanian Parliament in Hobart, the Committee held a High School Forum on Wednesday, 20 April 2011. The forum allowed the Committee to hear substantively from young adults in an environment where participants told of their experiences online and offered their insights into how safety in the online environment can be enhanced.
- 2.99 The Committee invited 45 students from a mix of public and private, co-educational and single-sex high schools and colleges from around the Hobart region. Participating schools included:
- Ogilvie High School;
 - St Michaels Collegiate;
 - Tasmanian Academy - Elizabeth College;
 - Calvin Christian School;
 - Cosgrove High School;
 - New Town High School; and
 - Guildford Young College.
- 2.100 The structure of the forum allowed Committee members to ask questions or pose scenarios to participants that were then debated amongst the participants.

Comments

- 2.101 The holistic view of technology taken by many young people has implications for their safety in the online environment. As at June 2010, the Alannah and Madeline Foundation reported that more than 1.6 million young Australians had received cyber-safety lessons in the classroom, yet rates of cyber-bullying, 'sexting', identity theft, breaches of privacy and sexual exploitation continue to rise.⁷⁷
- 2.102 Roar Educate believed that fear has been a major driver of the national response to cyber-safety issues, supported by 'sensationalist media reporting' of incidents. This focused 'considerable attention' on the negative features of the online environment, rather than the many positive

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

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

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

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

- The online environment is generally a positive place for young people, so that the situation is not all bad;
- Strategies for dealing with face-to-face-bullying are also effective for cyber-bullying;
- There is still time in Australia to put strategies in place to prevent serious problems, but 'action should be taken now';
- Young people need to be involved in developing solutions, as their involvement means that measures undertaken are likely to be accepted;
- Cyber-bullying is a behavioural issue that needs to be dealt with by the wider community, not only by schools;
- It is important not to punish the victim by removing access to the online environment when cyber-bullying is reported; and
- State and Territory educational authorities need to pursue coordinated responses to this problem.⁸⁰

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

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

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

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

- Cyber-bullying;
 - Inappropriate handling of the individual's and others' private information;
 - Exposure to and creation of inappropriate content;
 - Computer gaming addictions; and
 - Sexual predation.⁸¹
- 2.105 The Mental Health Council of Australia noted research from 2009 into Cyber-Safety from the Child Health Promotion Research Centre at Edith Cowan University on five major risks for young people:
- Cyber-stalking, grooming and sexual solicitation;
 - Cyber-bullying;
 - Exposure to illegal and inappropriate material;
 - Promotion of inappropriate social and health behaviours and
 - Identity theft, privacy and online security.⁸²
- 2.106 The many ways of interacting in the online environment expose people to a wider public than is possible offline. Young people often post personal and identifying material without thinking, or perhaps even being aware, of, any possible consequences. For example, sexting can have long term consequences for an individual as a potential employee.⁸³
- 2.107 The range of risks confirms the concerns of organisations, such as the Queensland Catholic Education Commission, about the need for a clear definition of 'cyber-safety' and identification of the key issues, to deal with some of the myths surrounding the term. It believed that the concept of cyber-safety should be framed within the larger issue of student protection in general, reaching out to the responsibilities of peers, teachers, parents/carers and school authorities.⁸⁴ The Australian Youth Affairs Coalition emphasised the need to ensure that cyber-safety strategies address peer relationships.⁸⁵
- 2.108 The chapters in Part 2 describe a range of threats to cyber-safety, with responses and strategies addressed in subsequent sections. Chapter 3 focuses on cyber-bullying, Chapter 4 on cyber-stalking, online grooming

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

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

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

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

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

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

PART 2

Cyber-Safety

Cyber-bullying

- 3.1 This Chapter examines the need for an agreed definition of cyber-bullying, the nexus with 'traditional bullying', who is cyber-bullying and the experience of some young people, the causes and means, prevalence, impact and implications, and concludes with coping strategies and the role of bystanders.

Definitions

- 3.2 The Australian University Cyberbullying Research Alliance drew attention to the need for a clear definition that would assist international and Australian researchers.¹ The Australian Council for Educational Research noted that it is 'very hard' to define cyber-bullying.²

If you ever, as I do, ask young people to talk about cyberbullying they go, 'What? I have never been cyberbullied.' If you ask, 'Have you ever had rumours spread about you? Have you ever been excluded?' They go, 'Oh yes.' I say, 'Under this definition that would be considered bullying behaviour.' We have much to learn from them and they have much to learn from us.³

- 3.3 The Murdoch Children's Research Institute stated that research into cyber-bullying in Australia was limited by two important factors: 'the use of

1 Professor Phillip Slee, Australian Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS11.

2 Dr Paul Weldon, Research Fellow, Australian Council for Educational Research, *Transcript of Evidence* 9 December 2010, p. CS42.

3 Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS35.

inconsistent definitions and the lack of longitudinal data' on the factors influencing it.⁴

- 3.4 The Alannah and Madeline Foundation noted that there was little agreement about use of the term. Many websites referred to any negative online behaviour using it, without stressing its repeated nature.

Like the traditional definition of bullying, Cyber Bullying usually involves systemic communication over a period of time. A one off communication would not usually be considered cyber bullying. The only exception would be messages containing death threats or indication of serious intended harm.⁵

- 3.5 As it related to young people, an American expert defined cyber-bullying as:

any cyber-communication or publication posted or sent by a minor online, by instant message, e-mail, website, diary site, online profile, interactive game, handheld device, cell phone, game device, digital camera or video, webcam or use of any interactive device that is intended to frighten, embarrass, hurt, set up, cause harm to, extort or otherwise target another minor.⁶

- 3.6 Even if it was seen simply as 'bullying', students described and appeared to understand cyber-bullying as a set of discrete behaviours such as ignoring or excluding, threatening, rumours and bullying, carried through mobile phones via text messages, pictures sent, phone calls, email, chat rooms, social networking, games, blogs or through websites.⁷

While there is no doubt Cyber Bullying is a real issue an accurate prevalence is hard to measure due to the vague definition of bullying in student based studies. Often students, particularly younger ones, confuse a one-off incident with systemic bullying.⁸

- 3.7 The WA Education Department suggested cyber-bullying occurs when:

4 Murdoch Children's Research Institute, *Submission 111*, p. 2.

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

6 Mr Hugh Kingsley, *Submission 37*, p. 1 citing Parry Aftab, 2010, <http://aftab.com/index.php?page=cyberbullying>.

7 Alannah and Madeline Foundation: *Submission 22*, pp. 17-18; Dr Judith Slocombe, Chief Executive Officer, *Transcript of Evidence*, 11 June 2010, p. CS15.

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

an individual or group misuses information and communication technologies such as email, text messages, instant messaging and website to engage in bullying of other individuals or groups.⁹

- 3.8 The Mental Health Council of Australia provided another, shorter definition, from *cyberbullying.us*: 'wilful and repeated harm through the medium of electronic text'.¹⁰

One of the often unseen consequences of Cyber Bullying is that because the intimidation or bullying action is delivered via the written word then the target can read and therefore be affected by the same words again and again.¹¹

- 3.9 The Stride Foundation specified that cyber-bullying had to have a minor on both sides, or at least have been instigated by a minor against another minor. With the involvement of adults, it became cyber-stalking.¹²
- 3.10 The Attorney-General's Department defined cyber-bullying as bullying using the Internet, interactive and digital technologies or mobile phones.¹³
- 3.11 In this Report, the term will be used to indicate a sub-set of bullying, or covert bullying using technology: unprovoked, aggressive and intentional behaviour involving the abuse of power in relationships.¹⁴
- 3.12 Whatever definition is preferred, the Australian University Cyberbullying Research Alliance noted that 'cyber-bullying' was 'an adult and media-generated' term. While young people have come to understand it, it is not a term that they use.¹⁵
- 3.13 Some bullying, initially at least, is exploratory: what might be construed as bullying in very young children is often a way of expressing things and trying to understand how they relate to other children.¹⁶

9 WA Education Department, *Submission 115*, p. 1. See BoysTown, *Submission 29*, p. 8, for a similar definition.

10 Mental Health Council of Australia, *Submission 52*, p. 5. See safety.lovetoknow.com/index.php/title=Cyber-Bullying_Statistics Accessed 8 February 2011.

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

12 Stride Foundation, *Submission 6*, p. 13.

13 Attorney-General's Department, *Submission 58*, p. 3.

14 See Associate Professor Marilyn Campbell, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, pp. CS16-17; NSW Government, *Submission 94*, p. 7.

15 Australian University Cyberbullying Research Alliance, *Submission 62*, pp. 9, 13 citing Child Health Promotion Research Centre (September, 2009). *Cyber Friendly Student Solutions Workshop*, Perth, Australia.

16 Professor Philip Slee, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS12.

some young people that we spoke to admitted that they may have actually engaged in cyberbullying behaviour without knowing it, not fully understanding the implications of their actions. They identified that this was particularly the case when they could not actually see their victim in some way, so they felt like they would not necessarily understand the full impact of their behaviours online.¹⁷

- 3.14 Researchers at Simon Fraser University concluded that 'youth see negative exchanges as just a regular part of the online world and something to be tolerated'.¹⁸

What conduct is cyber-bullying?

- 3.15 The Committee's *Are you safe?* survey asked respondents over 13 years of age what activities constitute bullying. Through free-text spaces in that survey, it appears that young people have doubts about what amounts to cyber-bullying.
- 3.16 For example, when asked about their experiences with cyber-bullying, respondents made the following comments:

A disagreement turned into some mild name calling. Over facebook however, name calling is common (and largely un-hurtful) and I don't think that it should be the focus of prevention (Male aged 17)

Cyber bullying can be seen almost every week on social networking sites like facebook, but often the victims don't feel genuinely threatened. Outsiders often interpret things differently than they may actually be, seeing as: if they see acts of cruelty between friends that might actually be a personal joke, they'll think that it is bullying (Female aged 14)

There is a huge fuss over cyber-bullying. I have been an online gamer since I was 6, and cop crap every day from anonymous gamers, and I have no trouble with it, I just treat it as banter and ignore it. Although, inter school cyber-bullying is a totally different thing, and on a more serious level (especially as the bully and the victim know each other), it is quite overated. Calling names etc, is so easily blockable, and ignorable. however, when it gets to matters such as, embarrassing pictures of the victim being posted by the bully, that's when the police

17 Ms Georgie Ferrari, Chief Executive Office, Youth Affairs Council of Victoria, *Transcript of Evidence*, 11 June 2010, p. CS15.

18 Simon Fraser University, *Submission 55*, p. 14.

should be involved straight away. I really think people my age just need to grow up (Male aged 15)

cyber bullying is hard to explain/determine. what are the boundaries between simple friendly teasing and cyber bullying? schools/tv programs and the government need to broadcast what is and what is not acceptable on the internet (Female aged 15).

Cyber-bullying just depends on how people take it... Sometimes it goes too far and some people don't think of it as being taken too far as some other people tend to take it as just joking. How do you know when one takes it as a joke and someone else thinks it's an attack...? Cyber-bullying doesn't seem like it's that simple of a problem to resolve (Female aged 17).

I think most children who cyber-bully don't realise they are doing it, because it is hard to tell what tone something is written in for example "nice pic" could be being nice and giving a good comment or it could be sarcastic and be being mean and only the writer really knows which one, if they meant to be mean or if they were just being nice (Female aged 14).

- 3.17 This topic was also discussed in the Committee's High School Forum in Hobart. Young people are concerned that their communications may be misinterpreted or misunderstood by their peers or by adults. This is highlighted by the following dialogue:

Georgia- ... We all have friends on Facebook that would like to swear and make the jokes about the parents who cannot do that sort of thing. It is nothing to do with trust; it is to do with the fact that most of our friends are really immature and-

CHAIR-So it is a sort of harmless banter, is it?

Georgia-Yes. and it can be taken out of context if you are not reading it the right way. My mum has said a few things to a few of my friends about stuff that has been on my Facebook that has been taken way out of context.¹⁹

It depends on how certain teasing comments are taken. Some posts snowball as sometimes about a hundred people all contribute to a discussion which can sometimes include abuse of a person for the opinion they express. While I believe this is often innocent, if the person

19 Georgia, *Transcript of Evidence*, 20 April 2011, p 12.

was hurt then this would be cyber-bullying. This sort of behaviour is not uncommon (Female aged 17).

Someone made a facebook group and it was only an 'inside joke' (a joke which only people who are 'in on it' will understand). It was taken the wrong way by an unwitting and easily offended person and the person who created it was harrassed and labelled a cyber bully (Male aged 15).

3.18 The importance of context was raised later in the Forum with the following comments:

Georgia-There is also a very fine line between bullying and mucking around. I have a lot of friends who go to the Hobart campus at aye and we communicate through Facebook. Our relationships are based on bagging one another out. My mum has also taken that out of context and said things like, 'Please stop saying that to my daughter' when I had given it as much as I had taken it.

CHAIR-So it was not offensive to you? You were not concerned about it but your mother saw it and she thought it looked as though someone was having a go at you?

Georgia-Yes. Like what was said, you can see parts of the conversation or you can see where people have wished you happy birthday so you only get part of the text and not all of it.

Sally-In talking about taking things out of context on social networking sites, I think it is a big issue. Because it is done over the internet you are not actually talking face-to-face with people. Sometimes it is hard to know what was intended seriously and what was intended as a joke or as a friendly sort of jest, because you do not get the expressions and the tone of voice. Sometimes things can be taken in the wrong manner as to how they are intended.

CHAIR-Is there a way you can overcome that?

Sally-Of course, there are little smiles and symbols that symbolise what you are feeling, but I think that can occur without either party having a problem with that. It is not always exactly clear.

Amanda-I am just agreeing absolutely with what you are saying. Texting as well is incredibly tone deaf, so it is really hard to establish the exact tone in which people are implying what they are saying. Lots of things these days can contain hidden messages or innuendoes. It is really difficult to figure out what exactly is being said and how to take it.

- 3.19 Involving children and young people in defining cyber-bullying will not only enhance the relevance but also their ownership of the issue, and may increase the effectiveness of resulting policies to deal with it.²⁰

Recommendation 2

That the Minister for Broadband, Communications and the Digital Economy invite the Consultative Working Group on Cybersafety, in consultation with the Youth Advisory Group, to develop an agreed definition of cyber-bullying to be used by all Australian Government departments and agencies, and encourage its use nationally.

- 3.20 While it is 'a relatively new phenomenon', cyber-bullying is an important and serious issue. According to the Alannah and Madeline Foundation, it has been and remains 'the most pervasive form of serious risk faced by young people when they use technology'.²¹
- 3.21 Because the two abuses are so closely related, the more general topic of bullying will be addressed before cyber-bullying is explored.

Nexus with 'traditional' bullying

- 3.22 The Australian University Cyberbullying Research Alliance made the point that:

Bullying itself, is an age-old problem, but has morphed according to the times, the social mores and social context ... While much is now known about the nature, prevalence, and impact of conventional bullying that occurs 'offline' in school settings, research is only beginning to help us understand 'online' bullying and the overlap between the two.²²

- 3.23 BraveHearts believed that the same young people who are being harmed online are also being harmed offline, and by the same perpetrators. Cyber-

20 See comments by Australian Psychological Society, *Submission 90*, p. 19.

21 Alannah and Madeline Foundation, *Submission 22*, p. 17; See also Dr Gerald White, Principal Research Fellow, Australian Council of Educational Research, *Transcript of Evidence*, 9 December 2010, p. CS43; NSW Government, *Submission 94*, p. 7.

22 Australian University Cyberbullying Research Alliance, *Submission 62*, pp. 10-12.

safety is broader than bullying because it cuts across sexual grooming and accessing inappropriate information that used not to be available so easily.²³ Most young people who are involved in cyber-bullying are also involved in face-to-face bullying. It seems that about 80 percent of children who are victims of bullying, in both senses, online at home as well as at school. Those who are bullied, therefore, need support against both abuses.²⁴

- 3.24 The National Children's and Youth Law Centre provides a confidential advice and information service for children and young people.

The most common of the questions we have received relating to the Internet relate to bullying, usually bullying that began at school and is continued online.²⁵

- 3.25 Bullying is a subset of aggression and not a fight between equals.²⁶

It is very, very clear that most young people do not bully. Of those who do bully, sometimes when things are going bad in the home or when things are going bad at school they engage in bullying behaviours, but when things are not going bad they do not. So we do not call them bullies because that is an inappropriate label. Sometimes those kids who engage in bullying behaviours are actually calling out for help, and they need help.²⁷

- 3.26 By projecting their anger, anxiety or depression onto others, bullying is a way young people (and adults) attempt to deal with these problems. Other traits associated with this behaviour can include insecurity, low self esteem, victim status and disempowerment.²⁸

- 3.27 Bullying can lead to anxiety, depression, decreased self-worth, hopelessness and loneliness, all of which can be precursors to suicide and suicidal behaviour. The Mental Health Council of Australia referred to evidence of the strong relationship between traditional bullying and victims' ideas of suicide. It can affect victims vocationally, educationally,
-

23 Ms Hetty Johnston, Founder and Executive Director, BraveHearts, *Transcript of Evidence*, 17 March 2011, p. CS39.

24 Associate Professor Marilyn Campbell: School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS5; Australian University Cyberbullying Research Alliance, *Submission 62*, p. 12.

25 National Children's and Youth Law Centre, *Submission 138*, p. 4.

26 Associate Professor Marilyn Campbell, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS11.

27 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS21.

28 Mr Hugh Kingsley, *Submission 37*, pp. 1-2; Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS21.

emotionally, socially and developmentally. Significantly, it can also affect how young people seek help, and how they feel when help is available.²⁹

Some experiences

Jayne was a 14 year old student with a 'rather good view' on cyber-bullying. She/he had experience it first hand, as some friends had been subjected to it 'to the point of self-harm'. While there have been 'many cases' of cyber-bullying on the news, 'a lot' goes undetected. Although 'a few' police officers have been assigned to lecture at schools about appropriate online practices, she/he believed that there is a need for a greater police presence on the Internet.³⁰

A female respondent aged 14 said that, while she had not been cyber-bullied, it had upset one of her good friends: 'everyone supported her and stuck up for her'. While the bully had tried to apologise, that could not repair the damage done by the 'mean things' that had been said about the friend's personal life.³¹ Cyberbullying is not the problem, bullying is the problem. Cyberbullying is an extremely small part of a far greater whole, if someone is being cyberbullied I can guarantee you that they're being bullied in the traditional sense of the word. Everyone over the age of twenty five seems to forget that bullying still exists in the real world, and now assume it all takes place online. This could not be more wrong.

I have not been a victim of bullying since I moved to my current school in year nine (three and-a-bit years ago), but in years seven and eight I got bullied a lot. A group of kids would come up to me and hurl abuse at me, sometimes they got violent. All this time talk of "cyberbullying" was on the rise, and the problems of us regular victims got left behind. I was cyberbullied to an extent, sure, but this was not what concerned me. I did not dread coming home to an email from someone who hated me, I dreaded the prospect of going to school with someone who hated me and having those written words be spat at me before getting my jumper ripped off me and being put into some new and innovative choke hold.

In an email there's always a delete button, in an instant message there's always a block button, in a five on one fight behind the

29 NSW Government, *Submission 94*, p. 9; Mental Health Council of Australia, *Submission 52*, p. 5; Ms Michelle Noon, Program Manager, Youth, beyondblue, *Transcript of Evidence*, 9 December 2010, pp. CS1-2.

30 Jayme, *Submission 139*.

31 Abbie, *Submission 132*.

school building there's no such thing.

Please, put the focus back on preventing bullying as a whole, not looking through a microscope at the issue and running around condemning all online interaction which is what it feels like is often being done.

Please, I realise this program is designed specifically to help the youth achieve a safe online experience, but I haven't seen a single initiative (government or otherwise) to stop schoolyard bullying since mid primary school (9 years ago). In early high school there were no such things, and that's where my problems started. What's the use of a safe online experience if offline experiences are riddled with torment?³²

- 3.28 Significantly, young Australians who participated in the Committee's *Are you safe?* survey were keen to highlight that differentiating between bullying and cyber-bullying is not helpful or accurate. For example, the following comments were made in response to various questions throughout the survey:

Stop distinguishing between 'cyber' bullying and bullying in reality. It implies it is not real (Male aged 17).

Bullying is something unto itself: cyber bullying is not its own form; it's bullying just using another outlet. There's nothing special about cyber-bullying. We should be just as wary of it as normal bullying. The same way we need to know about safety just as much as cyber-safety. Adding the word 'cyber' doesn't make a negative activity any more important (with the exception of Cybermen) (Female aged 14).

Cyber bullying, I think is the most common form of bullying. Everything in this day in age is all about fights starting on facebook and people tend to feel more comfortable behind the keyboard instead of saying it face to face. I guess what im trying to say is that people need to realise what there saying on the internet. About themselves and others, i have lost a friend over bullying on facebook because of the threats she got, so she killed herself. This was and still is a very sad matter and ever since that has happen I think people should do something about bullying and tell us teenagers that there are other options (Female aged 14).

Cyberbullying is awfully hurtful, and even though these things are said

online, doesn't mean they aren't affecting people in the real world. Cyber World DOES meet with the Real World (Female aged 13).

I think cyber-bullying is simply an extension of regular bullying and that the fundamental issue that must be solved is not rooted in the technology but social interactions. Although, young people should be aware of their safety while on the internet (Female aged 17).

Cyber bullying, from what I've seen, is exactly the same as bullying in real life, just online. The main provocations are 'different' people, and the only way I can think of to reduce it is to educate younger people that there's nothing wrong with any 'different' groups of people (Female aged 14).

i personally don't see the difference between bullying and cyber bullying, cyber bullying is just directed through a different outlet. with this in mind you will never fully stop bullying so why treat cyber bullying any different (Female aged 14).

Weirdly enough, the government seems to have this idea that cyber bullying is somehow different from normal bullying. It isn't, it's fundamentally the same thing, teasing, harassing, etc, except it is aided by the constant accessibility provided by electronic media., and "staying safe online" has nothing to do whether you'll be bullied or not. As always, people will bully and there will be people who are bullied, the only way to stop that would be to make people realise the ramifications of their actions, even though there will be some people who won't care regardless, but there's not much you can do to stop that (Male aged 17).

- 3.29 The online component of bullying adds a significant factor in terms of depressive symptoms.³³ A major difference between cyber-bullying and offline bullying is that it may have no respite, as it occurs at any time and can be difficult for parents/carers to detect.³⁴

The always-on nature of modern communication means that the child can be bullied 24x7 without regard to where they are or what they're doing. There is no safe-haven, no let-up, no relief, no way to escape. The child can't read their email, contact their social

33 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS15.

34 Australian Parents Council, *Submission 10*, p. 3. See also Australian Education Union, *Submission 11*, p. 2.

networks, or read the text messages on their mobile phone without letting the bullies into their lives.³⁵

- 3.30 Mr Nick Abrahams and Ms Ju Young Lee believed that cyber-bullying spilt over naturally from the school playground, and that it gained a further dimension once mobile phones became easily available to young people.³⁶ In a final free text space, the following comment was submitted:

Cyberbullying is really bad because there is no escape. Yes, bullying at school is horrible but at least it stays at school. Cyberbullying follows you everywhere and is at home, the one place your meant to feel safe. There needs to be more information on how to prevent or stop it (Female aged 14).

- 3.31 Cyber-bullying has all the features of bullying, with the additional feature of deliberate, covert misuse of the online environment that makes attacks quicker and easier. The NSW Government noted that research into cyber-bullying is in its infancy. Some studies suggest that it may be more harmful for young people than traditional bullying because it is covert. Harmful messages can also potentially be received by many people, and they can be re-read many times by the victim.³⁷

- people who are bullied have no place to hide, and can be targeted anytime and anyplace;
- cyber-bullying can involve a very wide audience;
- people who bully are relatively protected by the anonymity of electronic forms of contact, which can safeguard them from consequences or retaliation; and
- people who bully do not usually see the response of the victim, changing the satisfactions or inhibitions normally generated by bullying.³⁸

- 3.32 It is possibly the most insidious form of bullying identified to date, and its key elements are:

- Imbalance and misuse of power;
- Repetition;

35 Mr Mark Newton, *Submission 15*, p. 6.

36 Mr Nick Abrahams and Ms Ju Young Lee, *Submission 66*, pp. 2-3.

37 NSW Government, *Submission 94*, pp. 7-8.

38 NSW Government, *Submission 94*, p. 7.

- Deliberate
- Intention to change power status; and
- Lack of empathy.³⁹

3.33 Dr Helen McGrath commented that:

In the long term, you would predict that the results could be at least as bad as face-to-face bullying and possibly worse because we do have some suggestions from the research that those kids who contemplate cyberbullying probably see it as being much more devastating even than other forms of overt and covert bullying. This is because of the fact that their victim does not know who it is because they can have multiple email sites, multiple ways of targeting them.⁴⁰

3.34 The Association of Children's Welfare Agencies noted that cyber-bullying is pervasive and not usually a one-time communication. It can present itself in many forms and can have many sources, limited only by the perpetrator's imagination and access to technology.⁴¹ The cyber-bully one moment may be a victim the next.⁴² It is often those on the receiving end of bullying who will retaliate from behind closed doors, or from the safety of a mobile phone, without fear of exposure.⁴³

3.35 Direct and indirect forms of cyber-bullying may include:

- direct harassment or intimidation;
- publication of malicious content;
- systems or technology attack, including hacking or intrusion of computer viruses;
- manipulation of systems to exclude an individual; and
- false impersonation to defame or misrepresent.⁴⁴

3.36 Common types of cyber-bullying behaviour include:

- text-based name-calling, use of coarse language, profanity and personal attacks (many examples involve racism, sexism, as well as other types of prejudice);

39 Mr Hugh Kingsley, *Submission 37*, pp. 1-2.

40 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS8.

41 Association of Children's Welfare Agencies, *Submission 35*, p. 2.

42 Stride Foundation, *Submission 6*, p. 13.

43 Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS11.

44 Association of Children's Welfare Agencies, *Submission 35*, p. 2.

- “flaming” (overt attacks on a person), harassment or denigration (put-downs);
- cyber-stalking (use of the Internet to “stalk” or threaten);
- using masquerade, trickery and exclusion;
- “outing” (publicising that someone is gay); and
- sending out humiliating photo or video messages, including visual pornography and sharing videos of physical attacks on individuals (sometimes called “happy slapping”).⁴⁵

3.37 The *Australian Covert Cyber-bullying Prevalence Study* found that the ‘strategies undertaken to cyber bully change with age in developmental association to the uses of, interests in and availability of technology’.⁴⁶

Cyberbullying arose in the context of covert bullying in this study, yet is neither uniquely *covert* nor *overt* in its execution. Where the goal is to be circuitous, cyberbullying is secretive, hidden and concealed. Where the goal is to raise status and gain infamy, then it is open and deliberate.⁴⁷

3.38 This abuse of the online environment can be perpetrated from peer-to-peer, adult-to-child, involve groups and unknowing third parties.⁴⁸ Peer-to-peer abuse may involve ‘the most harmful material’.⁴⁹

3.39 Cyber-bullying is made easier once a young adult makes herself/himself vulnerable by, for example, by posting or sending inappropriate photos to others, by writing personal blogs, or by posting personal photos on Facebook. This can result from peer pressure, or from ignorance of potential consequences.⁵⁰

Reputation and status amongst peer group relationships with friends is vitally important and covert and cyber bullying are weapons in the repertoire which enable manipulation of reputation; denigration or elevation of status and stalking⁵¹

3.40 BoysTown found that ‘the most prevalent forms of cyberbullying were name calling (80 percent), abusive comments (67 percent) and spreading rumours (66 percent). While name calling showed little difference by age

45 Australian Institute of Family Studies, *Submission 39*, p. 3.

46 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 16 citing Cross *et al*, 2009, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre.

47 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 20.

48 Association of Children’s Welfare Agencies, *Submission 35*, p. 2.

49 Mrs Sue Hutley, Executive Director, Australian Library and Information Association, representing the Safer Internet Group, *Transcript of Evidence*, 8 July 2010, p. CS11.

50 Mr Nick Abrahams and Ms Ju Young Lee, *Submission 66*, p. 2.

51 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 19

or gender, abusive comments were found to be significantly more common among victims aged 15-16 years'.⁵²

- 3.41 The following comments were made by young Australians who participated in the *Are you safe?* survey. The comments were made in response to questions about witnessing bullying online:

people harass each other and get involved in issues that their friends have and end up threatening or fighting people because they took their friends issues to the heart. and people post comments about other students intentionally so they can see what they are writing, constant nagging (Female aged 14).

A girl at my old school cyber bullied a dark skinned girl and got five other friends to join in and post racist photo's, drawings and comments about her so that her facebook wall was full of them. She even got threats asking her to leave the school (Female aged 13).

On formspring, a site that enables you to post anonymous comments, I have seen quite a few rude and mean things said to people I know, often repeatedly. (Female aged 14).

I think the main problem or reason that cyber bullying seems to be increasing is that most young people are unaware that cyber bullying can be as serious/harmful as face-to-face bullying. It seems that many people are willing to post a nasty comment online, often people who would never dream of saying the same to a person's face. Young people need to be made aware that cyber bullying is just the same and can have the same disastrous consequences as other bullying forms. There is also the issue of anonymity, where bullies believe they cannot be traced and are therefore able to say whatever they wish. Ensuring young people are aware that police or other authorities have full access to internet history and the ability to track internet use I think would reduce the number of people willing to bully on the internet (Female aged 17).

Comments about a bunch of immature people in a year level. Done in retaliation or annoyance. Not written maliciously, but not particularly subtle either. I am mentioning this because it was a number of people making these comments or liking these status's. It wasn't a hate campaign (Female aged 18).

During a fight between friends, someone got their facebook account hacked and altered. She shouldn't have given her password to her

⁵² BoysTown, *Submission 29*, p. 8.

friend, especially because they fought and that was the result of trusting someone (Female aged 16).

Girls didn't get along at school, attacking each other on the internet through facebook making rude comments and suggestions to each other on facebook e-mail, meaning that I got the messages, being sent to multiple people. I watched it all unfold, but being at a separate school to them at the time I was not heavily involved, I received the e-mails. The school was notified by the girls parents and the e-mails were shown and the situation was sorted (Female aged 14).

It's pure stupidity. They make rumours and comments that are utterly pointless. They only do this to seem superior on the internet, because they've never had the guts to say those things in real life (Female aged 15).

Name calling amongst girls in lower grades of high school. Social networking-attacking pictures, clothing, character of the person, actions the person has done, embarrassing stories, threats to the person and their family. It was done in a group with all members participating. From what I could tell there were three girls on each side attacking one another (Female aged 16).

Silly rumours or arguments of the junior years seem so immature... The seniors have definitely experienced it when they were juniors but bullying and foul-mouthing other kids just seems so common and re-occurring... It's like the domino effect... Involvement in situations with boyfriends, girlfriends, trying to get friends and 'groupies' to gang up on them and start a fist fight outside the internet..... (Female aged 17).

3.42 Similarly, during the Committee's High School Forum, Amanda commented:

A lot of stuff that happens over the internet escalates very quickly because you are not face to face with the person. It gets out of hand because you are not dealing with it immediately; you are just saying words. and I do not think you fully understand the implications, impacts and consequences of what you are saying. It is really difficult if someone does actually threaten you on Facebook. I do not know if there is a procedure on Facebook for dealing with that.⁵³

- 3.43 More specific comments were submitted in the *Are you safe?* survey that specifically discussed the site *Formspring*. When asked about how often they witness bullying online, the following comments were made:

A lot [of cyber-bullying] is centred around FORMSPRINGS. i think that site should be perminatly BLOCKED in australia, because i can't think of one thing that is good about it but at least 5 of my friends have had their last 3 years wrecked by it (Female aged 15).

A site called Formspring has been around for quite a while, and opens up the opportunity for anonymous questions to be asked to people. However the people creating these accounts are very much aware that sometimes they will receive the cruel question/comment (Female aged 15).

It involved the facebook & formspring websites. My friend was asked nasty questions on her formspring page about whether she had brain damage, her being adopted and about her and her boyfriend. She also received mean comments on her facebook page. This was all done by girls in her grade at school (Female aged 16).

- 3.44 In response to the same question, comments were also made about keyboard-warriors:

Fights between people escalated because they were 'keyboard warrioring'. People gang up on other people so they seem cool to their friends (Female aged 17).

The bullies themselves are what we call 'keyboard warriors'. They will repeatedly bully you online, but when push comes to shove, they will say nothing in real life (Female aged 14).

Causes and means

- 3.45 There are many different mediums for cyber-bullying, including:

- the Internet – via personal websites or weblogs (blogs), email messages, discussion groups,
- message boards, online personal polling sites, chat services, instant messaging (IM), or social networking websites such as MySpace, Facebook and Bebo;

- mobile phones – using short message service (SMS) or multimedia messaging service (MMS); and
- online games – used to abuse or threaten other players, or to lock victims out of games.⁵⁴

3.46 Evidence on the causes of cyber-bullying is mixed.

Kids are going to engage in risk behaviours because of their developmental needs to, regardless of what intellectually they know.⁵⁵

3.47 The National Children’s and Youth Law Centre stated that:

There is a misconceived sense of empowerment in the online world where cyber users adopt aliases to maintain a degree of anonymity. Anonymity encourages thoughtless misuse of the Internet, producing instantaneous and often uncontrollable effects that are comparatively more permanent, probative and pervasive than otherwise in the offline world.⁵⁶

3.48 Some young people, however, say that they would do things online that they would not do offline, because anonymity affords them the opportunity to act on any anti-social impulses that might otherwise be tempered in public. Children, in particular, are ‘more likely’ to bully in the online environment because they are able to hide their identities.⁵⁷ Those who are bullied physically and feel powerless go online feeling totally empowered.⁵⁸

3.49 While this may be false, the sense of anonymity reported by some young people may influence the way they bully or are bullied. Some admitted that they had not fully understood the implications of their actions. This was particularly likely when they could not see their victims.⁵⁹ The Australian Parents Council stated:

While children and young people see the online environment differently from adults, their incorrect assumption of anonymity online needs to be addressed, with an understanding of the

54 Australian Institute of Family Studies, *Submission 39*, p. 3.

55 Mr John Dalglish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS15.

56 National Children’s and Youth Law Centre, *Submission 138*, p. 5.

57 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS14; Communications Law Centre, *Submission 63*, p. 6.

58 Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS35.

59 Ms Georgie Ferrari, Chief Executive Officer, Youth Affairs Council of Victoria, *Transcript of Evidence*, 11 June 2010, p. CS15.

long-term impact that bullying and harassment online (and off) has on the perpetrator and the victim.⁶⁰

- 3.50 The perceived anonymity of the online environment was commented on by participants in the *Are you safe?* survey, with many attesting to its emboldening effect on those that cyber-bully others. For example, the following comments were submitted in response to various questions throughout the survey:

People feel more confident when they are online and say things that they would not be able to say to the persons face. They feel more confident online because the person cannot see them (Female aged 17).

Formspring also proves a problem that anonymous messages can be posted, allowing Cyber-Bullying to be anonymous, more appealing to bullies (Male aged 14).

Usually it comes as being insulted by an anonymous. But the degree I've been exposed to is mild enough that should someone be emotionally damaged by the comment, they're not going to make it very well through life, let alone the internet. That's not to say that there aren't worse things out there though (Female aged 14).

A great majority of internet sites e.g. 'TeenChat' and 'Formspring' have no requirement for only registered users. The amount of untraceable, anonymous and fraudulent users of these sites could be as little as four, or as great as a million. Cyber bullying occurs so easily when the bullies have no fear of being recognised or caught, because they are anonymous. On sites which operate as the above mentioned do, no one can feel safe (Female aged 17).

It needs to be impressed upon kids that their digital footprint is part of their reputation and may come back to bite them in their adult life for example when they are seeking employment. They also need to know what constitutes cyber-bullying and what the penalties are.⁶¹

As a Year 9 student, cyber bullying has had varying effect on me. Knowing some of the many reasons why people cyber bully has made me more aware of it and its degrees of impact on people.

60 Australian Parents Council, *Submission 10*, p. 3.

61 Parents Victoria Inc, *Submission 143*, p. 2.

Anonymity plays a big role in cyber bullying – the idea of ‘being the one behind the screen’ and ‘pointing the finger without anyone knowing who you are’ gives the bully even more satisfaction and chances without being caught. The computer screen becomes a metaphor for a massive wall protecting the bully from backlashes & consequences.

A lot of people have a sudden change of personality when online – they may create fake accounts, imitate people or be very dissimilar to what they are in real life. Experiencing bullying myself, I know this is extremely common. Going online gives opportunities for many to experiment and compete for attention. This may be ideal for some individuals due to [in their opinion] boredom or hatred of their lifestyle and relationships with others, although there are various reasons why people have rifts within.

To prevent more cyber bullying, we could try:

- stronger website policy on bans & personal safety
- stronger police enforcement
- different kinds of education
- government-run youth forums

I do hope you take these things into consideration and try to create many combatants against cyber bullying.⁶²

- 3.51 The perception that this abuse is anonymous may be fast becoming a fallacy because the ‘vast majority’ of online bullies are also engaged in this behaviour offline. Research also suggested that there are both private and public ways of cyber-bullying, so that it is possible for a perpetrator to be covert and anonymous, or quite overt. The Australian Parents Council noted that the ‘incorrect assumption of anonymity’ online needs to be addressed because of the long-term impact that cyber-bullying (and bullying) has on both perpetrator and victim.⁶³
- 3.52 Internet users, especially young people, should be made aware that in certain circumstances law enforcement officers may be empowered to ascertain identities such as computers used to commit offences online.⁶⁴

62 Jedidiah, *Submission 133*.

63 Australian Parents Council, *Submission 10*, p. 3. See also Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS14; Dr Barbara Spears, Senior Lecturer, School of Education, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS15.

64 Communications Law Centre, *Submission 63*, p. 6.

- 3.53 When asked if they witnessed cyber-bullying in the last twelve months, the following experiences were shared by respondents in the Committee's *Are you safe?* survey:

Cyberbullying isnt just about the bully, there needs to be more help for the victim and less chances for the people who bully. There should be a one chance rule for bullies and it should not be tolerated by sites such as facebook who tend to turn a blind eye to these occurrences. My "friend" bullied me, through facebook, IM and formspring non-stop because she didnt like how I was becoming closer to her old friends. Formspring should also be banned because it gives bullies free reign on contrlling someones life via the internet, and trust me when I say that when your being cyber bullied you are scared and feel alone and NO ONE should ever have to feel like that (Female aged 14).

I have been cyber-bullied, but it was a few years ago. It was 27 pages of teasing and swearing, then my dad told the bullies that they will see him in the school office the next morning. I was too scared to go to school, but I did. The next morning, the principal said they couldnt do anything, because it was out of school, so they got no punishment. He said to not bother with the police because we were only 12. I still got cyber-bullied, and i got very upset. I hope in the future, they will get punished (Female aged 14).

A friend of mine was constantly being told nasty things on her formspring (eg.that she should commit suicide). It made her mental health condition worse than it already was. She knew she should never have signed up for the site and has deleted it now but she will never forget what was said on there (Female aged 15).

A girl I knew wouldn't have sex with her boyfriend, so he made his friends send her anonymous and abusive text messages. Once she found out who did it, she told her principal and the boys were suspended (Female aged 13).

a person i know had abusive messages sent to her because someone hacked into her facebook and decided to read her private messages. she was continuously abused over her facebook and through texts (Female aged 16).

I didn't know the full story at the time, but, a friend of mine made a comment to somebody i knew but wasn't exactly friends with at the time (though now we have gotten to be quite good friends) and then the person who the comment was made to decided to post on the person

who made the comment's wall on facebook. it was immature but in a way he was defending himself. but then, it was taken too far. he showed up at the school i currently attend (as does the boy who made the first comment) wanting to fight him. luckily, that boy had left for home an hour ago. he then started posting on his wall asking when and where he wanted to fight, the first boy's friends started to intervene and decided to jokingly make references to a Call of Duty (on some sort of electronic gaming device) battle instead of having a real fight which angered the boy who had posted these things as well as his friends. it was decided when and where the fight was to be held but the one who was my friend didn't show up thankfully, as the other boy and his friends had knives (i was actually told this by the boy who brought them, if it were a rumour i don't think i would've believed it) in the end, i know i had a talk with the boy who had been harassed first, told him not to worry about it because in a few years he probably won't even remember this guy and that writing on his wall is showing that his comment affected him. after that they had a talk and now they are not friends but not enemies, just mutual (Female aged 15).

i was the one getting cyber bullied, and i still am. but there isn't much you can do when it's more than one person, because if you tell the teachers or police, they talk to the bullies, warn them, punish them, whatever, it doesn't stop them from verbally making me feel bad when they see me, and it doesn't stop them spreading rumours. bottom line is, kids NEED to learn to get along, because whether they like it or not, we all fall into the same community and it makes life much easier if we get along (Female aged 15).

I've seen in with my younger sister who is 9 years old, and it's more that they don't realise how unsafe the internet can be and believe that they can get away saying certain things via email. It was nothing too serious, but it was concerning that a 9 year old was being affected by cyber bullying in some way, even though it was minimal (Female aged 16).

just one person posting unnecessary rumours about someone else they didn't like that then broke out in a lot of things being said that may not have been meant but were just said as a defence for themselves. then this disagreement that began with two people ended with at least twenty people becoming and getting themselves involved (Female aged 14).

My "friend" continually cyber bullied me until i stopped it by blocking and deleting her as a friend. She would continue calling me names and making up stuff to turn my friends against me, which really ruined a

few of the genuine friendships I had with people (Female aged 14).

my best friend was being bullied by 4-5 girls since the June last year and they were calling her with swear words and telling her she was ugly and no one likes her and then she (my friend) got irritated and she moved to another place, but they still bully her (Female aged 13).

My best friend was bullied very badly and she had depression and self harm issues because of it (Female aged 17).

My fourteen year old sister is frequently cyber-bullied over both the social networking site Facebook as well as Formspring, as are many of her friends and people she knows. It causes her a lot of distress, largely because she is unable to escape it. It affects her self-esteem and happiness(Female aged 17).

My sister has had trouble with her 'friends'. At school they were nice to her, face to face. But outside of school, in the Facebook world, they were very mean. And whenever there was a fight, it was over Facebook, and they said things they never would have said otherwise, face to face. I also see other things all the time, everyday on Facebook; status' and comments that either directly, or often indirectly bully others (Female aged 17).

One of my best friends for 10 years was talking to another girl online and this girl started calling her really mean names and my friend got really upset and it got so bad that she overdosed on headache tablets and ended up in hospital for a week. She's fine now though but it made us all feel really bad and worried for her (Female aged 13).

There was a girl at my old school who was disliked by the majority of people, and they were constantly mean to her. A couple of times I told them to stop it, but it never makes any difference. I think she told the school about what was happening, but it was hard for them to do anything. It still happens, and it makes me really angry because no-one is able to stop it, and no matter how much of a bad person she might be, no-one deserves that (Female aged 15).

- 3.54 In response to the same question, comments were made that specifically discuss where photos have been used to cyber-bully others:

My friend sent nude pictures to a few boys and flashed herself a few times over Skype. The photo was sent around my whole school along with two or three other schools (Female aged 15).

Someone at my school hacked into a few girls accounts and posted rude pictures(not of the girls) and copied their messages of what they had been saying about other people(inboxed messaged onh facebook) and posted them. They also got some pictures of a girl in a bikini- zoomed in on their chest, tagged all of her friends as well as my school facebook page (Female aged 14).

Strangers went out of their way to insult a girl repeatedly on the social networking site, Tumblr. Manipulating photos of her using photoshop and making them embarrassing and humiliating for the girl (Female aged 16).

- 3.55 Comments were also submitted in response to various questions throughout the survey that discuss instances of cyber-bullying from the perspective of those bullying their peers, or those witnessing their friends or siblings bully others:

a close friend of mine frequently has fights over facebook. She posts status' about it and will make threats and talk ig of herself on there. She can never back it up, and she usually gets abused in person by the people she was threatening (Female aged 14).

boy discussing how unattractive/fat/stupid his ex was publicly on his fb status, posting mean things about other peoples girlfriends, being generally sexist towards women Girls calling others sluts/homewreckers/threats etc (Female aged 16).

my brothers face book is the worst, he has 300+ friends and they all pick on the fat and ugly people just cause of the way they look (Female aged 17).

on facebook. when someone has a problem with someone else they like to post it on their profile so that everyone can see whats happening. usually they are the 'cool' kidspicking on the lesds popular kids so thats why they decide to post it cause they know they will always have a group of their friends to badger these poor children (Female aged 16).

Someone i know hacked into another persons facebook account and sent everyone in the school a variety of pictures of genetalia, aswell as teachers. The bully also falsly stated that they were gay in order to frame their victim in an attempt to embarass and shame them on the same e-mail (Male aged 18).

I am a troll, i provoke people, with my intellectual insults that a lot of

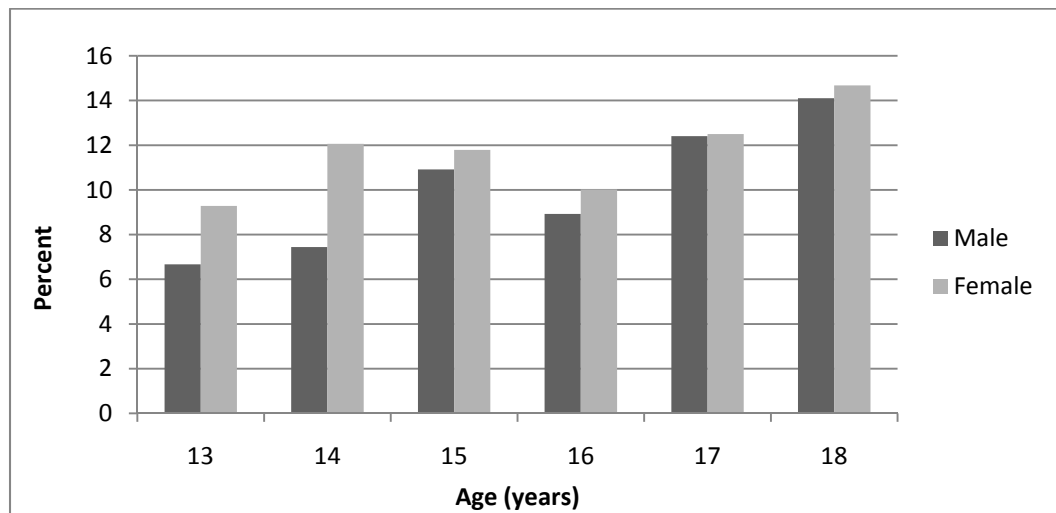
people don't understand, i poke harmless fun at them to get a reaction out of them, i only do this to my good friends, because they know of my joking. However if someone is bullying my friend i will troll the bully so they stop bullying my friend in need (Male aged 16).

- 3.56 The survey also asked its respondents aged 13 years or older if they had cyber-bullied someone else. Of total respondents (15,592), 1,379 respondents reported they had bullied another (8.8 percent).

Table 3.1 In the last 12 months have you been directly involved in cyber-bullying?

		Yes	No
Sex		#	#
13 Years	M	126	1890
	F	228	2456
14 Years	M	120	1612
	F	239	1982
15 Years	M	130	1191
	F	162	1374
16 Years	M	72	807
	F	100	998
17 Years	M	49	395
	F	71	568
18 Years	M	44	312
	F	38	259

Figure 3.1 Proportion (%) of those directly involved in cyber-bullying aged 13 years and over



3.57 Although the number of young people cyber-bullying others might be higher than these results found, the primary purpose of the question was to assess whether this group had also been on the receiving end of bullying.

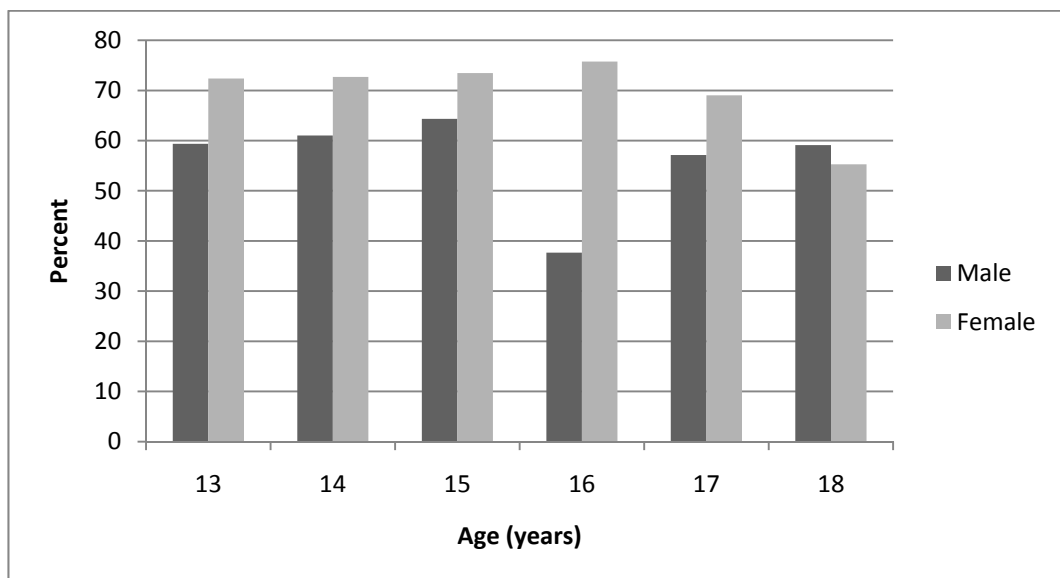
3.58 Of those that reported they cyber-bullied another person, 66 percent reported they had also been the victim of bullying online (n=910).

Table 3.2 Of those that cyber-bullied another, have they also been targets of cyber-bullying by others?

Sex	Yes a victim		Not a victim		
	%	#	%	#	
13 Years	M	59.3	73	40.7	50
	F	72.4	165	27.6	63
14 Years	M	61.0	72	39.0	46
	F	72.7	173	27.3	65
15 Years	M	64.3	83	35.7	46
	F	73.5	119	26.5	43
16 Years	M	37.7	26	62.3	43
	F	75.8	75	24.2	24
17 Years	M	57.1	28	42.9	21
	F	69.0	49	31.0	22
18 Years	M	59.1	26	40.9	18
	F	55.3	21	44.7	17

3.59 The graph below shows the differences in gender among those that reported they had cyber-bullied another, but were also on the receiving end of bullying. As is shown, female respondents reported a higher rate:

Figure 3.2 Proportion (%) of those that cyber-bullied who have also been targets of cyber-bullying by others aged 13 years and over



3.60 The Committee's survey sought young people's responses to the major reasons why people cyber-bully. Respondents were given a list of reasons and asked to select the main motivations. Those completing the survey aged 12 years or younger gave a very mixed response, with few differences between the options:

- Mixing with the wrong crowd;
- People looking for a fight and/or have an aggressive personality;
- Fighting over girls or boys;
- Copy cat of news stories;
- Boredom;
- Bad home life;
- Lack of respect for others;
- Not liking people with disabilities; and
- Not liking people from different backgrounds.

Table 3.3 What are the main reasons why people cyber-bully?

		Mixing with the wrong crowd	People looking for a fight	Fighting over girls or boys	Copy cat of news stories	Boredom	Bad home life	Lack of respect for others	Don't like people with disabilities	Don't like people from different backgrounds	Other
	Sex	%	%	%	%	%	%	%	%	%	%
6 Years	M	37.3	41.3	40.0	26.7	49.3	42.7	41.3	36.0	45.3	26.7
	F	46.3	46.3	31.7	23.2	41.5	48.8	37.8	30.5	41.5	31.7
7 Years	M	22.9	37.5	29.2	18.8	25.0	31.3	27.1	16.7	33.3	10.4
	F	37.5	28.1	34.4	17.2	31.3	37.5	32.8	31.3	21.9	10.9
8 Years	M	36.4	50.0	35.5	28.2	21.8	33.6	23.6	30.9	28.2	7.3
	F	19.6	41.2	30.9	25.8	14.4	35.1	19.6	24.7	19.6	7.2
9 Years	M	27.4	46.2	30.2	18.6	16.5	33.7	28.3	27.6	31.6	6.6
	F	30.0	44.2	30.4	24.1	14.2	34.5	27.4	25.6	30.4	8.7
10 Years	M	29.8	50.7	29.7	18.6	18.1	42.7	36.3	30.1	36.7	7.1
	F	30.3	49.9	30.9	17.9	17.0	42.3	37.4	27.1	36.8	9.5
11 Years	M	33.9	48.9	29.2	14.1	25.0	46.6	48.7	31.9	44.6	8.7
	F	35.1	51.3	27.7	14.1	25.3	54.9	50.8	32.5	46.7	13.6
12 Years	M	41.6	47.9	31.9	13.7	31.7	56.1	53.8	34.4	48.3	11.0
	F	42.9	49.2	30.0	13.3	31.9	64.8	56.1	36.5	52.6	18.0
13 Years	M	63.7	66.7	51.9	17.5	32.5	56.0	59.8	44.2	58.8	8.6
	F	62.3	68.7	50.7	15.6	31.5	61.0	61.9	41.9	56.8	10.7
14 Years	M	63.4	68.5	51.0	18.5	40.0	52.3	61.9	38.8	54.7	9.7
	F	58.9	71.2	53.6	16.5	40.1	57.4	68.5	36.6	51.9	9.9
15 Years	M	55.2	67.0	47.2	19.9	44.9	50.0	61.6	37.3	52.1	11.3
	F	56.6	69.4	55.0	16.2	46.0	54.7	69.1	33.7	49.6	9.7
16 Years	M	52.7	63.3	49.2	19.0	45.0	44.5	64.4	31.2	46.6	9.8
	F	52.0	67.1	51.9	15.8	50.0	44.0	72.9	30.0	43.9	9.4
17 Years	M	51.9	65.1	44.6	21.3	48.9	42.5	64.8	32.7	44.8	13.9
	F	48.8	63.6	50.4	15.7	57.2	42.4	78.5	27.3	44.9	10.9
18 Years	M	54.5	59.9	52.9	31.7	49.0	49.0	60.6	42.9	55.4	24.7
	F	50.2	57.5	51.4	28.2	52.5	43.6	61.4	37.5	51.0	24.7

- 3.61 More significance was noted between respondents aged 13 years and older. The most common reasons or motivations for cyber-bullies included:
- Mixing with the wrong crowd;
 - People looking for a fight;
 - Bad home life; and
 - Lack of respect for others.
- 3.62 Other motivations that were highly reported included fighting over boys or girls; and not liking others from different backgrounds.
- 3.63 Similarly, comments were submitted in free text spaces throughout the survey that shed further light on the motivations of those that cyber-bully:

Cyber bullying will always happen as long as there are people who has low self esteem so perhaps work on creating a more supportive community environment? (Female aged 17).

normally people dont cyber bully unless they have alot of support. they wont write something on facebook, myspace ect without knowing there are many people that agree with them or will back them up (Female aged 17).

a lot of bullies get bullied at home so home should be made safer and it won't help making nice places for them to stay (Male aged 14).

being the victim of bullying themselves and therefore wanting to hurt other people in return (Female aged 14).

Fear of the unknown, scared of differnces from the 'norm'. Not enough education (Male aged 14).

Having low enough self esteem that they have to find some kind of self-worth and a sense of authority by prodding a weaker audience because they refuse to come to the inevitable truth: they can't have a stable friendship because they're too afraid of getting hurt to let someone close. That or they have dodgy parents who raised them to think they own the world (Female aged 14).

I think that some cyber bullying starts by people incorrectly interpreting a situation. Communication through just words can often be misunderstood (Female aged 14).

In online communities it is common for fights to break out and grudges

to be held between people (Female aged 16).

Ignorance between people leading to conflicts and fights that could be considered cyber bullying (Male aged 16).

ignorance to different people's customs and religions, the need to take out their anger on others (Female aged 14).

Low self esteem, social prestige, to confirm a status in community- perhaps an online one or in life such as school or youth group (Female aged 16).

Low self esteem; Someone feels better if he/she can make someone else feel terrible about him/herself (Male aged 18).

Making the wrong choices or saying something when nothing should be said (Male aged 16).

Not accepting people of different personalities etc and being very judgemental as is our nature these days (Female aged 17).

People who try to be "heroes", think they are cool because they cyber-bullied someone, also, groups egging on other students to cyberbully someone (Male aged 15).

people who want to demoralise fellow peers who they have something against. (but normally the victim won't have done anything wrong) (Female aged 15).

supposed "Anonymity" being able to express opinion without consequence (Female aged 17).

They are going through a rough path in life, and get all of the anger out on the victims they bully (Female aged 14).

Prevalence

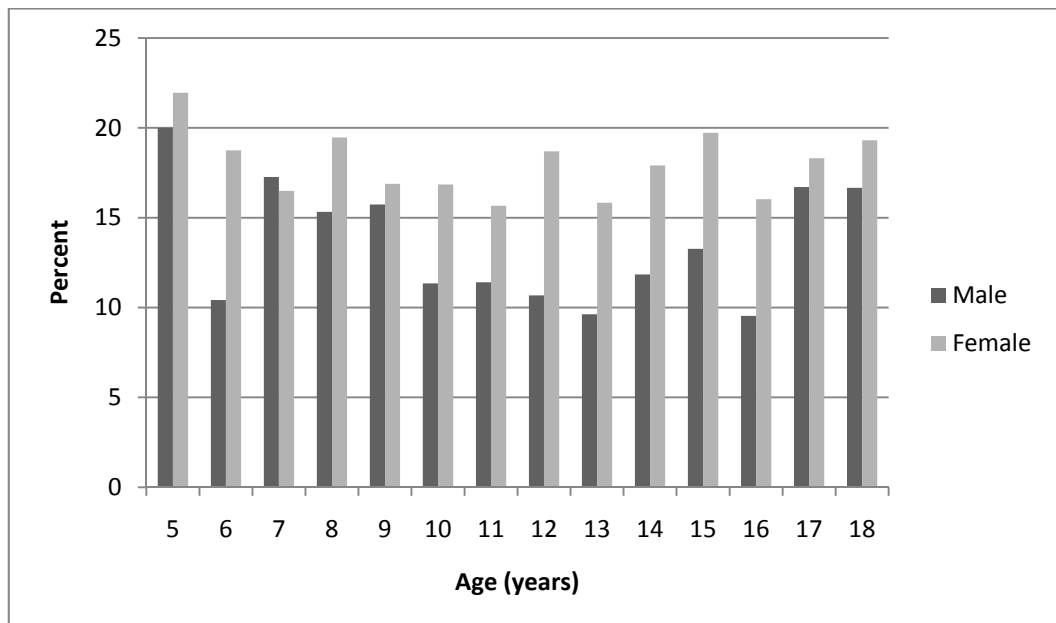
- 3.64 Research to date shows that rates of traditional bullying are higher than those of cyber-bullying.⁶⁵ The Australian University Cyberbullying Research Alliance stated that there was strong 'suggestive' evidence that cyber-bullying had increased 'in the last few years' with the technological

65 See Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS2; Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS14; Murdoch Children's Research Institute: *Submission 111*, p. 2; Associate Professor Sheryl Hemphill, Senior Research Fellow, *Transcript of Evidence*, 9 December 2010, pp CS22, 25; Dr Barbara Spears, Senior Lecturer, School of Education, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS12.

shift from Web1.0 to Web 2.0 platforms: from email to social networking sites. At the same time, from simply being a technological and safety device, a mobile phone had become a social tool that indicated connectedness and status.⁶⁶

- 3.65 The Committee found similar results in its analysis of its survey results. Respondents were asked if they had been cyber-bullied in the last year: rates of cyber-bullying remained under 22 percent, with females generally reporting higher rates.

Figure 3.3 Proportion (%) of those that have been the targets of cyber-bullying the past 12 months by age and gender



- 3.66 Recent research revealed that 10 to 15 percent of students surveyed have experienced it more than once. Other submissions quoted higher figures, in one case suggesting that the rate could be as high as one in every three Australian young people. Experience from America and Britain suggests that this will increase, as 30 to 40 percent of students in those countries have experienced it.⁶⁷

Cyberbullying has been and remains the most pervasive form of serious risk faced by young people when they use technology.⁶⁸

⁶⁶ Australian University Cyberbullying Research Alliance, *Submission 62*, p. 9.

⁶⁷ Alannah and Madeline Foundation, *Submission 22*, p. 17. See also WA Education Department, *Submission 115*, p. 1; Australian Communications and Media Authority, *Submission 80*, p. 7; Australian University Cyberbullying Research Alliance, *Submission 62*, pp. 12, 15-18.

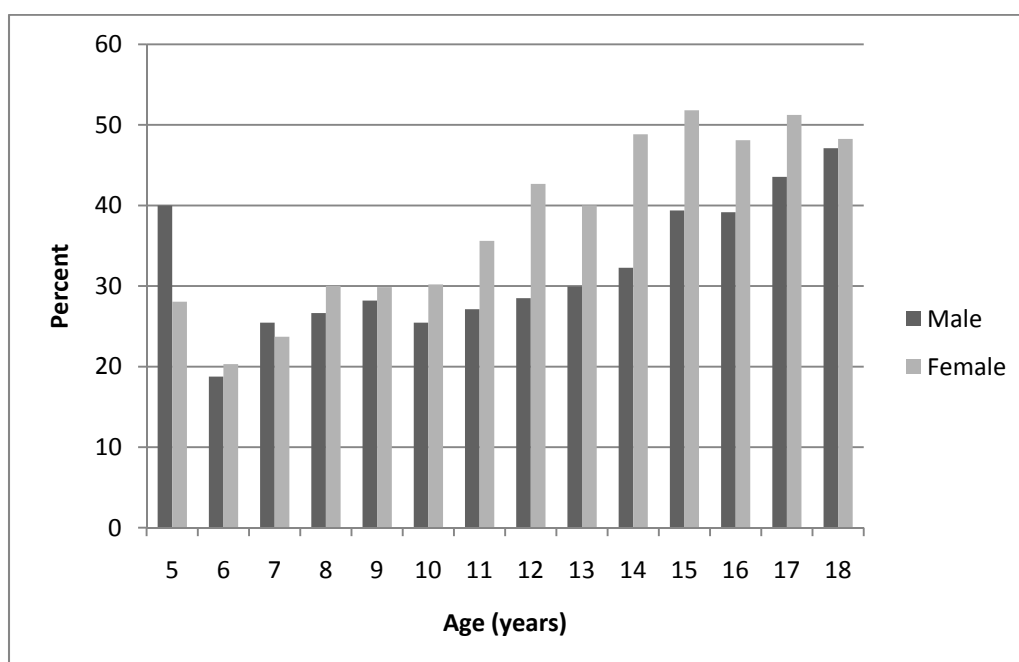
⁶⁸ Alannah and Madeline Foundation, *Submission 22*, p. 17.

3.67 While one in four Australian children has been exposed to bullying,⁶⁹ in a recent Vodafone survey:

The Vodafone report revealed just one in five parents surveyed believe that their child had been exposed to bullying, one in ten acknowledged their child had been a witness to bullying and a startling 0% responded their child was a bully.⁷⁰

3.68 The Committee's *Are you safe?* survey also asked its participants of their exposure to bullying online. Female participants aged eight to 17 years reported higher exposure to bullying online than their male counterparts, with the average rate peaking between 15 and 17 years.

Figure 3.4 Proportion (%) witnessing cyber-bullying in the last 12 months by age and gender



3.69 Microsoft Australia noted that parents/carers are challenged when dealing with cyber-bullying. Research commissioned in 2008 found that 83 percent did not know what to do if a child was being cyber-bullied, and two out of three were unsure of the best ways to help their children. Almost all the parents/carers surveyed were aware of the problem, and

69 Kidspot at <http://www.kidspot.com.au/School-Bullying-Facts-and-figures-about-bullying+258+article.htm>.

70 Vodafone Hutchison Australia, *Submission 141*, p. 8, citing *Vodafone Digital Parenting Report – Safety*, October 2010, Omnibus.

three-quarters said that they were more concerned about this issue than they had been a year previously.⁷¹

Studies have also found that children are more likely to talk to their parents than to teachers about being bullied, yet many parents of children who are bullied do not always know how best to talk to their children about the issue, and hence require appropriate information and support to deal with the incidence of bullying.⁷²

3.70 Researchers at Simon Fraser University concluded that 'much of the cyber-bullying activity is happening under the radar of school staff and parents'.⁷³ A recent survey of girls by the Department of Education, Science and Training found 57 percent had been defamed online, but most were reluctant to tell their parents/carers or teachers about it.⁷⁴

3.71 While parents/carers may be beginning to be more aware of what young people do online, as many as 60 percent of young people have had a negative experience online, but 52 percent of parents/carers did not realise it.⁷⁵ The Australian Parents Council stated:

parent use of the internet and social networking platforms, particularly those with children is now catching up to usage by children and young people so parents have a better understanding than 10 years ago.⁷⁶

3.72 Moreover, because parents/carers are not sure how to respond to cyber-bullying, children and young people may effectively be blamed for raising the issue. Although there is 'an enormous amount' of material available about cyber-bullying on the Internet, this range of information prevents parents/carers from establishing what among it is worthwhile.⁷⁷ Without the right strategies and tools, adults run the risk of further isolating their

71 Microsoft Australia, *Submission 87*, pp. 2-3.

72 Australian Psychological Society, *Submission 90*, p. 20, citing Cross *et al*, 2009, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre.

73 Simon Fraser University, *Submission 55*, p. 15.

74 Device Connections Pty Ltd, *Submission 51*, p. 12.

75 Mr Craig Scroggie, Vice President and Managing Director, Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, pp. CS3-4.

76 Australian Parents Council, *Submission 10*, p. 3.

77 Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS6.

young people.⁷⁸ Mr Chriss Watt, Federal Secretary, Independent Education Union of Australia noted:

there is general agreement about the importance of continuing research on all aspects of cyber safety and for disseminating updated research to parents and the community at large.⁷⁹

3.73 Some abuses, such as cyber-bullying and sexting, are usually carried out by those close to the victim, such as peers/schoolmates, neighbours or 'friends'. Others, such as cyber-stalking and sexual grooming, are generally undertaken online by adults with sinister intentions.⁸⁰

3.74 The Alannah and Madeline Foundation stressed the importance of looking at who is doing the bullying: 46 percent were other students, about one-third did not know who it was, 34 percent were friends and 16 percent were siblings.⁸¹

3.75 The following submission discusses a personal experience with cyber-bullying:

I have experienced cyber-bullying it is not a very nice feeling. I am 13 years old almost 14. I am also female. I haven't also been the best student or the skinniest or prettiest girl out there but that is why I have been bullied. I have had my father pass away 2 years ago and a very sick mother; I have also been bullied about this. I am strongly against bullying and it needs to be put to an end! It doesn't need to go to the extent of deleting all the social sites like Facebook and MySpace but it needs better rules for example stopping swearing on these sites should be stopped. I hope this email has helped you a little bit.⁸²

3.76 The *Click and Connect: Young Australians' use of online social media* research project by ACMA sought to understand the extent to which young people had experienced cyber-bullying, and had participated in it.

In Australia, the Australian Covert bullying prevalence study of May 2009 highlighted 7-10% incidences of cyber-bullying among

78 Mr Chris Watt, Federal Secretary, Independent Education Union of Australia, *Transcript of Evidence*, 30 June 2010, p. CS11.

79 Australian Parents Council, *Submission 10*, p. 3.

80 For example, NSW Government, *Submission 94*, pp. 7-10.

81 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. 33.

82 Jodie, *Submission 131*.

young people, and the Click and Connect reports recorded slightly higher incidences.⁸³

- 3.77 It demonstrated that cyber-bullying increased with age, in relation to access to technology. By the age of 16 to 17 years, nearly one in five respondents had experienced some form of cyber-bullying. Just one percent of eight to nine year olds reported experiencing it. The largest increase occurred between eight/nine and ten/11 years of age, followed by a second smaller increase from ten/11 and 12/13 years old.⁸⁴
- 3.78 A study of 548 young Australians by BoysTown found that cyber-bullying is a group phenomenon most prevalent during the transitional ages between primary and secondary school. Across the sample, 59 percent experienced cyber-bullying when aged ten-12 years, 52 percent when aged 13-14 years and 29 percent when aged 15-16 years. Significantly, the report also found that the majority of older participants also reported being cyber-bullied when aged 13-14 (15- to 18-year olds: 72 percent; 19- to 25-year olds: 50 percent).⁸⁵
- 3.79 The most common place for cyber-bullying is at home, followed by the schoolyard. Schools only have a 30 percent influence over what young people learn; 70 percent is about things outside their influence. Often something happens at school that is transferred to the online environment after the school day is over and, by the next day, it has been blown out of proportion. These issues can escalate very quickly.⁸⁶

I am sending you this email regarding cyber bullying. I am a female and I am 14 years of age and I personally have not been cyber bullied but many people around me that I know have. Cyber bullying is very wrong and can get very serious. It makes me sad to think that people can be so cruel and horrible to people and think it's alright. There have been many cases at my school where cyber bullying has occurred. It happened to one of my good friends and it was so cruel of this person to be so horrible, that my friend

- 83 Childnet International, *Submission 18*, p. 2 citing ACMA, 2009, *Click and Connect: Young Australians' use of online social media* and Cross et al, 2009, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, Edith Cowan University.
- 84 Australian Communications and Media Authority, 2009, *Click and Connect: Young Australians' use of online social media, Quantitative Report*, p. 12.
- 85 Price M and Dalgleish J, 2010, 'Cyberbullying: Experiences, impacts and coping strategies as described by Australian young people', *Youth Studies Australia*, 29 (2): 51-59 at p. 54.
- 86 See Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS33; Ms Georgie Ferrari, Chief Executive Officer, Youth Affairs Council of Victoria, *Transcript of Evidence*, 11 June 2010, p. CS33; Mr Jeremy Hurley, Manager, National Education Agenda, Principals Australia, *Transcript of Evidence*, 11 June 2010, p. CS9.

got upset but everyone supported her and stuck up for her. This bully said very mean things about my friend's personal life. The bully tried to apologize but they couldn't repair the damage they had done. I strongly think that cyber bullying should be put a stop to because it can lead to depression and people feel unhappy and sad. Bullies should have better things to do then putting people down and making them feel useless. Social Networking sites should have some more security and people who bullied should be banned from that networking site or have their account deleted.⁸⁷

- 3.80 BoysTown commented that although the data is inconsistent,⁸⁸ it seems that while boys are more likely to bully physically, girls are more prone to pursue avenues of harassment involving emotional and psychological abuse.⁸⁹
- 3.81 Bullying and cyber-bullying peak at times of transition, pre-school to primary school and primary to high school, and require special attention by teachers at those times.⁹⁰
- 3.82 Among other causes, difficulties in relationships between school friends can lead to increased cyber-bullying.⁹¹ In small children, initially at least, it can be exploratory, as they express themselves and try to understand how they will relate to other children.⁹²
- 3.83 Less than 10 percent of those asked admitted to any involvement in this abuse of the online environment, although older age groups were 'most likely' to engage in cyber-bullying.⁹³

We are now conscious of distinct differences between
cyberbullying and face-to-face bullying: a form of covert bullying,

87 Abbie, *Submission 132*.

88 Ms Megan Price, Senior Research Officer, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS20.

89 Australian Clearinghouse for Youth Studies, *Submission 121*, pp. 2-3; beyondblue, *Submission 5*, p. 2. See also Associate Professor Sheryl Hemphill, Senior Research Fellow, Murdoch Children's Research Institute, *Transcript of Evidence*, 9 December 2010, p. CS25.

90 See Alannah and Madeline Foundation, *Submission 22*, p 5; beyondblue, *Submission 5*, p. 1; Ms Megan Price, Senior Research Officer, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS20; Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS9.

91 Mr Philip Lewis, Chair, Association of Principals of Catholic Secondary Schools (SA), *Transcript of Evidence*, 3 February 2011, p. CS3.

92 Professor Phillip Slee, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS12.

93 Australian Communications and Media Authority, *Submission 80*, p. 7; WA Education Department, *Submission 115*, p. 1.

it can happen at any time, anywhere; and there is no escape behind doors. Audiences can be huge and reached quickly. Power is allocated differently, and bullying can be inter-generational. Perpetrators can have at least an illusion of anonymity and their behaviour can be disinhibited because of this; empathy is also reduced because the victim's reaction is not seen.⁹⁴

3.84 The Australian Youth Affairs Coalition expressed concern:

... about the rate of under-reporting of cyber-bullying by young people. Young people are more likely to confide in their peers and they may not speak up to authority figures fearing that their access to technology will consequently be restricted.⁹⁵

3.85 BoysTown also noted that, although cyber-bullying is 'a ubiquitous phenomenon', there is still a high level of under-reporting. This reinforces the need for active dissemination of information on the issue, and for the provision of integrated support for young people to speak out about it.⁹⁶

In general, most children when we talk to them about cybersafety think that adults are being hysterical about the issue. They do not see it as a big issue. They will, when pressed, talk about cyberbullying being something that they hear a lot about or might have been involved in, but the average child seems to have a lot of mechanisms to be able to deal with it. A lot of those mechanisms come from their peer-to-peer relationships and often from having good relationships within their family. It definitely is the marginalised youth, who are disconnected within the community, who are seeking connections through online forums. For them, sometimes it is the first time someone has actually engaged with them, so they are really compelled to follow through with that relationship because they are getting something back that they get from no other part of their life.⁹⁷

3.86 Responses about the prevalence of cyber-bullying vary with the questions asked in surveys. If adolescents are asked about it specifically, the

94 Alannah and Madeline Foundation, *Submission 22*, p. 17. 'The disinhibition effect is the psychological process that recognises that there is a screen and that when you put things beyond the screen there are no consequences and you walk away from it': Dr Barbara Spears, Senior Lecturer, School of Education, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS25.

95 Australian Youth Affairs Coalition, *Submission 28*, p. 6.

96 BoysTown, *Submission 29*, p. 11.

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

responses will be quite different to questions that seek to explore a range of abusive behaviours. If questions explored both areas, the answers reveal 'a high prevalence rate'.⁹⁸ While 'cyber-bullying' is not a term used by young people, they recognise it.⁹⁹ Professor Marilyn Campbell added that:

if you just ask, 'Have you ever received a nasty text message?' which is a behavioural term, then you do not know whether that is cyberaggression or cyberbullying. Because we know that there are different interventions both for prevention and intervention that work between distinguishing bullying as a subset of aggression and not just as general fighting, I think we have to be very careful that we do not shorthand something and label inappropriately on an individual level.¹⁰⁰

- 3.87 The Mental Health Council of Australia pointed out that, because of this lack of research, the prevalence of cyber-crimes in Australia is largely unknown. The five major risks that it identified pose great risks to young people, with potentially catastrophic impacts on their mental health and well-being, both immediately and chronically. From emerging international research, it is clear that the risks to young Australians can be serious, with action required to minimise psychological, social and physical harm.¹⁰¹
- 3.88 The prevalence of cyber-bullying and its severity were also commented on by young people consulted by the Committee:

it happens everywhere and all the time. threats have become a big issue, particularly from teenage boys to teenage girls and its not getting better. pubescent boys seem to think theyre better than everyone else in the world, and especially teenage girls, so we always cop it. something must be done about this. serious and severe effects have come out of things like this. im not prepared to let it keep happening (Female aged 15).

Tiger expressed the view that cyber-safety is 'getting worse' the more it is mentioned on the news and advertised.¹⁰²

98 Dr Barbara Spears, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS11

99 Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS35.

100 Associate Professor Marilyn Campbell, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, pp. CS10-11.

101 Mental Health Council of Australia, *Submission 52*, pp. 3-4.

102 Tiger, *Submission 144*.

The ratio of people who feel safe and unsafe/ get bullied or don't is different to how how media makes it. We only see the bad things in the papers/on the news, therefore making parents question it probably more than they should (Female aged 15).

3.89 Respondents to the *Are you safe?* survey aged 13 years or older were asked if they believe cyber-bullying was increasing. Almost 60 percent of respondents in this age group believe that cyber-bullying appears to be increasing (58.7 percent), and there is a difference between male and female respondents: 63.1 percent female; 54.2 percent male.

Table 3.4 Is cyber-bullying increasing?

		Seems to be increasing	Has not changed	Seems to be decreasing	Not stated
Sex		%	%	%	%
13 Years	M	62.1	27.8	7.2	2.9
	F	66.7	25.4	5.7	2.2
14 Years	M	57.9	32.7	7.3	2.0
	F	66.3	26.9	5.1	1.6
15 Years	M	56.3	33.3	7.8	2.5
	F	68.1	25.1	5.5	1.3
16 Years	M	53.5	35.7	7.8	3.0
	F	62.3	28.6	6.0	3.1
17 Years	M	49.1	38.5	9.4	3.0
	F	63.6	27.1	6.9	2.5
18 Years	M	46.2	41.7	9.0	3.2
	F	51.7	32.4	10.4	5.4

3.90 Some young people are targeted because of their racial or cultural background. Ignorance, fear and/or prejudice mean that lesbian, gay and bisexual young people tend to be disproportionately victimised by cyber-

bullies.¹⁰³ There have been community concerns about the increasing prevalence of bullying 'sexting' via mobile phones, and the impact that these abuses are having on Indigenous young people.¹⁰⁴

Impacts and implications

3.91 A considerable amount of evidence was presented to the Inquiry on the impacts of cyber-bullying. All forms of bullying can have serious and negative effects on those involved, both victims and bullies. Young people who are regular perpetrators are more likely to engage in anti-social behaviour, criminality, have problems with substance abuse, demonstrate low academic achievements and be involved in child/spouse abuse later in life.¹⁰⁵

3.92 The research by BoysTown called for effective prevention and intervention strategies for those who have been cyber-bullied. It also showed:

that the negative impacts of Cyberbullying include diminished self-confidence, low self-esteem, interpersonal conflicts, below-average school performance, extreme sadness and anger, self-harming behaviour, suicidal ideation, and in some notable cases, death by suicide. A number of researchers have also proposed that the impacts of cyberbullying may in fact be more severe compared to those from traditional forms of bullying. This underpins the need for immediate and effective prevention and intervention strategies for those impacted by cyberbullying.¹⁰⁶

3.93 As these effects can persist in later life, they may contribute to depression in young people, or they may not seek help early for their difficulties.¹⁰⁷

cyberbullying is a little different from some of the other things that we were talking about, like inappropriate content, because you are

103 Mr John Dalglish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*; 17 March 2011, p. CS20; Alannah and Madeline Foundation, *Submission 22*, pp. 17- 19; beyondblue, *Submission 5*, p. 2.

104 NT Government, *Submission 84*, p. 7.

105 Alannah and Madeline Foundation, *Submission 22*, pp. 18-19; Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS10.

106 BoysTown, *Submission 29*, p. 9.

107 See, for example, Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS15; Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS8; Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. 9; Mental Health Council of Australia, *Submission 52*, pp. 5-6; Alannah and Madeline Foundation, *Submission 22*, p. 18; beyondblue, *Submission 5*, p. 2.

dealing with young people who think they are in control and do not recognise when they are not. That is why having easy ways for other parts of the community to be involved in talking about appropriate and inappropriate behaviour becomes very important.¹⁰⁸

3.94 While there has only been limited research in Australia on cyber-bullying, it is clear from international research, and from research on traditional bullying, that the impact on victims is especially serious for young people who are not adequately skilled to deal with this abuse. Those who experience it often have drops in self esteem, with long-term effects on well-being.¹⁰⁹

3.95 Because it is covert, cyber-bullying has the potential to result in more severe psychological, social and mental health problems than overt bullying. The Alannah and Madeline Foundation believed that, because it 'mirrors and magnifies' traditional bullying, it often has severe effects on the mental, social and academic well-being of victims. In the short term, in addition to anxiety and depression, it can impact on school work and cause a sense of helplessness. In the longer term, they have a higher likelihood than their peers of experiencing bad health and problems with social adjustments:

there were more mental health problems, more anxiety and more depression in those children who reported that they had been cyberbullied than those children who reported that they had been schoolyard bullied. If they had been cyberbullied and schoolyard bullied, they had that same increase of poor mental health afterwards. However, the adolescent students actually said to us that they thought that cyberbullying was not as bad as face-to-face bullying, but the actual results of the mental health showed that it was.¹¹⁰

3.96 While every case of cyber-bullying does not lead to it, some victims are so overwhelmed by this abuse that they decide that suicide is their only option.¹¹¹ The Mental Health Council of Australia referred to the stories of young people who had been victims shortly before they made decisions to

108 Hon Mozelle Thompson, Advisory Board and Policy Adviser, Facebook, *Transcript of Evidence*, 21 March 2011, p. CS16.

109 Ms Michelle Noon, Program Manager, Youth, beyondblue, *Transcript of Evidence*, 9 December 2010, p. CS1.

110 Associate Professor Marilyn Campbell, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, pp. CS16-17.

111 Murdoch Children's Research Institute *Submission 111*, p. 2.

take their lives. It provided three examples of young Australians for whom this seems to have been the sequence of events.¹¹²

- 3.97 Cyber-bullying affects young people because of its viciousness, not knowing the identity of the person or persons responsible, the public humiliation of seeing images of themselves posted on an online platform, and their seeming inability to escape. No one seems to be available or able to help them. They worry that parents and teachers will find out, adding to the public humiliation.¹¹³ The abuse is difficult to report because of the pain, the shame, reliving the experience and the possibility of further victimisation people feel in reporting in a culture where it is not encouraged.¹¹⁴

those children who perpetrate bullying are just as disadvantaged in later life as those children who are the victims. So all children who participate in bullying have mental health problems – substance abuse, anxiety or depression.¹¹⁵

- 3.98 It is ironic that the victims are also concerned that, in an effort to protect them, their access to technology will be removed. This probably strengthens the tendency for victims to hide negative online experiences from their parents/carers.¹¹⁶ It is a matter for concern but not surprising that, when asked to whom they would turn if threatened online by a predator or bully, some young people placed their parents/carers last in a list of ten. They would go to a friend first, and this should be the basis of communication to provide support.¹¹⁷
- 3.99 Most victims of cyber-bullying will tell their friends because they trust them.¹¹⁸ Another survey suggested that ‘only a minority’ were

112 Mental Health Council of Australia, *Submission 52*, pp. 5- 6.

113 Alannah and Madeline Foundation, *Submission 22*, p. 18.

114 Ms Catherine Davis, Federal Women’s Officer, Australian Education Union, *Transcript of Evidence*, 30 June 2010, p. CS12.

115 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS9.

116 Alannah and Madeline Foundation, *Submission 22*, p. 18; Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS11.

117 Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS11; Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS10.

118 Dr Barbara Spears, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS14.

approaching peers, but that this was very effective when it happened. This should be the basis of communication when support is needed.¹¹⁹

3.100 Inspire Foundation's focus groups of young people aged from 14 to 25 demonstrates that restrictive approaches to technology are ineffective and do not justify the negative impact they can have on the enabling characteristics of technology.¹²⁰ These focus groups found that:

- Many existing online safety programs emphasise a restrictive approach, in which access to technology is limited to minimise risks;
- Few online safety resources adequately address cyber-bullying;
- A 'large proportion' of young people who had participated in focus groups demonstrated a 'relatively high' awareness of online safety risks. Many reported using risk reduction strategies to stay safe online;
- Young people in the Foundation's focus groups were dissatisfied with safety initiatives that restricted Internet access, although they knew that such restrictions could be circumvented easily;
- Restrictive approaches may discourage young people from discussing online safety issues and/or report problems;
- A 'large number' of young people reported experiencing cyber-bullying, either as victims or perpetrators, but acknowledged that such behaviours were not exclusively products of technology but 'existing social norms and attitudes'; and
- Significantly, there was a prevailing attitude that parents/carers, teachers and youth workers did not really understand technology, or how young people use the Internet, and therefore were not in a position credibly to advocate safe Internet practices.¹²¹

3.101 The Mental Health Council of Australia noted recommendations from the 4th Biennial Conference of the Australian National Centre Against Bullying, held in 2010. It found that a national commitment was required to increase cyber-safety and reduce bullying across the community. As part of the process to achieve these goals, it recommended ten steps:

- Early intervention;
- Training for teachers;
- An appropriate legal framework;

119 Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS10; Mr John Dalgleish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS13.

120 Inspire Foundation, *Submission 3*, p. 6.

121 Inspire Foundation, *Submission 3*, pp. 8-9.

- An increased focus on transitions at schools;
- A whole-school approach;
- A whole-community approach;
- Young people to be part of the solution;
- Technology to be part of the solution;
- Support for on-going Australian research; and
- Federal funding.¹²²

Coping strategies

- 3.102 It is clear that any two young people, approached by a bully, will react in different ways. Some have skills, a better sense of self, and can deal with the abuse. It is important to build up that sense of self in children.¹²³
- 3.103 BoysTown also found that across their lifetime, participants had tried a number of strategies to cope with cyber-bullying. These included traditional 'offline' strategies of confronting the bully, seeking help from parents, siblings, family and teachers, retaliation and staying offline. 'Online' strategies of blocking the bully, removing them from friendship lists as well as changing profile names or mobile numbers.¹²⁴
- 3.104 Similar results were found in the Committee's survey. Of its participants aged 12 years or younger, commonly used strategies were talking to friends or family and staying offline or blocking the bully. Many respondents who had been bullied in the previous 12 months reported using multiple strategies to address the problem. A relatively low percent reported that they ignored the bullying behaviour, with a higher percent reported among the male respondents.

122 Mental Health Council of Australia, *Submission 52*, p. 6.

123 Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS15.

124 Price M and Dalglish J, 2010, 'Cyberbullying: Experiences, impacts and coping strategies as described by Australian young people', *Youth Studies Australia*, 29(2): 51-59.

Figure 3.5 If you were cyber-bullied, what did you do?

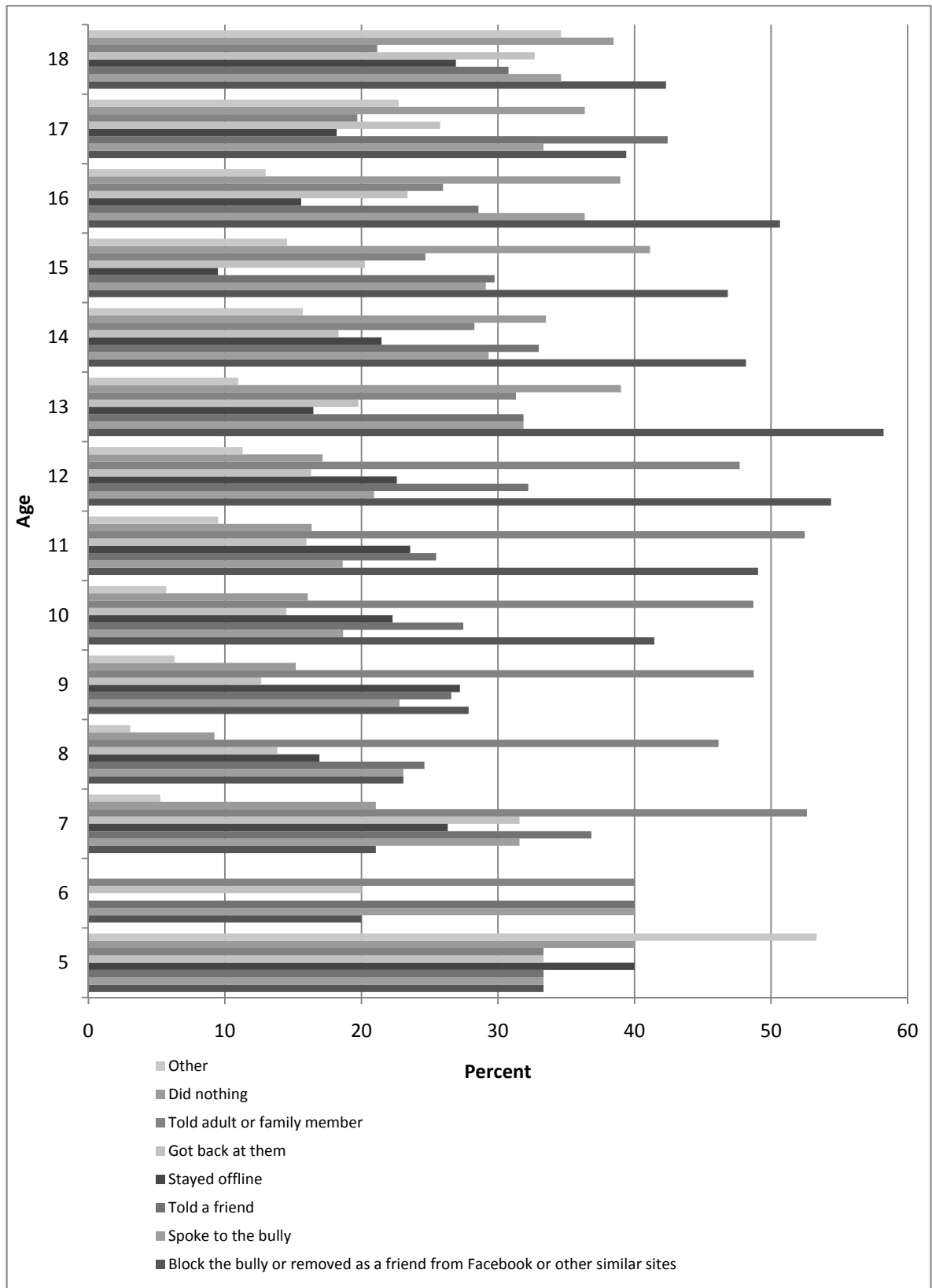


Table 3.5 If you were cyber-bullied in the last 12 months, what did you do?

	Sex	Blocked or removed bully as a friend		Spoke to the bully/ Confronted the bully		Told a friend		Stayed offline		Told an adult or family member		Sought revenge or paid them back		Did nothing/ Ignored it		Other	
		%	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#
5 Years	M	33.3	5	33.3	5	33.3	5	40.0	6	33.3	5	33.3	5	40.0	6	53.3	8
	F	44.4	8	44.4	8	44.4	8	44.4	8	38.9	7	44.4	8	55.6	10	44.4	8
6 Years	M	20.0	1	40.0	2	40.0	2	0.0	0	40.0	2	20.0	1	0.0	0	0.0	0
	F	25.0	3	33.3	4	58.3	7	25.0	3	50.0	6	25.0	3	41.7	5	16.7	2
7 Years	M	21.1	4	31.6	6	36.8	7	26.3	5	52.6	10	31.6	6	21.1	4	5.3	1
	F	6.3	1	31.3	5	43.8	7	25.0	4	37.5	6	6.3	1	18.8	3	6.3	1
8 Years	M	23.1	15	23.1	15	24.6	16	16.9	11	46.2	30	13.8	9	9.2	6	3.1	2
	F	17.7	17	19.8	19	30.2	29	18.8	18	56.3	54	5.2	5	9.4	9	6.3	6
9 Years	M	27.8	44	22.8	36	26.6	42	27.2	43	48.7	77	12.7	20	15.2	24	6.3	10
	F	28.6	52	24.2	44	34.6	63	30.8	56	60.4	110	1.6	3	15.4	28	7.1	13
10 Years	M	41.5	80	18.7	36	27.5	53	22.3	43	48.7	94	14.5	28	16.1	31	5.7	11
	F	51.8	157	11.6	35	32.3	98	29.0	88	62.7	190	4.6	14	8.3	25	13.2	40
11 Years	M	49.0	129	18.6	49	25.5	67	23.6	62	52.5	138	16.0	42	16.3	43	9.5	25
	F	55.1	216	16.6	65	34.2	134	24.7	97	64.3	252	4.3	17	7.4	29	16.1	63
12 Years	M	54.4	130	20.9	50	32.2	77	22.6	54	47.7	114	16.3	39	17.2	41	11.3	27
	F	69.0	292	22.0	93	44.7	189	20.3	86	61.0	258	13.2	56	8.5	36	10.9	46
13 Years	M	58.2	106	31.9	58	31.9	58	16.5	30	31.3	57	19.8	36	39.0	71	11.0	20
	F	59.1	230	28.0	109	44.7	174	17.2	67	42.9	167	9.8	38	36.5	142	13.1	51
14 Years	M	48.2	92	29.3	56	33.0	63	21.5	41	28.3	54	18.3	35	33.5	64	15.7	30
	F	60.6	215	32.4	115	49.0	174	14.4	51	41.7	148	11.8	42	46.5	165	10.1	36
15 Years	M	46.8	74	29.1	46	29.7	47	9.5	15	24.7	39	20.3	32	41.1	65	14.6	23
	F	56.8	154	33.6	91	39.5	107	15.5	42	38.7	105	11.8	32	45.4	123	10.7	29

16 Years	M	50.6	39	36.4	28	28.6	22	15.6	12	26.0	20	23.4	18	39.0	30	13.0	10
	F	55.0	88	33.1	53	46.9	75	13.8	22	37.5	60	7.5	12	47.5	76	10.6	17
17 Years	M	39.4	26	33.3	22	42.4	28	18.2	12	19.7	13	25.8	17	36.4	24	22.7	15
	F	58.7	61	38.5	40	40.4	42	14.4	15	32.7	34	10.6	11	51.9	54	8.7	9
18 Years	M	42.3	22	34.6	18	30.8	16	26.9	14	21.2	11	32.7	17	38.5	20	34.6	18
	F	48.0	24	40.0	20	32.0	16	30.0	15	24.0	12	42.0	21	36.0	18	28.0	14

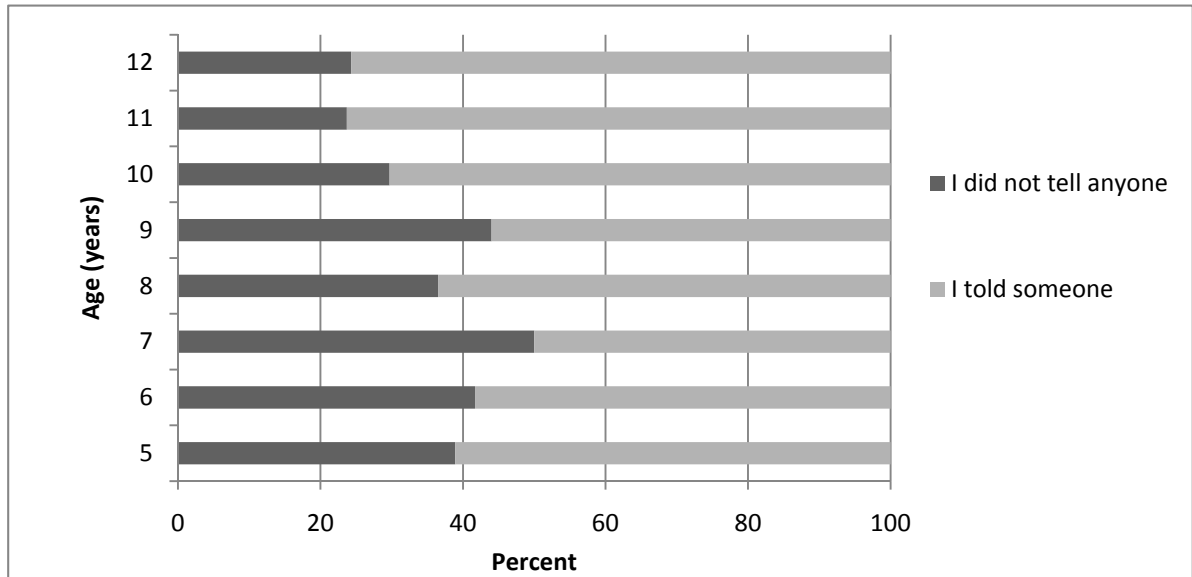
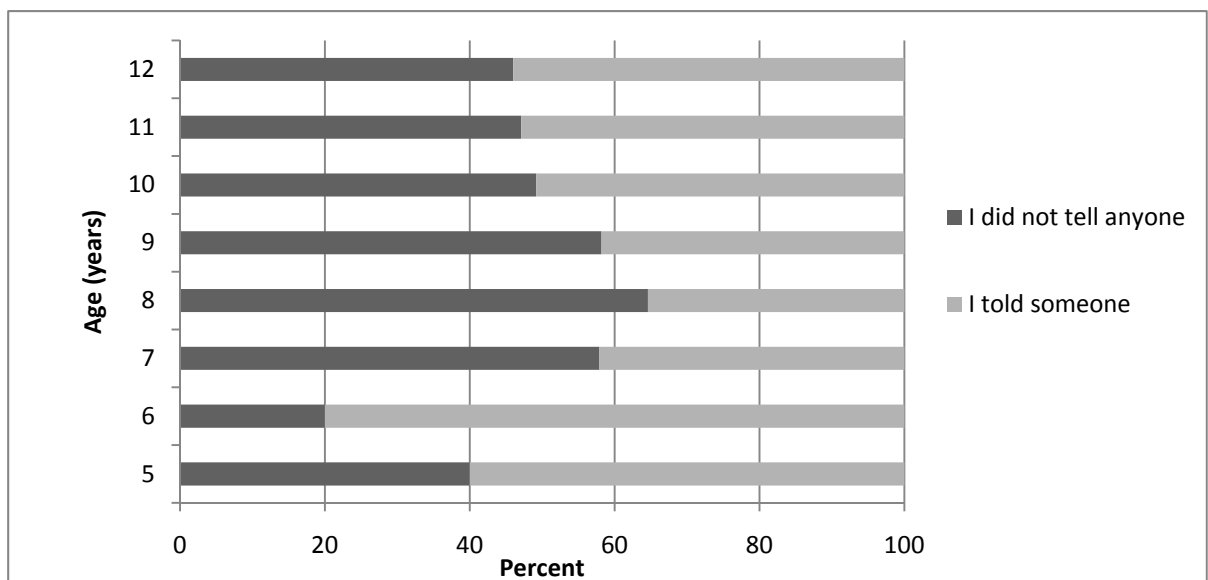
Figure 3.6a Of those cyber-bullied, did they tell someone (*Female, aged 12 years and younger*)Figure 3.6b Of those cyber-bullied, did they tell someone (*Male, aged 12 years and younger*)

Table 3.6a If you were cyber-bullied, did you tell someone? *Aged 5-12 years)*

		I did not tell anyone		I told someone	
Sex		%	#	%	#
5 Years	M	40.0	5	60.0	9
	F	38.9	7	61.1	11
6 Years	M	20.0	0	80.0	4
	F	41.7	3	58.3	7
7 Years	M	57.9	9	42.1	8
	F	50.0	5	50.0	8
8 Years	M	64.6	23	35.4	23
	F	36.5	26	63.5	61
9 Years	M	58.2	81	41.8	66
	F	44.0	67	56.0	102
10 Years	M	49.2	84	50.8	98
	F	29.7	71	70.3	213
11 Years	M	47.1	110	52.9	139
	F	23.7	78	76.3	299
12 Years	M	46.0	97	54.0	129
	F	24.3	93	75.7	320

Figure 3.7 If you were cyber-bullied in the last 12 months, who did you tell? (Aged 13-18 years)

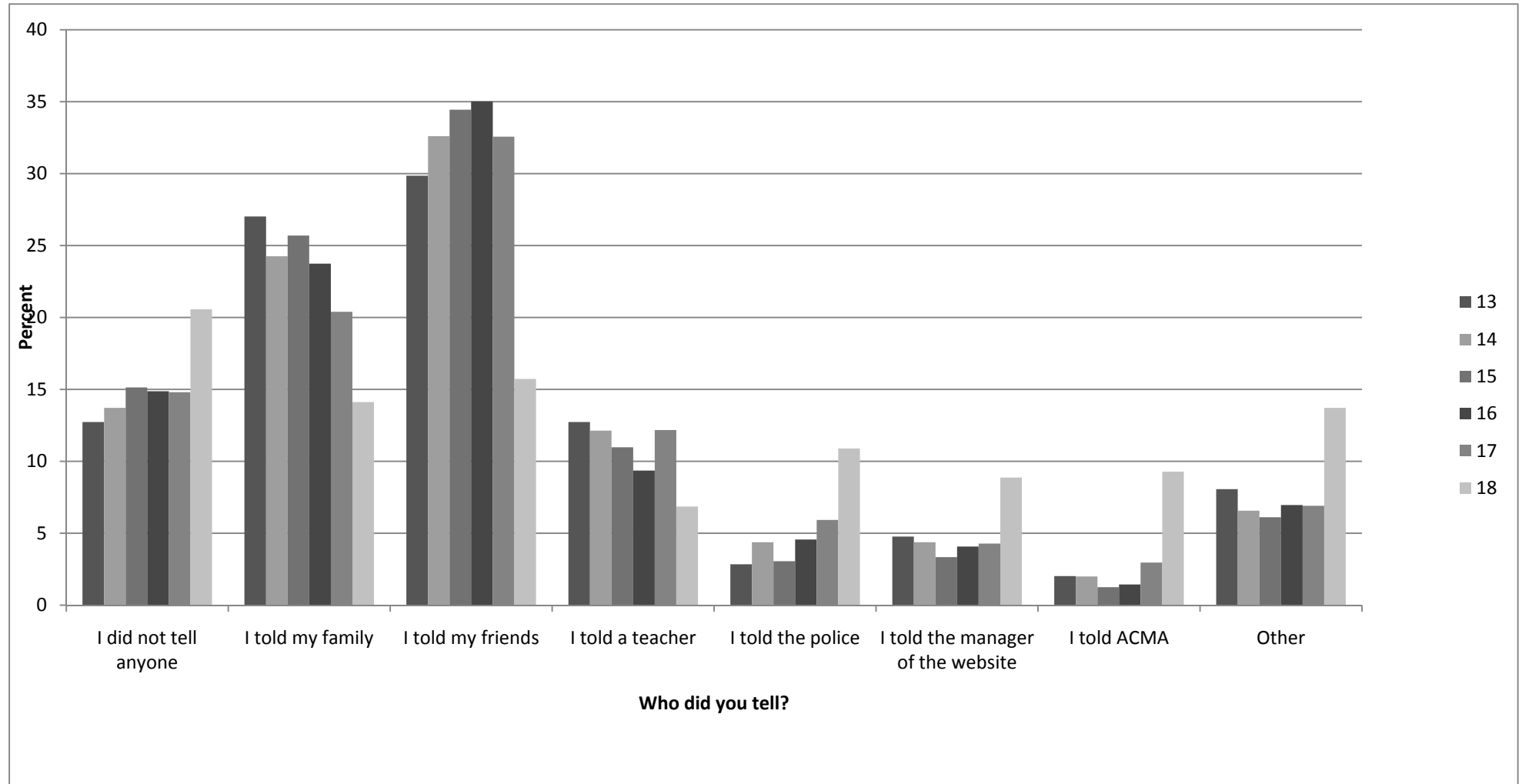


Table 3.6b If you were cyber-bullied in the last 12 months, who did you tell? (Aged 13-18 years)

	Sex	I did not tell anyone		I told my family		I told my friends		I told a teacher		I told the police		I told the manager of the website		I told ACMA		Other	
		%	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#
13 Years	M	35.2	64	47.3	86	41.2	75	21.4	39	7.1	13	14.3	26	6.6	12	7.7	30
	F	19.3	75	53.7	209	64.5	251	25.7	100	4.6	18	6.7	26	2.6	10	14.9	58
14 Years	M	34.6	66	37.7	72	47.6	91	19.4	37	13.6	26	11.5	22	8.4	16	8.7	31
	F	20.3	72	48.5	172	66.8	237	23.9	85	5.1	18	6.2	22	1.1	4	9.9	35
15 Years	M	43.0	68	33.5	53	41.8	66	14.6	23	7.0	11	8.9	14	5.1	8	7.4	20
	F	15.1	41	50.6	132	67.2	182	20.7	56	4.1	11	3.7	10	0.4	1	8.9	24
16 Years	M	41.6	32	29.9	23	46.8	36	14.3	11	7.8	6	13.0	10	6.5	5	6.9	11
	F	18.8	30	47.5	76	68.8	110	17.5	28	8.1	13	4.4	7	0.6	1	11.3	18
17 Years	M	36.4	24	24.2	16	47.0	31	21.2	14	16.7	11	15.2	10	10.6	7	13.5	14
	F	20.2	21	44.2	46	65.4	68	22.1	23	6.7	7	2.9	3	1.9	2	6.7	7
18 Years	M	46.2	24	32.7	17	40.4	21	17.3	9	25.0	13	23.1	12	21.2	11	40.0	20
	F	54.0	27	36.0	18	36.0	18	16.0	8	28.0	14	20.0	10	24.0	12	28.0	14

- 3.105 The coping strategies of respondents aged 13 years or older were not substantially different to their younger counterparts: reaching out to friends and family remain high in this age group.
- 3.106 Differences existed on the rate of seeking revenge, ignoring the bullying and staying offline. The rate of retaliation among male respondents was higher (23.8 percent) in males aged 13 or older sought revenge compared with 12.7 percent of males aged 12 or younger.
- 3.107 Another difference was the rate of ignoring the bullying behaviour: 37.9 percent of males and 44.0 percent of females aged 13 years or older reported ignoring the bully.
- 3.108 Finally, the rate of staying offline as a coping strategy declined in the older age category: 18.1 percent of males aged 13 or older, 17.6 percent of

females aged 13 or older compared to 22.4 percent of males aged 12 or younger; 27.25 percent of females aged 12 years or younger.

3.109 The Australian Institute of Family Studies stated that common coping techniques used by young people experiencing cyber-bullying include denying the seriousness of the experience, avoiding the perpetrator, and acting aggressively towards others online.

- Most young people are reluctant to seek help or tell an adult about their Cyberbullying victimisation. One of the reasons cited for their reluctance is a fear that their access to technology will be taken from them (e.g., that their parents might confiscate their mobile phone or take away their Internet access).
- The use of problem-solving strategies, characterised by organising a plan of action to deal with the issue while remaining optimistic, may lead to de-escalation, while passive coping puts young people at risk of future victimisation.¹²⁵

3.110 The BoysTown study argued that its findings ‘highlight that a critical response to effectively addressing cyberbullying relies on both increasing the help-seeking behaviour of victimised young people and improving the efficacy of those they speak to. While evidence suggests that cyberbullying presents its own unique set of characteristics, it is also important to recognise that it is strongly interrelated with traditional bullying. This suggests a need for interventions that focus on improving peer relations in general’.¹²⁶

Cyberbullying is bullying. It is a complex, deeply embedded social relationship problem. I think the solutions need to look at both prevention and intervention. This calls for legal solutions, for technological solutions, for educational solutions delivered by both the parents and the schools, for more training for preservice teachers and for public health campaigns, but we have no evidence that any of them might work.¹²⁷

125 Australian Institute of Family Studies, *Submission 39*, pp. 3-4, citing Lodge J and Frydenberg E, 2010, ‘Cyber-bullying’ in D J Christie (Ed) *Encyclopaedia of peace psychology*, New Jersey, Wiley Blackwell.

126 Price M and Dalglish J, 2010, ‘Cyberbullying: Experiences, impacts and coping strategies as described by Australian young people’, *Youth Studies Australia*, 29 (2): 51-59.

127 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS6.

i think the thing that we can address is how people RESPOND to bullying. it is much easier to ignore it and to delete that person from your fb, than to respond and get in a fight, but it seems that too often people chose to respond and get themselves into a mess. the bully wants a reaction so bullying would decrease if people didn't respond. other things people need to know about is not to add strangers onto their fb. ALL my friends i know of have added 100+ strangers. also not to 'meet' people online. if something serious happens, people should not be too embarrassed to go straight to their parents or teachers or in some cases police.¹²⁸

3.111 Research by BoysTown has shown that:

... young people used a number of offline and online strategies to address cyber-bullying. The majority of cyber-bullied young people blocked the bully (71%); many of them also decided to remove the bully as a friend (46%) and to confront the bully (44%); almost 40% decided to tell a friend; 32% opted to stay offline or stopped looking at the offending messages or images; and 44% decided to tell an adult (based on individual responses).¹²⁹

3.112 Researchers at Simon Fraser University in Canada found that 74 percent of victims of 'cyberspace infractions' would tell their friends, and 57 percent would tell their parents. Only 47 percent would tell school officials, and 'almost no one' would tell police. About 27 percent of victims would report cyber-bullying to schools, as opposed to 40 percent who would report that they had witnessed it.¹³⁰

3.113 The following comments were made by respondents in response to various questions in the *Are you safe?* survey:

I wasn't affected by the bullying so i didn't really care... I just let it go. If that guy wants to be an idiot that's his choice (Female aged 14).

because i confronted them, the school said, i was bullying them so i was suspended and they got off scott free (Female aged 16).

I sent a report of their behaviour which resulted in them getting banned from the game (Male aged 14).

128 Verity, *Submission 142*, p. 1.

129 BoysTown, *Submission 29*, p.10.

130 Simon Fraser University, *Submission 55*, p. 9.

i spoke to the bully about it, that didnt get me far. i told my friends. then i removed the bully off of my facebook (Female aged 15).

My mother saw it and told me why this was happening and i said i didnt know. She took my facebook away (Female aged 13).

talked it over with my parents and they helped me decide what was the best thing to do or not to do (Female aged 15).

We worked it out. We had both misunderstood each other. We calmed down and stopped acting so aggro, until it had all blown over (Female aged 16).

- 3.114 In the Simon Fraser University study, of the respondents who would not tell school personnel, 30 percent feared retribution from the cyber-bully. This finding appears to contravene much of the current literature which posits that young people are reluctant to report incidents to adults primarily out of fear that time on line will be reduced or taken away.¹³¹
- 3.115 The BoysTown study also reported the effectiveness of these strategies. Notably, 68.5 percent rated that telling a friend was helpful, and 67.5 percent found telling a parent or carer was helpful.

What might have exacerbated the problem is that despite the serious emotional impacts of cyberbullying, over a quarter of victims did not seek support from others nor did they take any action to address the issue. This particular finding by BoysTown is supported by related literature showing that young people are rarely proactive in informing adults about being cyberbullied. In fact, one study found that as many as 90% of victims claimed to have not told an adult. Other studies have yielded similar findings, attributing the inhibition to fears of humiliation and embarrassment; not being believed; concerns about the incident being trivialised; and/or access to technology devices being restricted.¹³²

- 3.116 An extensive research project in Western Australia spoke to nearly 1,000 young people aged between five and 18 years. It revealed that 38 percent

131 Simon Fraser University, *Submission 55*, p. 9.

132 BoysTown, *Submission 29*, p. 10, citing Juvonen J and Gross E, 2008, 'Extending the school grounds? Bullying experiences in cyberspace', *The Journal of School Health*, 78 (9): p. 496; Campbell M, 2007, *Cyber bullying and young people: Treatment principles not simplistic advice*; Smith P, Mahdavi J, Carvalho M, Fisher S, Russell S and Tippett N, 2008, 'Cyberbullying: Its nature and impact in secondary school pupils', *The Journal of Child Psychology and Psychiatry*, 49 (4): 376-385.

of respondents did not have anyone to talk to about bullying, or preferred to keep problems to themselves. The latter response was 'considerably higher' among boys and young Indigenous people.¹³³

Bystanders

3.117 Research has recognised the important role of bystanders in bullying, and the role the peer group plays in reinforcing this behaviour. There are benefits in engaging bystanders to take a stand against bullying by intervening safely but directly, telling a trusted adult, or at least not encouraging the bully/bullies. Bystanders may be easy to influence because they often think that bullying is wrong and would like to do something to help the victim.¹³⁴

3.118 Dr McGrath noted that there is:

a reasonable amount of research which says not only that the children who are either bullying or being bullied are adversely affected by this kind of situation but that all students are affected. We have considerable and building evidence that the kids who witness bullying are, to some extent, as traumatised as the kids who are on the receiving end, to the point where we have studies which can demonstrate a negative impact¹³⁵

3.119 The Australian Psychological Society emphasised the need for children and young people to be part of the solution because while cyber-bullying may occur privately, other students often know about it and thus have the option of intervening.¹³⁶ Converting existing attitudes into positive behaviour is a challenge, and young people need help in understanding their responsibility to intervene when bullying occurs.¹³⁷

Peer education and interventions are important in reducing the impacts of cyber-bullying. The majority of peer interventions have been found to be effective, with the bullying stopping within a short period of time of peer intervention and reconciliation occurring when bystanders intervened.¹³⁸

133 Commissioner for Children and Young People WA, *Submission 54.1*, pp. 1-2.

134 NSW Government, *Submission 94*, p. 26.

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

136 Australian Psychological Society, *Submission 90*, p. 19, citing Cross *et al*, 2009, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, Edith Cowan University.

137 NSW Government, *Submission 94*, pp. 26-27.

138 Australian Psychological Society, *Submission 90*, p. 19, citing Cross *et al*, 2009, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, Edith Cowan University.

- 3.120 Confident bystanders are important because bullies like an audience, whether it is online or at school, but they are most likely to stop when peers show disapproval. Evidence suggests that, when a peer or bystanders do intervene, bullying stops ‘within ten seconds’: much more quickly than if an adult does the same thing. Education is required so that bystanders can be defenders, stand up for victims, or, if that is not possible, walk away to deprive the bully of attention.¹³⁹

Getting you as a bystander to help online is so much easier than if you were in a physical place and too scared to do something by yourself, even though you want to stand up for your friend. If your friend is being publicly humiliated in a chat room, by messaging or on a website, you can privately email or text them and say: ‘This isn’t good. I know everybody really doesn’t say that about you. I’ll see you tomorrow and we’ll try and work something out.’ If they get 10 messages from their peers that say that they know it is happening, we can utilise that technology and the young people to support each other.¹⁴⁰

- 3.121 At the National Day of Action Against Bullying and Violence on 18 March 2011, ACMA promoted the following messages:

- Don’t just stand by. Speak out!
- Protect and support your friends.
- Tell a trusted adult.¹⁴¹

- 3.122 It also staged a national *Cybersmart Hero* event, in which more than 1000 upper primary school students across the country took part in the event. This is an online activity for upper primary students addressing the responsibilities of bystanders, those in the best position to influence bullying and cyber-bullying.¹⁴²

Children need help understanding their social responsibility to intervene when bullying is taking place. For example:

139 *acma(sphere)*, Issue 62, April 2011, p. 6; Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS29; Dr Julian Dooley, *Transcript of Evidence*, 11 June 2011, p. CS28; Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS13. Professor Phillip Slee, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS14.

140 Associate Professor Marilyn Campbell: School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS29.

141 *acma(sphere)*, Issue 62, April 2011, p. 6

142 *acma(sphere)*, Issue 62, April 2011, p. 6.

- peers can be coached in taking a stand when bullying occurs;
- children and young people may need scripts for what to say and do to intervene in a positive way;
- adults need to establish conditions in which children feel responsible, and to encourage children to take the risk of speaking out against bullying;
- adults need to listen respectfully and respond with relationship solutions to empower children to act.¹⁴³

One of the things that came out in our research is that kids just do not know where to go to. When they are cyberbullied – or when they are face-to-face bullied, but we are talking here about cybersafety – they feel humiliated, they feel embarrassed, they feel that they may be blamed for that behaviour because kids will internalise what happens to them. If something happens to them they will blame themselves for that. So, there is a whole range of barriers to them seeking help and then on top of that they do not know where to go to.¹⁴⁴

Who do victims tell?

3.123 The following comments were made by survey respondents in response to questions asking if they told anyone about their experiences:

no tennager willingly goes to their parents to tell them they have been bullied online, ever! so something else, somehow, needs to happen to protect all these people from getting bullied (Female aged 15).

I didn't tell anyone for about a month. But i eventually broke down and ended up telling mum because i couldn't take it anymore. I got depression because of this and didn't want to go to school, i took a whole week off school because I didn't want to be seen (Female aged 14).

i only told my friends. but my dad somehow found out (and no it wasnt through my friends) (Female aged 15).

i told no one but when my mum found out i started telling my family what was really going on (Female aged 15).

143 NSW Government, *Submission 94*, p. 27.

144 Mr John Dalglish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS13.

- 3.124 In 2006, a project began to reduce cyber-bullying experienced by Indigenous children in the mid-west of the Murchison region in Western Australia. Community members, including children and young people spoke about what they called 'bullying', why they think it happens and how it feels to be Indigenous and bullied. This led to development of a website that provides evidence-based and culturally appropriate information on strategies for young Indigenous people, schools and families.¹⁴⁵ There is only limited knowledge of how young Indigenous Australians use technology for traditional and cultural purposes.
- 3.125 BoysTown is interested in exploring the use of technology for seeking help.¹⁴⁶ It has suggested that:
- the Australian Government work in collaboration with community services to develop an awareness raising strategy that targets children and young people to:
- a) Encourage them to speak out about cyberbullying and other cybersafety concerns to trusted adults and;
- b) Informs them about available services that can assist in ameliorating the impacts of cyberbullying and other cybersafety issues and in particular, in view of their effectiveness, telephone and online counselling resources'.¹⁴⁷
- 3.126 Two additional matters should be noted.
- 3.127 Ms Robyn Treyvaud expressed the view that because of the technological focus, there was not enough emphasis on decisions enhancing lives, friendships, or acquisition of information. She referred to a 'moral compass', the test for which was what an individual did when no one else was watching. Thus, young people are not watched at their computers and no one holds them responsible for their actions. Much anti-social and mean behaviour is driven by whether perpetrators think that they are likely to be caught.¹⁴⁸

In many cases, children who bully others are asserting their social power and have learned to use that power aggressively. The challenge is to redirect this leadership potential from the negative strategies of bullying to positive leadership skills and

145 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS5.

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

147 BoysTown, *Submission 29*, p. 12.

148 Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS35.

opportunities. These children require support to find positive ways of gaining power and status within their peer relationships. They need to be provided with formative rather than punitive consequences. Interventions should provide a clear message that bullying is unacceptable, but also build awareness, skills, empathy and insights and provide appealing alternatives to bullying.¹⁴⁹

- 3.128 The Alannah and Madeline Foundation saw cyber-bullying as a matter of personal behaviour, rather than of the misuse of applications in the online environment. It believed that responses to the problem were best focused on changing behaviour in schools and beyond. These were most effective when developed collaboratively, involving the victim, his/her school, the perpetrator(s), parents/carers, appropriate representatives of the online environment and the wider community. This whole-of-community approach will be addressed in Chapter 10.¹⁵⁰

The critical factor is that with bullies we have a small percentage who continue, no matter what we do, and those young people may go on to other antisocial or deviant pathways.¹⁵¹

- 3.129 The NSW Government commented that, given the vulnerabilities of children in out-of-home care, an interagency response may be required, regardless of whether the person is a victim or a perpetrator.¹⁵²

- 3.130 The Australian Youth Affairs Coalition stated that:

A coordinated approach is adopted so that young people, parents and schools are involved in the process of raising awareness of risks and developing measures to counter inappropriate behaviours online.¹⁵³

- 3.131 Professor Phillip Slee suggested the use of the available technology to send out anti-bullying messages.¹⁵⁴

I think a lot of young people were well aware of the well-publicised risks like cyberbullying and those sorts of things, but a

149 NSW Government, *Submission 94*, p. 26.

150 Alannah and Madeline Foundation, *Submission 22*, p. 19; Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS5.

151 Dr Barbara Spears, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS14.

152 NSW Government, *Submission 94*, p. 29.

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

154 Professor Phillip Slee, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS17.

lot of young people were not really aware of what happens to their information once it is put online. They are not aware that other people can access their information. They view their Facebook profile as their personal space and do not realise that others can access it, and the longevity of that – something they say in the heat of the moment can be there forever. I think that was the biggest thing that came through around their understanding of it.¹⁵⁵

bullies from other schools, there are ways and means of dealing with that, if the bullying constitutes significant harm. There are always friendly agreements between neighbouring principals.¹⁵⁶

3.132 Professor Bjorn Landfeldt commented that:

there is definitely a place for law enforcement agencies, but it should not really get that far. If it gets that far it would be a very unusual case, I would assume. I would assume that in most cases it is something that goes on in the school environment or between students in a school, and the local community, the immediate community, should be able to deal with it. If they are not able to deal with it, they should have clear guidelines on how to deal with it. If they cannot, maybe they should escalate it to law enforcement agencies but also have definite and clear guidelines and responsibilities for law enforcement agencies, if they get such a matter tabled.¹⁵⁷

3.133 The Australian Institute of Criminology pointed out that there is ‘relatively little’ research on how young people, or their parents/carers, deal with or respond to risks in the online environment.¹⁵⁸ It believed that research tended to focus on the incidence of the abuse rather than on its consequences, such as coping strategies or the long-term effects of exposure to risks.¹⁵⁹ Yahoo!7 also commented that ‘research into the prevalence and scale of online safety risks would greatly inform and shape the debate around which safety measures would be more effective in managing these risks.’¹⁶⁰

155 Mrs Tiffany Downing, Director, Office of Youth, *Transcript of Evidence*, 3 February 2011, p. CS19.

156 Mr Michael Wilkinson, Executive Secretary, Queensland Catholic Education Commission, *Transcript of Evidence*, 17 March 2011, p. CS28.

157 Associate Professor Bjorn Landfeldt, University of Sydney, *Transcript of Evidence*, 24 March 2011, p. CS30.

158 Australian Institute of Criminology, *Submission 56*, p. 13.

159 Ms Samantha Yorke, Legal Director, Yahoo!7, *Transcript of Evidence*, 8 July 2010, p. CS23.

160 Yahoo!7, *Submission 2*, p. 2.

- 3.134 Dr Julian Dooley commented that the first empirical trial has been set up to examine the effectiveness of resources devoted to cyber-bullying work, and to determine whether messages schools and parents/carers are asked to deliver are enhancing cyber-safety. However, one of the challenges to increasing cyber-safety in Australia is that, except to an extent on cyber-bullying and some work on what is sometimes known as 'Internet addiction', little other research is being carried out.¹⁶¹ There is a considerable focus on some online abuses, while others such as 'required' fields in documents have received little attention. This abuse has implications for the collection of unnecessary personal information.¹⁶²
- 3.135 Some schools in the United Kingdom have introduced peer mentoring for students in relation to cyber safety matters. In the British system, fellow students, in a model similar to school prefects, are identified as being able to assist others with cyber-safety issues.

Recommendation 3

That the Minister for Broadband, Communications and the Digital Economy and the Minister for School Education, Early Childhood and Youth work with the Ministerial Council for Education, Early Childhood Development and Youth and the Australian Communications and Media Authority to investigate the feasibility of developing and introducing a cyber-safety student mentoring program in Australian schools.

Committee comments

- 3.136 While there are no specific sanctions for cyber-bullying in most Australian jurisdictions, the more serious cyber-bullying activities will often contravene other relevant legislation. These sanctions are dealt with in Chapter 11.

161 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS39.

162 Victorian Privacy Commissioner, *Submission 59*, p. 4.

Cyber-stalking, online grooming and sexting

- 4.1 Cyber-stalking, online grooming, sexting and illegal and inappropriate content all represent significant cyber-safety and are the focus of this chapter. The prevalence, impact and sanctions and research status of these activities is also discussed. Sanctions against these abuses are set out in Chapter 11.

Cyber-stalking

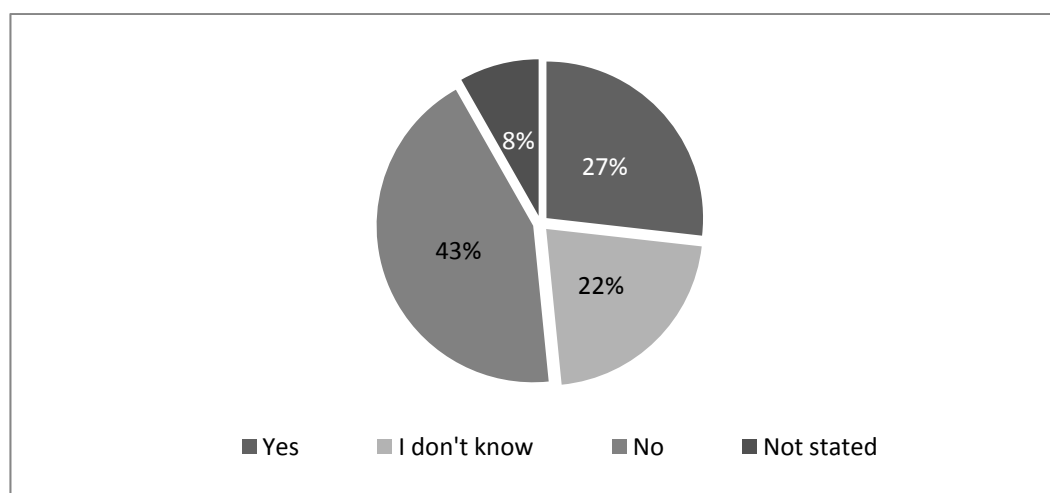
Cyber-stalking and grooming are emerging phenomenon that often do not have their origins offline unlike cyber-bullying ... Those who received sexual solicitations were more likely to share personal information with strangers online and engage in offline risky behaviours.¹

- 4.2 According to the Australian Institute of Criminology, cyber-stalking can include:
- Sending repeated unwanted messages using email and SMS, or posting messages on blogs, profiles on social networking sites;
 - Ordering goods and services on behalf of a victim that could result in legal and financial losses to the victim, including to her/his reputation;
 - Publicising private information about a victim;
 - Spreading false information;
 - Gathering information online about a victim;

1 Peer Support Australia, *Submission 48*, p. 6.

- Encouraging others to harass a victim; and
 - Unauthorised access to a victim's computer(s) or Internet accounts (e.g. email and social networking site accounts).²
- 4.3 Cyber-stalking is harassing behaviour using one or more of the platforms in the online environment. It can include frequent and intrusive threats, cryptic messages and sexual innuendo. Its usual goal is to create a sense of fear in the recipient based on control and intimidation. Some adult predators pretend, by creating fake profiles with false ages and identities, to be a young person to befriend and gain the trust of young people online.³
- 4.4 There appears to be a relationship between bullying and stalking, as episodes are sometimes preceded by bullying behaviour.⁴
- 4.5 Young Australians appear unsure of what cyber-stalking involves. Participants in the Committee's *Are you safe?* survey aged 13 years or older were asked if repeatedly accessing a stranger's Facebook page is stalking. Of the survey's participants in this age category, 26.8 percent believe that this conduct is stalking, 43.4 percent believe that it is not, and 21.6 percent are unsure. The remaining 8.2 percent of respondents did not answer the question.

Figure 4.1 Is repeatedly accessing someone's Facebook page stalking? (*Aged 13 years and older*)



2 Australian Institute of Criminology, *Submission 56*, p. 10 citing Mullen PE, Pathé M and Purcell R 2009. *Stalkers and their victims (2nd ed)*. Cambridge: Cambridge University Press.

3 See Attorney-General's Department, *Submission 58*, p. 4; Ms Sonya Ryan, *Transcript of Evidence*, 3 February 2011, p. CS59. Cyber-stalking may also become sexual grooming: see below.

4 Mental Health Council of Australia, *Submission 52*, p. 4 citing Purcell R, Flower T, Mullen P, 2009, 'Adolescent stalking: Offence characteristics and effectiveness of intervention orders', *Trends and Issues in Crime and Criminal Justice*, 369. Canberra, ACT.

Table 4.1 Is repeatedly accessing someone's Facebook page stalking?

	Yes		No		I don't know		Not stated		Total
	%	#	%	#	%	#	%	#	#
Male	29.9	1855	48.5	3013	19.8	1230	1.8	109	6207
Female	27.6	2108	45.1	3446	26.2	2001	1.1	82	7637
Gender Not Stated	11.6	196	16.3	274	7.6	128	64.5	1086	1684
Total	26.8	4159	43.4	6733	21.6	3359	8.2	1277	15528

4.6 The wealth of personal information and pictures online can potentially be used by individuals and sexual predators to identify, locate, contact, stalk and harass their victims. More than half of victims and offenders did not have prior relationships, probably because of the ease of locating victims online. Opportunities for cyber-stalking may increase with age, as older students will have greater access to platforms in the online environment.⁵

When engaging with the pre-teen audience, particularly younger children aged between 5 and 10, Childnet's privacy messages focus on the importance of keeping personal information, such as full name, email address, phone number, home address, photos, school name and passwords, private. The 2010 Safer Internet Day message of "Think Before You Post" is particularly important for those who frequently use social media services like Facebook. Information and images online have longevity and an incredible reach, which should be factored into any decision to post content and Childnet encourages all users to think about the possible implications and impact of their posts.⁶

4.7 People with online profiles are more likely to be harassed and bullied online, and to receive personal messages via email, instant messaging chat or text messages from strangers, than those without such profiles. Those

5 Australian Institute of Criminology, *Submission 56*, p. 9 citing Slonje R and Smith PK, 2008, 'Cyberbullying: Another main type of bullying?' *Scandinavian journal of psychology* 49(2): 147-154.

6 Childnet International, *Submission 18*, pp. 3-4.

who have posted photographs of themselves and created profiles on social networking sites are more likely to have been contacted online by people that they do not know. Girls are significantly more likely than boys to be contacted by someone they do not know.⁷

Genuineness of others online

i was chatting to a friend of mine, but slowly realised that it didn't seem like her. i asked and they replied that they were her cousin. without writing anything else i signed of and deleted that account (Female aged 16).

- 4.8 BraveHearts noted that meeting and corresponding with new people is an exciting aspect of the online environment. However, the Child Exploitation and Online Protection Centre found in 2007 that, of the eight million children in the United Kingdom with Internet access, one in 12 admitted to meeting someone they had initially met online.⁸ An Australian Institute of Criminology study in 2009 reported that 7 percent of young people reported that they had met someone offline, after meeting them online.⁹
- 4.9 BraveHearts noted that 24 percent of the young people in an Australian Institute of Criminology study published in 2009 reported that the person who had purported online to be a child was an adult. BraveHearts believed that meeting a person only previously encountered online is 'one of the most dangerous things' young people can do.¹⁰
- 4.10 Predators can often use the identities of professional musicians and celebrities to lure young people into conversations online because of their popularity among targeted age groups. Ms Sonya Ryan said that she has received 'hundreds' of emails from children seeking help, too afraid to talk to their parents in fear of punishment or removal of technology, or because they are embarrassed. She has also been contacted by parents who

7 Australian Institute of Criminology, *Submission 56*, p. 9, citing Cox Communications, 2007, www.cox.com/TakeCharge/includes/docs/survey_results_2007.ppt

8 BraveHearts, *Submission 34*, p. 6, citing Choo K, 2009, 'Online Child Grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences', *Canberra, Australian Institute of Criminology Research and Public Policy Series No. 103* and Child Exploitation and On-line Protection Centre, 2007, available at <http://www.ceop.gov.uk/>

9 BraveHearts, *Submission 34*, p. 6.

10 BraveHearts, *Submission 34*, p. 6.

do not know what to do, and are looking for information because they do not know what their young people are doing online.¹¹

- 4.11 With implications for their safety and their privacy, many young people have no knowledge:
- of the terms and conditions of access to social networking sites;
 - about privacy settings being continuously updated without notification;
 - that, if they have devices that are enabled for access to Global Positioning System, they can be found through photographs posted on their Facebook pages, or
 - about the different Facebook applications that give details of where someone has logged on, via Google Maps for example, so that potential predators could locate other people while they are on computers or a social networking sites.¹²

Prevalence

- 4.12 The prevalence of cyber-stalking in Australia is not known because little research has been published. It is therefore difficult to estimate how many young people are subject to this abuse. One study indicated that 5 percent of people overall are stalked online. Combined estimates from Australia, the United States and the United Kingdom indicate that about 7 percent of people are victims of cyber-stalking.¹³
- 4.13 iKeepSafe referred to a European Union study that showed meeting a stranger online was the 'least common risk': about 9 percent (one in 11), rising to one in five in some Eastern European countries. However, in several (unspecified) countries 15 to 20 percent of teenagers reported 'a degree of unease', or feeling uncomfortable or threatened online.¹⁴
- 4.14 The Committee's *Are you safe?* survey asked its respondents aged between five and 18 years of age, if they feel unsafe online. Female respondents reported higher rates of feeling unsafe than their male counterparts:

11 Ms Sonya Ryan, *Transcript of Evidence*, 3 February 2011, pp. CS59, 64, 72.

12 Ms Sonya Ryan, *Transcript of Evidence*, 3 February 2011, p. CS59.

13 Mental Health Council of Australia, *Submission 52*, p. 4, citing Cross *et al*, 2009, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, Edith Cowan University.

14 iKeepSafe, *Submission 101*, p. 5.

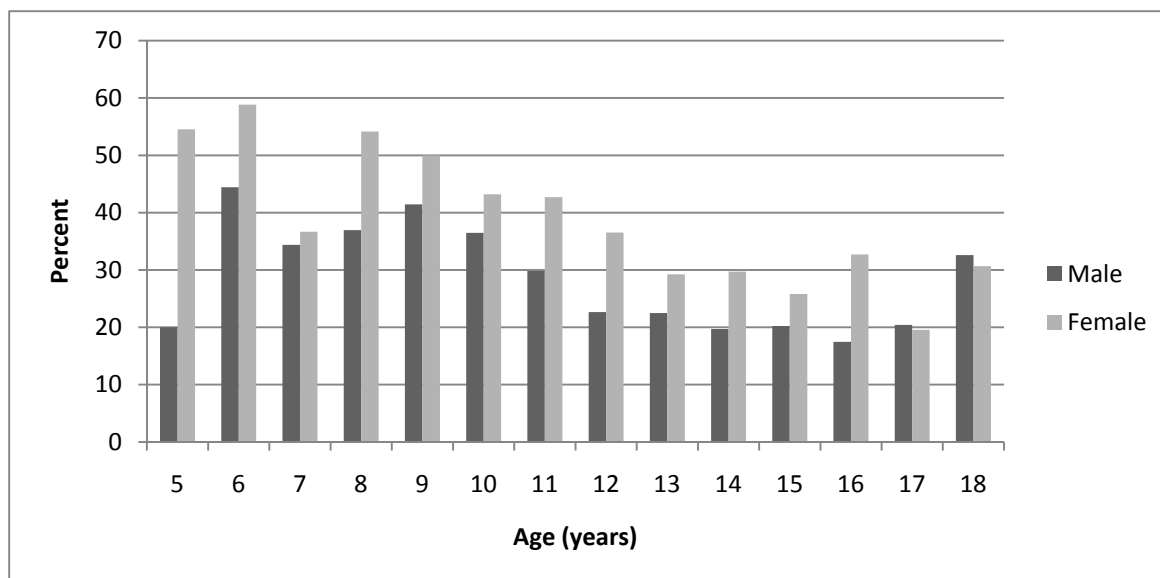
Figure 4.2 Proportion (%) of those who have felt unsafe online (*Age and gender*)

Table 4.2 Do you feel unsafe online?

		Yes		No	
Sex		%	#	%	#
5 Years	M	36.0	27	64.0	42
	F	32.9	27	67.1	46
6 Years	M	33.3	16	66.6	27
	F	37.5	24	62.5	37
7 Years	M	35.5	39	64.5	60
	F	39.2	38	60.8	51
8 Years	M	36.8	156	63.2	221
	F	45.4	224	54.6	230
9 Years	M	36.0	361	64	554
	F	46.1	497	53.9	514
10 Years	M	29.0	493	71.0	1084
	F	41.8	752	58.2	953
11 Years	M	26.2	603	73.8	1585
	F	37.4	935	62.6	1459
12 Years	M	22.3	499	77.7	1650
	F	33.1	749	66.9	1428

	Sex	Yes		No	
		%	#	%	#
13 Years	M	22.2	420	77.8	1470
	F	31.6	775	68.4	1681
14 Years	M	21.3	343	78.7	1269
	F	31.1	617	68.9	1365
15 Years	M	21.4	255	78.6	936
	F	31.5	433	68.5	941
16 Years	M	17.1	138	82.9	669
	F	29.7	296	70.3	702
17 Years	M	23.0	91	77.0	304
	F	29.4	167	70.6	401
18 Years	M	28.8	90	10.0	222
	F	30.5	79	21.0	180

4.15 Respondents in the *Are you safe?* survey explained their reasons for feeling unsafe when online:

A few unknown people have added me before or talking to me on a social networking sites, but most of them seemed harmless but all of them I blocked and haven't heard from since (Female aged 15).

A man contacted me after I posted on a public thread on Facebook. I thought nothing of it until recently, when he wanted to be more than just friends (Female aged 15).

A man on facebook sent me an 'inbox' message. Who I didn't know. And didn't plan on. He told me to add him as a friend and that I was beautiful and stuff... (Female aged 14).

About a month ago I went on msn and had heaps of friends that I knew that wanted to add me. While I was accepting the ones I knew and declining the ones I didn't, I accidently accepted one I didn't know. When I saw that I'd added them, I messaged them and said "Hey, do I know you?" They replied by saying "Noo. Well, sort of." But I honestly didn't know this person, I had never met them or even heard of them. Anyway, I left the room with my friend and I left for about 2 hours and completely forgot about my msn. When I got back in my room I remembered and

went and checked it. When I looked at my chat screen with this person, there was a massive amount of abuse towards me on there. Such as threatening to rape me, then kill me, and then eat my flesh. I was so scared. I still am today, I'm afraid that this person knows a lot about me, knows what school I go to or knows where I live and that they are going to come and do what they said. It's scary going through that thought everyday (Female aged 15).

i feel uncomfortable when people that have no mutual friends try to get me to be their friends. how did they find me? (Female aged 13).

I feel unsafe at times because there is always evidence of what you do on the net (Male aged 14).

I googled myself as a joke, to look at others with the same name as me... but i found pictures of myself on there aswell. This freaked me out (Female aged 15).

I have a close friend who, a few years ago, was not very careful with posting personal information on the Internet. The issue has since been resolved, but at the time I was quite worried that her carelessness was putting us both in danger (Female aged 16).

I have had a recent issue with a group of girls who have threatened me, thus feeling unsafe (Female aged 17).

- 4.16 Some respondents went on to explain the dangers they perceive when asked why they feel unsafe:

I believe that the cyber world is a dangerous place and I believe that the amount of information about yourself and other without their permission should be kept to a minimum or should not be expressed in the cyber world (Female aged 16).

I love being online talking to friends. But there are the chances of something bad happening. My parents always warn and inform me to be aware when being online for e.g. don't tell anybody your personal details (Female aged 15).

- 4.17 Conversely, those that feel safe online, commented through free text spaces their reasons for feeling safe:

I don't [feel unsafe] because all of my accounts have the highest security settings and my parents check my accounts regularly (Female aged 13).

I don't feel unsafe because I'm aware of the dangers. I do not have Facebook or other exposing things like Twitter, MySpace. The only thing I have is MSN which I'm really safe with and I don't use it that often. The detail I put on there is very limited even to my friends because I do not know what the dangers of a predator are and if my friends are really my friends. I do not talk to strangers and ask my friends if they have MSN and add them myself (Female aged 13).

I don't have any online accounts that I use except for a family shared email account and my own. Therefore my family can always see who I'm keeping in touch with (Female aged 13).

I don't have Facebook or any of those things because I don't like them but I don't think that they are safe either. They aren't safe because people can track you down and you have to put some information on that you shouldn't be asked to show (Female aged 13).

I have always been very careful on the internet and make sure I'm not putting myself in a dangerous situation (Male aged 13).

I think that the internet can be a safe place if you know how to use it properly. For example if you are using a site like Facebook it is very important that you know who you are talking to when you are in a chat room and only accept people as friends if you know them like your family members and close friends (Female aged 13).

If you reject people you don't know, and control and limit the information you put up there, it is a safer way to be. I don't go out looking for strangers on the internet (Female aged 16).

Impact

- 4.18 By using fake profiles and false ages, criminals lured young people such as Carly Ryan and Nona Belomesoff to their deaths in Australia, and there have been 'a number' of similar cases in the United Kingdom. Although murder is not always the outcome, rapes, assaults and kidnappings can result from cyber-stalking.¹⁵ Further, cyber-stalking may progress to sexual grooming.¹⁶

15 Ms Sonya Ryan, *Transcript of Evidence*, 3 February 2011, p. CS59.

16 Attorney-General's Department, *Submission 58*, p. 4.

- 4.19 Mr Mark Newton commented on the impact that cyber-stalking can have on the target:

The aim of a stalker is to undermine the victim's sense of personal security. A stalker will use any means available to carry out their task: Physical presence, telephone calls, letters, text messages: Anything that makes the victim think about the stalker ... The online world can also assist a stalker by providing access to any parts of the victim's life which have been published online with inadequate privacy: Blogs, networks of acquaintances stored by social networking sites, photographs on personal websites. Any personal information the victim has published during the entirety of their pre-stalked life can aid the stalker.¹⁷

- 4.20 Ms Candice Jansz cautioned that on average young people's profiles on social networking sites contain 40 separate pieces of personal information including full names, ages, contact details, sexual experience and relationships.¹⁸

Such exposure in what is an essentially public setting, can leave young people open to potentially unsavoury consequences, including but not limited to damage to their long-term reputations and employment prospects, cyberbullying and online solicitation.¹⁹

- 4.21 The Mental Health Council of Australia believed that cyber-stalking was a risk area that posed great risks to the mental health of young people, both immediately and chronically.

- 4.22 The National Children's and Youth Law Centre's Lawmail service had received Lawmails relating to threat or concerns about a stalker:

Community legal education should be increased to make young people aware that such threats are not tolerated by the law and will be taken seriously by police.²⁰

- 4.23 Similarly, the NSW Primary Principal's Association commented:

In Primary schools, children's names are regularly reported in documents such as newsletters and Annual School Reports - this could potentially put them at risk of harm as these documents are now published on school websites. A child's name combined with

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

18 Ms Candice Jansz, *Submission 44*, p. 3.

19 Ms Candice Jansz, *Submission 44*, p. 4.

20 National Children's and Youth Law Centre, *Submission 138*, p. 6.

knowledge of the suburb in which they live could potentially give a person sufficient details to contact a child via a social networking site at home. Schools are now considering ways to protect children's identities to avoid the possibility of being contacted online inappropriately.²¹

Sanctions against cyber-stalking

- 4.24 All Australian jurisdictions have laws dealing with cyber-stalking. Victoria and Queensland have explicitly extended the definition of the crime to include the sending of electronic messages. State/Territory jurisdictions can also rely on offences in the Commonwealth Criminal Code which directly address these abuses.²² These offences are listed in Appendix E.
- 4.25 Sanctions for cyber-stalking are dealt with in more detail in Chapter 11 where legislative options are considered.

Sexual grooming

- 4.26 Sometimes known as 'child grooming' or 'online grooming', sexual grooming refers to a range of calculated behaviours designed to make it easier for an offender to procure a young person for sexual activity.
- 4.27 While technology has not been shown to substantially increase the number of paedophiles (older people with a pathological interest in children/young people), it has sped up the process and intensity of sexual exploitation. Potential offenders do not now have to look around their neighbourhoods to gain access to a child or a young person, as personal information is easily found about individuals online. Targets are easily found.²³

Most offenders who initiate sexual contact via the Internet met their victims in chat rooms.²⁴

- 4.28 Before a subject is targeted, it may be preceded by cyber-stalking. For example, an offender might build a relationship of trust with a child and

21 NSW Primary Principal's Association Inc, *Submission 69*, p. 3.

22 Attorney-General's Department, *Submission 58*, pp. 3-4.

23 Alannah and Madeline Foundation, *Submission 22*, pp. 19- 20.

24 Mental Health Council of Australia, *Submission 52*, p. 4 citing Cross *et al*, 2009, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, Edith Cowan University.

then seek to sexualise that relationship by encouraging romantic feelings, or by exposing the child to sexual concepts through pornography.²⁵ There is:

... a subgroup of the whole – a very small proportion – who actually go through and, if you like, consummate the relationship. They do this even once they become aware that the person on the other end of the conversation is not actually a 23-year old but, rather, a 45-year old, for argument's sake. They still feel that there is something in that relationship that meets whatever needs they feel they have. It is a very alarming and unfortunate subset of kids.²⁶

4.29 The Youth Affairs Council of South Australia added that:

In fact, research suggests that in the majority of online sexual solicitation cases referred to police, adult offenders are honest about being an adult, and are honest about their intentions to have sex with the young person they have solicited.²⁷

4.30 Research has shown that 75 percent of young people who meet the adult physically do so on more than one occasion:

This suggests that offenders are using young people's natural curiosity towards sex and sexuality to build relationships – no matter how inappropriate – rather than coercing or threatening young people.²⁸

4.31 The Alannah and Madeline Foundation expressed concern that:

Young people are often unaware of the offline consequences of their online actions. Adolescents who are vulnerable for a variety of reasons and who may be having trouble at school or at home tend to engage in the most serious risk-taking online. They are the group that is the least likely to self-protect online by guarding passwords, or showing caution in posting pictures and so forth.²⁹

25 Attorney-General's Department, *Submission 58*, p. 5; Alannah and Madeline Foundation, *Submission 22*, p. 19.

26 Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association, *Transcript of Evidence*, 11 June 2010, p. CS31.

27 Youth Affairs Council of South Australia, *Supplementary Submission 25.1*, p. 9, citing Ybarra M and Mitchell K, 2008, 'How risky are social networking sites? A comparison of Places Online where youth sexual solicitation and harassment occurs', *Pediatrics* 121: 350-357.

28 Youth Affairs Council of South Australia, *Supplementary Submission 25.1*, p. 9, citing Ybarra M and Mitchell K, 2008, 'How risky are social networking sites? A comparison of Places Online where youth sexual solicitation and harassment occurs', *Pediatrics*, 121: p. 355.

29 Alannah and Madeline Foundation, *Submission 22*, p. 21.

- 4.32 Children have always been at a higher risk of being the prey of older people with a pathological interest because of their incomplete social and emotional development:

Unfortunately, not everyone is honest about who they are and children and young people can be particularly susceptible to trusting people on-line. The reality is that there are predators who pretend to be a young person in order to befriend and gain the trust of children and young people. Twenty-four percent of the young people in findings discussed in Choo (2009) reported that the person they met had presented themselves as a child on-line, but had turned out to be an adult.³⁰

- 4.33 While some children engage in inherently risky behaviour, those with 'low self-esteem, lack of confidence and naivety' are more at risk and likely to be targeted by offenders.³¹

We increasingly live in a society where online users are forced to enter their personal data to access services, purchase goods or interact with one another. Nothing online is private and in fact every keystroke leaves a digital footprint. Law enforcement agencies find this digital footprint useful and increasingly use it to track arrest and bring offenders of many persuasions to account.³²

- 4.34 The South Australian Police use a number of methods for policing suspicious communications between adults and children including covert and under-cover operations and these matters are referred to other law enforcement agencies where there is a jurisdictional nexus.³³

- 4.35 When asked if they have ever felt unsafe online, the Committee received comments from female respondents addressing attempted sexual grooming:

I have occasionally recieved friend requests from strangers through social networks Myspace and Facebook. They are generally male, and

30 BraveHearts, *Submission 34*, p. 6, citing Choo K, 2009, 'Online Child Grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences', *Canberra, Australian Institute of Criminology Research and Public Policy Series No. 103*. .

31 Alannah and Madeline Foundation, *Submission 22*, p. 19 citing Australian Institute of Criminology, 2009, research: www.aic.gov.au/publications/current_series/tandi/361-380/tandi379.aspx.

32 Alannah and Madeline Foundation, *Submission 22*, p. 26.

33 South Australia Police, *Submission 86*, p. 2.

middle-aged. I never accept. However, they can (and sometimes have in the past) contacted me via the 'message' section, which freaks me out (Female aged 17).

i dont like men looking at my profile, not knowing who they are, it freaks me out! i have trued to put my account on private but im not sure how (Female aged 13).

I am almost 18 so I feel like I would be less of a target for paedophiles and the like, so I feel more comfortable putting up details like my age and the school I attended. I don't think this should be done by younger children and teenagers who are more at threat (Female aged 17).

Prevalence

- 4.36 About 75 percent of young people who are sexually solicited online were able to deal with approaches because they had strategies to block them and it did not bother them.³⁴

The degree to which children are targeted for online sexual purposes is difficult to determine because of its illegal nature and the secretive behaviours of both perpetrators and victims. Child victims are unlikely to report for the same reasons they do not report bullying: shame, fear that adult intervention will make the problem worse or that their access to favourite applications will be removed.³⁵

- 4.37 The Australian Institute of Criminology provided the following summary of the available statistics:

Until 2007, there have been over 130 completed prosecutions for online procuring, grooming and exposure offences in Australia (Griffith & Roth 2007). The number of police investigations into online child exploitation has increased considerably in recent years. Statistics compiled by the Commonwealth Director of Public Prosecutions indicated that in the financial year 2008-2009, there were;

- two Summary (Charges) and 18 Indictable (Charges) under Section 474.26 Criminal Code 1995 (Cth) - Using a carriage service to procure persons under 16 years of age'; and

34 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS28; Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association, *Transcript of Evidence*, 11 June 2010, p. CS31.

35 Alannah and Madeline Foundation, *Submission 22*, p. 20.

- five Summary (Charges) and 15 Indictable (Charges) under Section 474.27 Criminal Code 1995 (Cth) – Using a carriage service to “groom” persons under 16 years of age (CDPP 2010).³⁶

4.38 Mr Bruce Arnold pointed out that, while sexual grooming certainly occurs in Australia, most molestation of children is independent of the Internet, and of strangers.³⁷ The Youth Affairs Council of South Australia reported that ‘the type of sexual solicitation most often reported by the media, and most dreaded by parents and caregivers – that of the adult stranger targeting a young person – is very rare’.³⁸

The experience of the stranger danger” in real world settings is instructive here. The focus on stranger danger initially adopted by authorities was eventually discarded when it became clear that the most common source of adult abuse of children was from adults known to them.³⁹

4.39 Adolescents are in fact more at risk from parents/carers, cousins, older siblings or babysitters, rather than from the unknown ‘monster behind the modem’.⁴⁰ The Youth Affairs Council of South Australia commented:

There are four common misconceptions raised by adults when considering the sexual solicitation of young people online: that adults who sexually solicit young people online conceal their identity and trick or coerce young people into meetings; that the majority of sexual solicitations are directed at children, rather than adolescents; that social networking sites the online places young people are in most danger of receiving unwanted sexual solicitations; and that it is predominantly older adults who target and solicit children and young people. Not one of these assumptions is supported by any of the existing research into online victimisation of young people.⁴¹

36 Australian Institute of Criminology, *Submission 56*, p. 5 citing Griffith G and Roth L, 2007, ‘Protecting children from online sexual predators’, *NSW Parliamentary Library briefing paper* no. 10/07. Sydney: NSW Parliamentary Library, [http://www.parliament.nsw.gov.au/prod/parlament/publications.nsf/0/3043E49AB3F4ABF9CA2573530006F989/\\$File/Dealing%20with%20Online%20PredatorsFINAL&INDEX.pdf](http://www.parliament.nsw.gov.au/prod/parlament/publications.nsf/0/3043E49AB3F4ABF9CA2573530006F989/$File/Dealing%20with%20Online%20PredatorsFINAL&INDEX.pdf) and Commonwealth Director of Public Prosecutions, 2010, *Annual report 2008 – 2009*, <http://www.cdpp.gov.au/Publications/AnnualReports/CDPP-Annual-Report-2008-2009.pdf>

37 Mr Bruce Arnold, *Submission 60*, pp. 5-6.

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

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

40 Mr Bruce Arnold, *Submission 60*, p. 6.

41 Youth Affairs Council of South Australia, *Supplementary Submission 25.1*, p. 4.

- 4.40 The Youth Affairs Council of South Australia highlighted some related research:

Additionally, research suggests that those young people who are more likely to take significant risks online– such as responding to sexual solicitation – are also more likely to take risks in other areas of their lives. Young people who take such risks often demonstrate characteristics including elevated rates of substance use, involvement in offline victimisation, perpetration of relational, physical, and sexual aggression, a propensity to respond to stimuli with anger, poor emotional bonds with caregivers, and poor caregiver monitoring.⁴²

- 4.41 The National Children’s and Youth Law Centre noted that:

Although statistically, most child sex abuse takes place within the family or social circles rather than by strangers on the Internet, it is apparent that sexual predators do exist online and both sources of risk must be seriously and comprehensively addressed.⁴³

Impact

- 4.42 The Office of the Victorian Child Safety Commissioner commented that the effects of sexual grooming include:

cognitive disorders, emotional pain, avoidance behaviours, low self-esteem, guilt, self-blame, self-harming behaviours, delinquency, substance abuse, vulnerability to repeated victimisation, interpersonal difficulties, dissociation and disbelief about the abuse, functional amnesia and effects on relationships with others (Calmer Classrooms, 2007). These can affect a young person’s ability to experience success at school, either by the effects the abuse has had on the cognitive capacity of the child, or, exclusion from school due to extremely challenging behaviours. As can be seen the effects are long lasting and for many, the damage is permanent.⁴⁴

- 4.43 Parents Victoria provided the following example:
-

42 Youth Affairs Council of South Australia, *Supplementary Submission 25.1*, p. 11, citing Ybarra M, Espelage D and Mitchell K, 2007, ‘The occurrence of internet harassment and unwanted sexual solicitation victimisation and perpetration: association with psychosocial indicators’, *Journal of Adolescent Health* 41: 31-41.

43 National Children’s and Youth Law Centre, *Submission 138*, p. 7, citing Lamont A, 2011, ‘Who Abuses Children’, Resource Sheet, Australian Institute of Family Studies, p. 3.

44 Alannah and Madeline Foundation, *Submission 22*, p. 21.

I never imagined my child (14) would have been preyed upon. I considered our family to be really diligent with internet use but now I feel we did drop our guard. People would say we were lucky as our school were very communicative and supportive. We have worked closely with them and Victoria Police not just for our child but for any other students at risk. There were signs, we discussed and dismissed these behaviours as typical adolescent changes but unbeknown to us it was far more intrusive and sinister. Now the person has come to the attention of the authorities and it was confirmed our child was being groomed. I advise to all families that where there is information or opportunities on offer to learn prevention or strategies to remain cybersafe please pay attention and attend, you could save a family member from being another statistic.⁴⁵

Sanctions against sexual grooming

4.44 The sanctions against sexual grooming will be consider in detail in Chapter 11 which considers legislative options.

Research

4.45 It is difficult to determine the extent of online grooming in Australia. ninemsn supported the call for additional research:

we do not have any data regarding the level of cyber-grooming in Australia. ninemsn believes more Australian-based research into cyber safety risks is needed so that we are better informed about the prevalence of particular risks and the specific contexts in which they arise.⁴⁶

4.46 Yahoo!7 commented that:

There is a distinct lack of research and evidence into how Australian children are engaging with the Internet and how they, and their parents / carers perceive the safety risks associated with their children's use of the Internet. It would be extremely valuable for government and industry to gain a better understanding of the level of awareness amongst parents and carers of the range of

45 Parents Victoria, *Submission 143*, p. 2.

46 ninemsn, *Submission 91*, pp. 5-6.

existing safety tools available to assist in keeping their children safe online by way of example.⁴⁷

Sexting

4.47 Although sexting is seen as a 'new' technological trend, it was first reported in media in the United Kingdom in 2005. It is described as the practice among some young women and men of creating, sharing, sending or posting sexually suggestive or explicit messages or images via the Internet or mobile phones. This material often portrays the individual sending the message.⁴⁸

A recent survey in the UK in 2009 by the South West Grid for Learning revealed that around 40% of teens questioned said that they knew friends who had been involved in sexting. Over a quarter, 27%, of respondents said that sexting happened regularly or 'all of the time'. Additionally, 56% of respondents were aware of instances where images and videos were distributed further than the intended recipient, indicating that the majority of respondents knew that these images and videos were sent on beyond the people for whom they were intended, highlighting where sexting and cyberbullying can converge.⁴⁹

4.48 Once a message or image is sent, it is usually stored on the mobile phone, email inbox or on the social networking site of the individual or the group to whom it was sent. If a relationship deteriorates, the image may be posted online, used to cyber-bully, or go into collections of such material held by the offender(s).⁵⁰

4.49 The Australian University Cyberbullying Research Alliance commented that sexting raises moral, ethical, legal and parenting concerns at a significant time in young people's lives, as they are developing their sexual identities and engaging in early romantic relationships.⁵¹ However, Professor Karen Vered commented that:

47 Yahoo!7, *Submission 2*, p. 2.

48 BoysTown, *Submission 29*, p. 12; Alannah and Madeline Foundation, *Submission 22*, p. 22. See also Device Connections, *Submission 51*, p. 3, for another definition.

49 Childnet International, *Submission 18*, pp. 2-3 citing www.swgfl.org.uk/Staying-Safe/Sexting-Survey.

50 Alannah and Madeline Foundation, *Submission 22*, p. 22.

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

I increasingly find it very interesting that we continue as a society to deny young people's interest in sexual experience, for instance. We simply do not want to accept the fact that teenagers are sexually active, and by ignoring that and by pretending it is not so we make a lot of mistakes, and some of them have consequences for young people's health that they wear for the rest of their lives. It is that kind of thing. We really need to be realistic about what young people are doing with their time, whether we approve of it or not. You might not like it, but the fact is that if young people are engaged in certain behaviours and if we still feel responsible for them then we need to provide them with the tools, the means and the guidance to make those activities safe for them.⁵²

- 4.50 Sexting reflects the increasing sexualisation of the way young people present themselves. Dr Judith Slocombe from the Alannah and Madeline Foundation commented that young people have picked up 'adult values' in our society: bullying, violence and sexualised images.⁵³ This raises the issue of whether it is an error to approach cyber-safety in isolation without considering a wider spectrum of behavioural issues.

Prevalence

- 4.51 It is not clear how common sexting is in Australia. Kids Helpline has found that while sexting is a topic of interest among young people that 'due to its rising social stigmatisation, young people may not willingly admit that they engage in this behaviour'.⁵⁴
- 4.52 American research has indicated that about 4 percent of young people have sent nude or near-nude images to other people, and about 15 percent have received them. This suggests that such images had been passed to a wider group by the recipients.⁵⁵ Another American study revealed that 20 percent of young people 13 to 19 years have electronically sent or posted online nude or semi-nude pictures or videos of themselves: 22 percent girls, 18 percent boys.⁵⁶
- 4.53 Recent Australian research showed that, of 5,000 female and male students surveyed, about 10 percent had sent nude photos of themselves by mobile

52 Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, p. CS42.

53 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. CS46.

54 BoysTown, *Submission 29*, p.13.

55 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS45.

56 iKeepSafe, *Submission 101*, p. 6.

phone. However, numbers rose from year 9 so that, by Year 11, about 17 percent had sent such photos.⁵⁷

Generation Next (Public Seminar Group on Children & Teenagers) reported 69% of teenagers have engaged in 'sexting' their girlfriends or boyfriends.⁵⁸

4.54 Sexting has become 'normalised behaviour' in adolescent culture. The American research referred to above showed that 17 percent of teenagers who send these images to people they know and trust manage their own mobile phone accounts, usually pre-paid. Of those whose parents manage the accounts, only 3 percent have sent such images which are then spread rapidly.⁵⁹

4.55 Dr Barbara Spears commented that,

Regarding sexting, we certainly had evidence in the insights project where counsellors were reporting the sexting going on but one of the issues was not that it was being sent from peer-to-peer initially but that a sibling within the family, as a payback, would take the mobile phone and send something on.⁶⁰

4.56 Participants in the Committee's *Are you safe?* survey were asked if they have sent nude or semi-nude photos to others via email, text or other communication methods. Overall, 91.2 percent of participants would not or have not sent nude or semi-nude pictures via new technologies.

4.57 There was a peak of this activity at the both ends of the age sample in that survey. Notably, 22.8 percent of female respondents aged 18 years answered that they would send nude or semi-nude photos. There was also a peak in 18 year old males: 17.3 percent identifying that they send nude or semi-nude photos to others. Such actions may expose these young adults to significant risk, and can have huge implications later in life.

57 Dr Paul Weldon, Research Fellow, Australian Council for Educational Research *Transcript of Evidence*, 9 December 2010, p. CS46.

58 Device Connections Pty Ltd, *Submission 51*, p. 12.

59 Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS39.

60 Dr Barbara Spears, Senior Lecturer, School of Education, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS46.

Figure 4.3 Do you send nude or semi-nude photos? (Age)

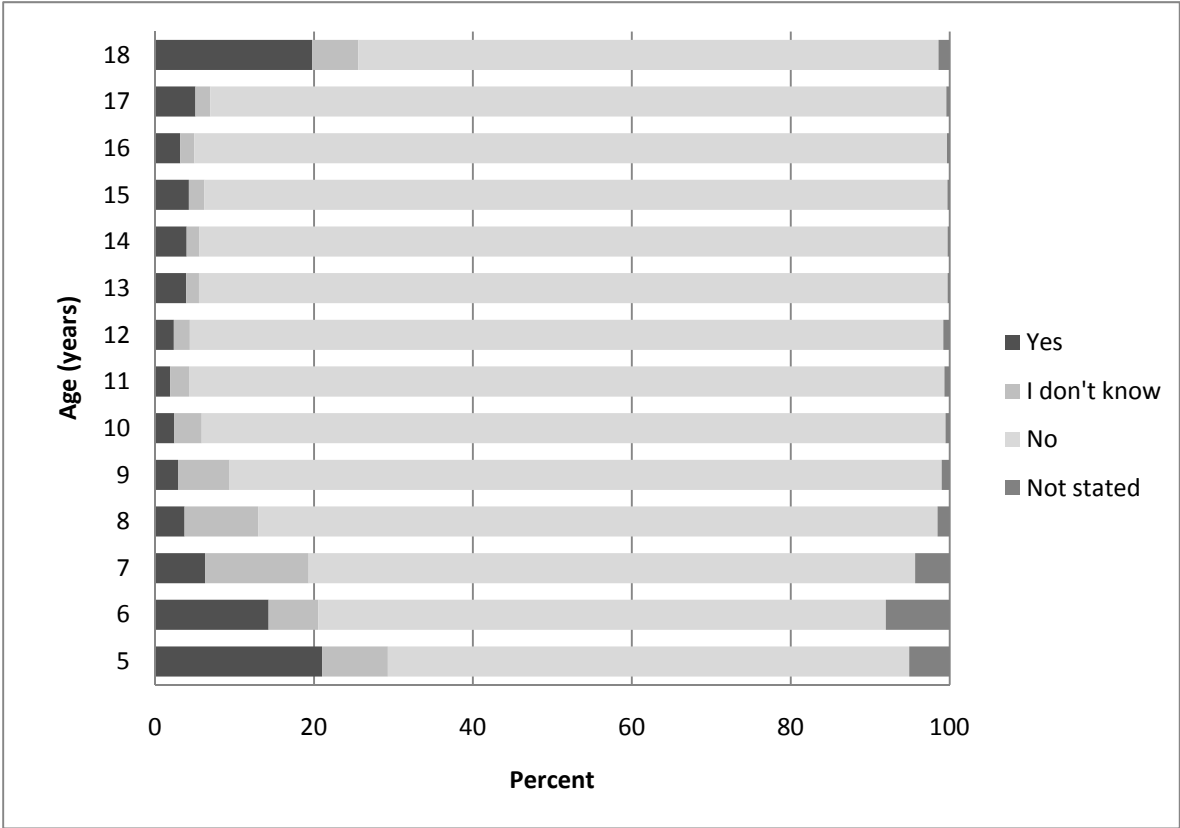


Table 4.3 Do you send nude or semi-nude pictures?

		Yes		No		I don't know		Not stated		Total
Sex		%	#	%	#	%	#	%	#	#
5 Years	M	18.7	14	70.7	53	6.7	5	4.0	3	75
	F	23.2	19	61.0	50	9.8	8	6.1	5	82
6 Years	M	16.7	8	64.6	31	8.3	4	10.4	5	48
	F	12.5	8	76.6	49	4.7	3	6.3	4	64
7 Years	M	6.4	7	76.4	84	11.8	13	5.5	6	110
	F	6.2	6	76.3	74	14.4	14	3.1	3	97
8 Years	M	5.0	21	84.2	357	8.7	37	2.1	9	424
	F	2.6	13	86.6	427	9.7	48	1.0	5	493
9 Years	M	3.9	39	87.8	882	7.3	73	1.0	10	1004
	F	1.9	21	91.3	984	5.8	62	1.0	11	1078
10 Years	M	3.4	58	92.2	1568	3.8	65	0.6	10	1701
	F	1.5	27	95.0	1708	3.1	55	0.4	8	1798
11 Years	M	2.3	53	94.2	2171	2.8	64	0.7	17	2305
	F	1.5	38	95.9	2399	2.0	50	0.6	15	2502
12 Years	M	2.9	65	93.5	2093	2.7	60	0.9	21	2239
	F	1.8	41	96.2	2176	1.4	31	0.7	15	2263
13 Years	M	5.0	95	92.3	1745	2.4	45	0.3	5	1890
	F	3.1	75	95.7	2350	1.0	25	0.2	6	2456
14 Years	M	5.9	95	91.6	1476	2.2	35	0.4	6	1612
	F	2.4	48	96.3	1908	1.2	23	0.2	3	1982
15 Years	M	6.7	80	90.0	1072	3.2	38	0.1	1	1191
	F	2.1	29	96.6	1327	0.9	12	0.4	6	1374
16 Years	M	4.8	39	92.7	748	2.4	19	0.1	1	807
	F	1.8	18	96.4	962	1.3	13	0.5	5	998
17 Years	M	9.4	37	87.3	345	2.5	10	0.8	3	395
	F	2.1	12	96.3	547	1.4	8	0.2	1	568
18 Years	M	17.3	54	76.3	238	5.1	16	1.3	4	312
	F	22.8	59	69.1	179	6.6	17	1.5	4	259

- 4.58 Analysing its own research, Berry Street commented that for vulnerable young people:

Between 7 and 15% of respondents indicated they had either sent, requested or received naked or semi-naked photographs of themselves or others online or via mobile phone. In consultations staff, carers and educators told us that they were concerned about the growing trend in 'sexting' among their clients. More concerning were the stories about teenage girls using photographs of themselves in suggestive poses and varying states of undress to barter with strangers as well as their peers for drugs, phone credit and cigarettes.⁶¹

- 4.59 Concerns were also expressed by parents and communities who have noted an increased prevalence of sexting via mobile phones, and the impact it is having on Indigenous young people.⁶²

Impact

- 4.60 While most originators seem to send these messages voluntarily, the consequences of sexting are clear, including invasion of privacy via subsequent distribution, the impact on the individual's reputation, and shame. BoysTown commented:

Consequences include poor self-esteem and self-image, isolating behaviours, school avoidance, eating disorders, self-harm and suicidal ideation and behaviours.⁶³

- 4.61 Civil Liberties Australia added that other possible consequences include:

While it may make parents unhappy, young people are going to be in relationships, and some of these may involve sex. As such, and given that young people are now in possession of camera-equipped mobile phones, it is inevitable that some will choose to send sexual pictures to each other. Whilst the sexual education above should discourage this behaviour, no minor involved in a healthy relationship should ever be considered a "child pornographer" nor in possession of "child pornography" for such behaviour. About the worst thing we can do to our young people is brand them as sex offenders: the current laws turn experimenters into criminals. The real issue is when and how the

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

62 NT Government, *Submission 84*, p. 7.

63 BoysTown, *Submission 29*, p.14.

images are made publicly available. The person(s) who makes the images publicly available should be made responsible for that act.⁶⁴

4.62 Distribution of such images also invites possible long term effects on the sender's 'digital reputation', potentially causing problems with possible employers in the future.⁶⁵ Material can be traced; what is posted on line may come back and remain online forever because the digital footprint of Internet access is indelible. Some private investigation firms now have the capacity to search for a variety of personal information.⁶⁶

4.63 The Alannah and Madeline Foundation highlighted a significant concern:

A number of companies now routinely review a potential employee's online history, particularly on facebook and other social networking sites, and use this information as part of their decision making in the recruitment process. Because of permanent records or the 'digital footprint' that young people leave on the internet, naïve and inappropriate postings may have a long term and detrimental effect on a young person's life.⁶⁷

4.64 The NSW Secondary Principals Council commented on the permanence of postings:

One of the greatest risks to young people is the permanence of the postings made on the internet. This concept is not fully understood by Gen Y and Gen Z. Government needs to consider protections to reduce the permanence of postings for under 18s.⁶⁸

4.65 BoysTown added that:

Like cyberbullying, the impacts of 'sexting' can also be permanent as it is almost impossible to withdraw inappropriate images or messages created and shared through mobile and internet technologies once they are sent and/or posted. This means that these images and messages could be circulating as young people

64 Civil Liberties Australia, *Submission 23*, p. 4.

65 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS13.

66 Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, pp. CS6-7, 9; Dr Gerald White, Principal Research Fellow, Australian Council for Educational Research, *Transcript of Evidence*, 9 December 2010, p. CS49; Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS65.

67 Alannah and Madeline Foundation, *Submission 22*, p. 24.

68 NSW Secondary Principals Council, *Submission 32*, p. 2.

start applying for universities or jobs which may impact on the individual's reputation and life opportunities.⁶⁹

4.66 An American study showed that 70 percent of recruiters and human resource professionals said that they had rejected candidates for jobs based on information found online. While only 7 percent of consumers thought that their online information affected their searches for jobs, 75 percent of American companies required their hiring personnel to do online searches about candidates. Among recruiters and human resource professionals, 85 percent said that 'positive' online reputations influenced hiring decisions, 'at least to some extent'.⁷⁰ While it is possibly illegal to do so, potential employers can, and some do, 'automatically' check on Internet search engines, and in other ways, on potential employees, whether for part-time staff aged 15 or graduates.⁷¹

4.67 'Data mining' is now one of the fastest growing industries in Australia, whereby information can be collected on many aspects of an individual's life and behaviour. Civil Liberties Australia commented:

people simply do not realise that the Internet never forgets, and information posted online in the heat of the moment may come back to haunt him/her at a later date.⁷²

4.68 However, Dr Helen McGrath emphasised that:

if we get out a message that says, 'It is the end of the world if something you foolishly put up about yourself when you 13, particularly a semi-nude picture, will be up there forever and it will come back to bite you,' then we are going to get lots of kids who become deeply depressed and self-harm as a result of that. I am very concerned about that, if they have done it and they find out afterwards that it really was dumb. It is a silly thing to do, in the same way that you should never have a webcam in your bedroom – and it is amazing how many parents do not understand how a boyfriend at one end and a girlfriend at the other end, both with webcams, can have interesting times with the door shut. But if they think it is going to destroy their lives it can

69 BoysTown, *Submission 29*, p.14.

70 iKeepSafe, *Submission 101*, p. 6. For a different figure of use of social networking sites by potential employers in the US, see also Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, pp. CS13, 45.

71 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, pp. CS45-46; Dr Gerald White, Principal Research Fellow, Australian Council for Educational Research, *Transcript of Evidence*, 9 December 2010, p. CS49.

72 Civil Liberties Australia, *Submission 23*, p. 5.

lead to incredible depression and occasionally self-harm. That is why I think going down the path of wise education, with warnings but not necessarily terrifying sensationalism, is the way to go.⁷³

4.69 The Alannah and Madeline Foundation commented that,

the use child abuse legislation to prosecute regardless of age, on the grounds of production and distribution of images ...can mean young people may have a criminal record and in a worst-case scenario, although unlikely, find themselves on the sex offenders register.⁷⁴

4.70 In Australia, 32 Victorian teenagers were charged with child pornography offences resulting from 'sexting'.⁷⁵ Many young people are unaware that 'sexting' may be considered a criminal offence.⁷⁶

4.71 Furthermore, not all young people view 'sexting' as unsafe:

58 percent of the respondents in the Cox Communications (2007) study did not think that posting personal information and photos on public networking sites was an unsafe practice, 47 percent were not worried about other people using their personal online information in ways they did not want them to, and 49 percent were unconcerned that the posting of personal information online might negatively affect their future.⁷⁷

4.72 The Australian Council for Computers in Education commented that:

The reported prevalence of posting of photographs of students to SNS, suggests that the legal and ethical issues involved with the posting of photographs - which include privacy, confidentiality, defamation and copyright - merit specific attention in any cybersafety curriculum. The significance of understanding these issues is emphasised by the incidents involving a Melbourne

73 Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS66.

74 Alannah and Madeline Foundation, *Submission 22*, p. 22.

75 BoysTown, *Submission 29*, p.15, citing Battersby, Lucy: 'Sexting: fears as teens charged'. July 10, 2008 <http://www.smh.com.au/articles/2008/07/10/1215282979671.html>.

76 BoysTown, *Submission 29*, p.14, citing Lenhart A (2009) *Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging*. Pew Internet and American Life Project.

77 Australian Institute of Criminology, *Submission 56*, p. 9.

teenager posting naked photos of AFL footballers to her Facebook site.⁷⁸

- 4.73 The NSW Government is conducting a campaign entitled *SAFE SEXTING: No Such Thing*:

This work is designed to warn young people of the negative consequences of sexting; the campaign produced a fact sheet available to schools, parents and teenagers on the topic. This is a good example of positive government efforts to educate, inform and help reduce negative online behaviour.⁷⁹

- 4.74 The National Children's and Youth Law Centre Lawmails contained questions about nudity or pornography, demonstrating a concern about criminal sanctions and a desire to comply with legislation. In relation to naïve young people transmitting sexually suggestive photos, if child pornography laws are rigidly applied, 'these children will not only suffer personal consequences but also potentially very serious criminal consequences'.⁸⁰

Sanctions against sexting

- 4.75 The sanctions are dealt with in more detail in Chapter 11.

Research

- 4.76 Sexting is an area where further research is needed to understand the motives behind this behaviour and to develop effective intervention strategies.⁸¹
- 4.77 BoysTown suggested that the Australian Government fund a nationally-representative study on sexting in relation to Australian children and young people with the purpose of identifying effective prevention strategies.⁸²

78 Australian Council for Computers in Education, *Submission 128*, p. 3.

79 Family Online Safety Institute, *Submission 38*, p. 9.

80 National Children's and Youth Law Centre, *Submission 138*, p. 7.

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

82 BoysTown, *Submission 29*, p.15.

Illegal and inappropriate content

4.78 There are no restrictions on access to the online environment because of the age of users, or potential users. Young people may therefore be exposed to content that is inappropriate, regardless of their age. This could include illegal and inappropriate sexual, violent, racist or hate material, promotion of consumption, perpetuation of negative stereotypes, as well as misinformation and other problematic content.⁸³

4.79 Sexual content may include legal adult pornography, illegal child abuse or self-produced sexting images or other inappropriate images, video or audio files. The Alannah and Madeline Foundation submitted that:

While the likelihood of stumbling across child abuse images is relatively low, these images are deliberately sent as part of the 'grooming processes' to normalise sexual behaviour. On the other hand, very graphic adult pornography is easily accessed and often free. While young adults have viewed pornography in 'magazine format' for decades, at no other time have we experienced such heightened access to pornographic material.⁸⁴

4.80 Illegal material may be accessed accidentally when music or videos are being downloaded. While the great majority of young people will never encounter, or use, any of the sites offering illegal material, its presence in the online environment is a sufficient threat to need attention.⁸⁵

My daughter was seven when she first encountered pornography online. Her school (she was in Year 2) participated in the online maths practice program Mathletics. One day when she clicked on the link to Mathletics, it took her to a pornography website and she called me saying 'Mummy the computer has done something funny and there are strange people on the Mathletics site. Some hacker or virus had attached itself to the Mathletics address and was taking children to a porn site. Fortunately, it was one that needed you to accept that it was an adult site and you had to click a link to access the more graphic content The images would have been classified as images of full frontal male and female nudity in sexualised depictions and have been at least in the MA15+ classification range.'⁸⁶

83 Alannah and Madeline Foundation, *Submission 22*, p. 21.

84 Alannah and Madeline Foundation, *Submission 22*, p. 21.

85 Alannah and Madeline Foundation, *Submission 22*, p. 22.

86 Name withheld, *Submission 140*, p. 1.

4.81 Industry also has a role to play. For example, Facebook does not allow materials such as nudity, hateful speech, abusive behaviour or threat to life or safety:

It is important to understand just as a matter of how Facebook operates and what its terms of service are – how it is laid out, what is allowed and what is not allowed – that it is much more restrictive than almost any legislation I have ever seen in any place in terms of what is allowed on the site, what is not allowed on the site and what we police for.⁸⁷

4.82 The National Children’s and Youth Law Centre expressed concern about the lack of community legal education which would enable people to make wise decisions and given the serious nature of the potential consequences, young people must have this information to make informed and reasoned decisions.⁸⁸

4.83 Sanctions in relation to illegal content are dealt with in Chapter 11.

87 Hon Mozelle Thompson, Chief Privacy Advisor, Facebook, *Transcript of Evidence*, 11 June 2010, p. 26.

88 National Children’s and Youth Law Centre, *Submission 138*, p. 7.

Breaches of privacy and identity theft

Introduction

- 5.1 This chapter explores the links between identity theft and breaches of privacy, and also addresses the complexities of third parties collecting personal information.

Privacy Act 1988 (Cth)

- 5.2 The *Privacy Act 1988 (Cth)* does not make special reference to young people, on the basis that they have the same rights to privacy as adults. In practice, primary care-givers are usually responsible for exercising their rights under that Act until individuals reach levels of maturity and understanding to make independent decisions.¹

- 5.3 The Office of the Privacy Commissioner commented that:

this approach to the privacy of young people is appropriate, as it accommodates different rates of development. Mature young people are entitled wherever possible, to make decisions about their personal information as soon as they are able, rather than on reaching a prescribed age. It is the Office's view that this level of autonomy should be maintained in respect of young people's privacy.²

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

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

5.4 However, the NSW Government expressed concern that:

children's privacy is subject to some specific risks. Children and young people are more vulnerable in the sense that they are less likely to have the nous or capacity to be alerted to potential privacy breaches, to read and understand the fine print of contracts with internet service providers and web page administrators, or to know what action may be available to them if their privacy is breached.³

5.5 Australian privacy legislation does not impose any obligations on individuals acting in a private capacity, but instead relates to how organisations deal with the personal information of others. As there are also exemptions for small businesses with annual turnovers of \$3 million or less, a large proportion of the Australian private sector is not subject to any privacy laws.

5.6 Such legislation may be insufficient to protect young people from cyber-safety risks occurring as a result of individuals acting in private capacities.⁴ The Victorian Privacy Commissioner stated that:

I have identified in the submission the gaps in privacy laws, with one of the greatest being small business exemption and also the fact that privacy laws do not apply to individuals acting in a private capacity. That gap was identified by the Australian Law Reform Commission, which recommended that it be filled by a statutory tort of privacy.⁵

5.7 The Committee supports Recommendation 3 in the Senate Environment and Communications References Committee's recent Report.⁶ It therefore recommends:

3 NSW Government, *Submission 94*, p. 14.

4 Victorian Privacy Commissioner: *Submission 59*, p. 3; Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, pp. CS68, 79.

5 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS68.

6 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

Recommendation 4

That the Australian Government consider amending small business exemptions of the *Privacy Act 1988* (Cth) to ensure that small businesses which hold substantial quantities of personal information, or which transfer personal information offshore, are subject to the requirements of that Act.

- 5.8 The Committee supports Recommendation 3 in the Senate Environment and Communications References Committee's recent Report.⁷ It therefore recommends:

Recommendation 5

That the Australian Privacy Commissioner undertake a review of those categories of small business with significant personal data holdings, and make recommendations to Government about expanding the categories of small business operators prescribed in regulations as subject to the *Privacy Act 1988* (Cth).

Privacy and young people

- 5.9 Young people desire to maintain a degree of privacy but are less cognisant than adults about what privacy actually entails. For example, young people most often discuss privacy in the context of independence from their parents or teachers, and not in the adult or legalistic way of appropriately securing private personal information.⁸
- 5.10 The Mental Health Council of Australia identified privacy as one of five major risks for young people, with potential impacts on their health and well-being.⁹ The Consultative Working Group on Cybersafety believed that inappropriate handling of private information was likely to be

7 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix. Tabled on 7 April 2011.

8 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 5; Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS71.

9 Mental Health Council of Australia, *Submission 52*, p. 4.

significant and have long-term implications for Australians into the future.¹⁰

- 5.11 The Office of the Privacy Commissioner stated that little Australian research has been done about the awareness or attitudes of young people to privacy issues.¹¹ The Association of Independent Schools of SA submitted:

It is apparent that many students are not fully cognisant about the permanent nature of postings on the Internet. It appears they lack the foresight to realise that once a photo, phone number or rumour is posted onto the Internet, it is out of their control. An example used in schools to teach children about this is asking them if they would like that photo enlarged and shown at school assembly.¹²

- 5.12 However, the Victorian Privacy Commissioner commented that:

It is certainly the case in my view that young people do value their privacy and are open to understanding and educating themselves about how they can make themselves safer online.¹³

- 5.13 The 2010 Social Networking Education and Awareness Campaign run by the South Australian Government recorded 'a large number' of concerns about the level of access others can have to an individual's information. These concerns included:

- Over-sharing of personal information;
- Third party access to information;
- Apathy about privacy settings;
- Lack of information on how information can be used for identity theft;
- Being too trusting and accepting anyone as a 'friend';
- Pressure to collect 'friends'; and
- If an individual has many 'friends', many other people can have access to her/his information.¹⁴

10 Consultative Working Group on Cybersafety, *Submission 113*, p. 9.

11 Office of the Privacy Commissioner, *Submission 92*, p. 5.

12 Association of Independent Schools of SA, *Submission 19*, p. 11.

13 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS69.

14 South Australian Office for Youth, *Submission 98*, p. 3.

- 5.14 The Office of the Privacy Commissioner expressed concern that:
- The available evidence suggests that more effort needs to be directed to ensuring young people gain the skills needed to make sensible decisions around privacy and to understand their rights and obligations under the Privacy Act.¹⁵
- 5.15 The many ways of interacting on the online environment exposes people to a wider public than is possible offline. Young people are particularly at risk, as they frequently post personal and identifying material without being fully informed of the consequences and risks.¹⁶ Chapter 4 noted in the discussion of cyber-stalking, potential offenders often do not have to look long for targets because personal information about other people is so easily found online.¹⁷ Chapter 7 provides the results of the Committee's consultations with young people about their perceptions of what it is appropriate to post online.
- 5.16 When people go online, a 'disinhibition effect' occurs: there are no consequences when they put things on the screen. The online environment speeds up the disclosure process, so that what would normally take a long time to disclose face-to-face happens quickly and without incurring an immediate, visible consequence. Young people are therefore more likely to post material online without considering possible consequences.¹⁸
- 5.17 Young people can also be victims of their peers, as online identities can be assumed and used as part of abuses such as cyber-bullying. Email accounts can be opened in other names to send malicious emails. Embarrassing or hurtful material can be sent after social networking accounts have been hacked into, or passwords shared and then re-used maliciously.¹⁹
- 5.18 Armorlog International noted that many networks do not prevent users using easily guessed passwords, and allow user names and passwords to be stored in Internet browsers:
- Some networks have unfortunately incorporated procedures in the management of their systems, sometimes in order to try and control fraud, that inadvertently actually result in greater amounts

15 Office of the Privacy Commissioner, *Submission 92*, p. 5

16 Australian Psychological Society, *Submission 90*, p. 11.

17 Alannah and Madeline Foundation, *Submission 22*, p. 19.

18 Dr Barbara Spears, Senior Lecturer, School of Education, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS25.

19 Attorney-General's Department, *Submission 58*, p. 7; Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS18.

of private information being revealed about users that actually facilitates identity crime as it provides opportunities for fraudsters to accumulate further knowledge about a target that assist in change user details to take over their accounts & thus identity.²⁰

Most networks facilitate users duplicating passwords used elsewhere. When this occurs users are at greater risk in regard to identity theft.²¹

- 5.19 Similarly, the Committee's *Are you safe?* survey asked if respondents had felt unsafe online. Many respondents chose to comment in free text spaces to explain their answer. The following comment was submitted in response to that question:

i was chatting to a friend of mine, but slowly realised that it didn't seem like her. i asked and they replied that they were her cousin. without writing anything else i signed of and deleted that account (Female aged 16).²²

- 5.20 The Murdoch Children's Research Institute referred to anecdotal evidence linking cyber-bullying to breaches of privacy. People often use the same password for many accounts and, if this can be guessed by a friend, it can be used to post bullying material about others, posting embarrassing stories or photos.²³

Privacy settings

- 5.21 The South Australian Office of Youth have found that a large proportion of people do not engage their privacy settings.²⁴ While notices and settings exist on the majority of sites, including social networking sites, ways of protecting privacy are often so complex and difficult that people frequently do not examine, understand or even set them.

20 Armorlog International, *Submission 4*, p. 3.

21 Armorlog International, *Submission 4*, p. 2.

22 For authenticity, throughout the Report, emails from young people have been incorporated in the form received.

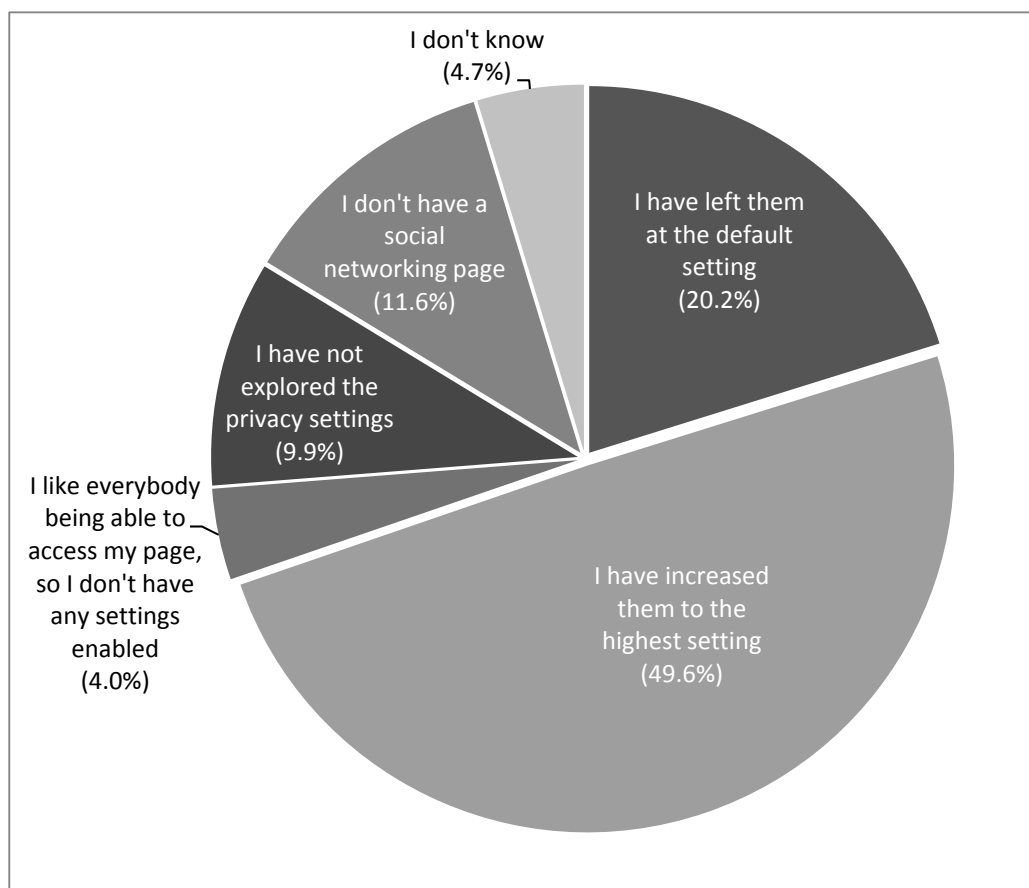
23 Murdoch Children's Research Institute, *Submission 111*, p. 4.

24 Mrs Tiffany Downing, Director, South Australian Office of Youth, *Transcript of Evidence*, 3 February 2011, p. CS25.

5.22 The *Are you safe?* survey asked participants aged 13 years and over about their use of privacy settings on their social networking and gaming sites. The survey found:

- 49.6 percent identified they had increased them to the highest setting;
- 20.2 percent identified they had left the settings at the default level;
- 9.9 percent identified they had not explored the privacy settings at all; and
- 4.0 percent identified that they have disabled all privacy settings to allow everybody access.

Figure 5.1 Have you explored the privacy settings of your social networking pages?



5.23 Figures 5.2a and 5.2b show the differences in between male and female respondents.

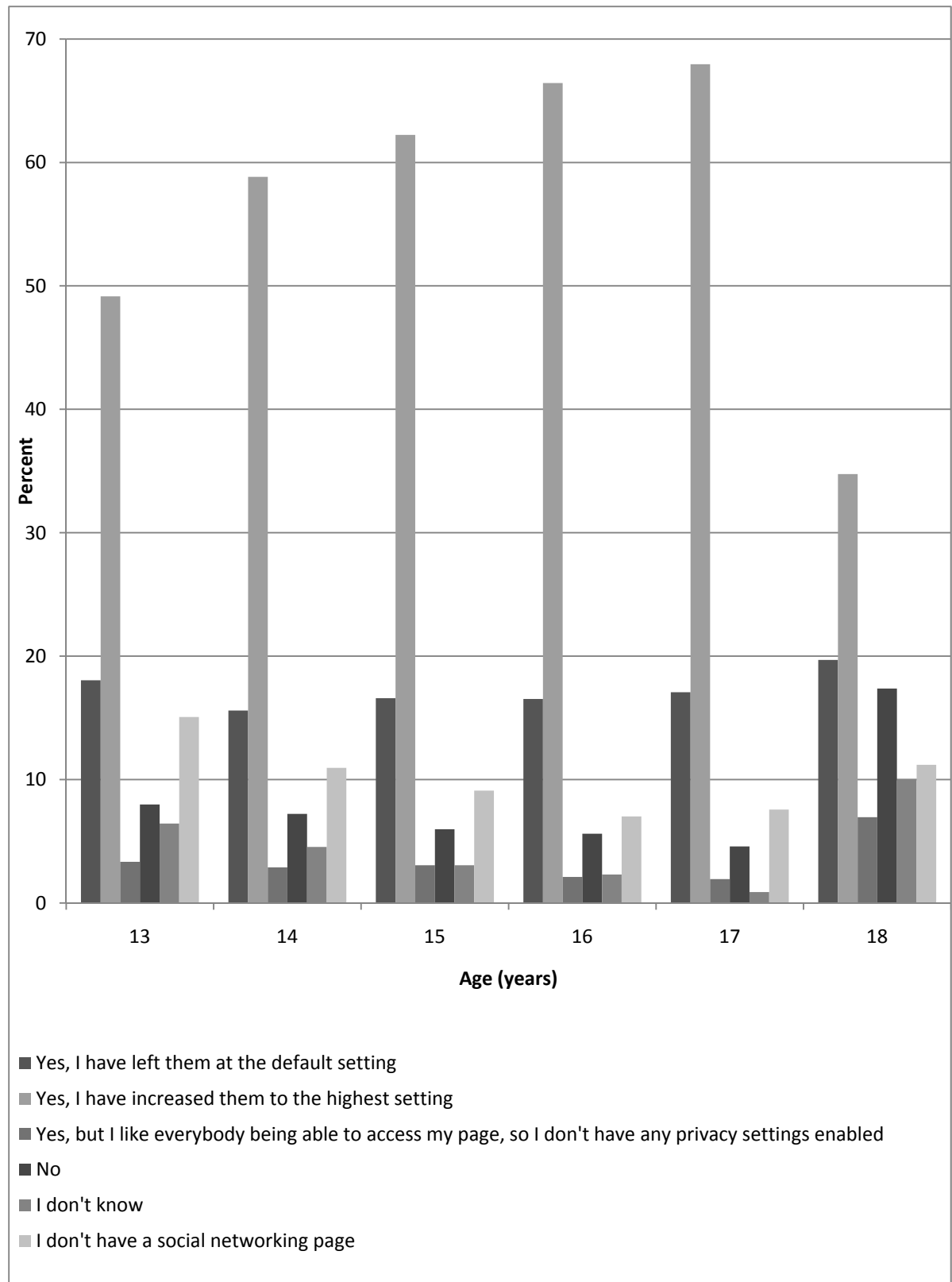
Figure 5.2a Have you explored the privacy settings on your social networking pages? (*Female*)

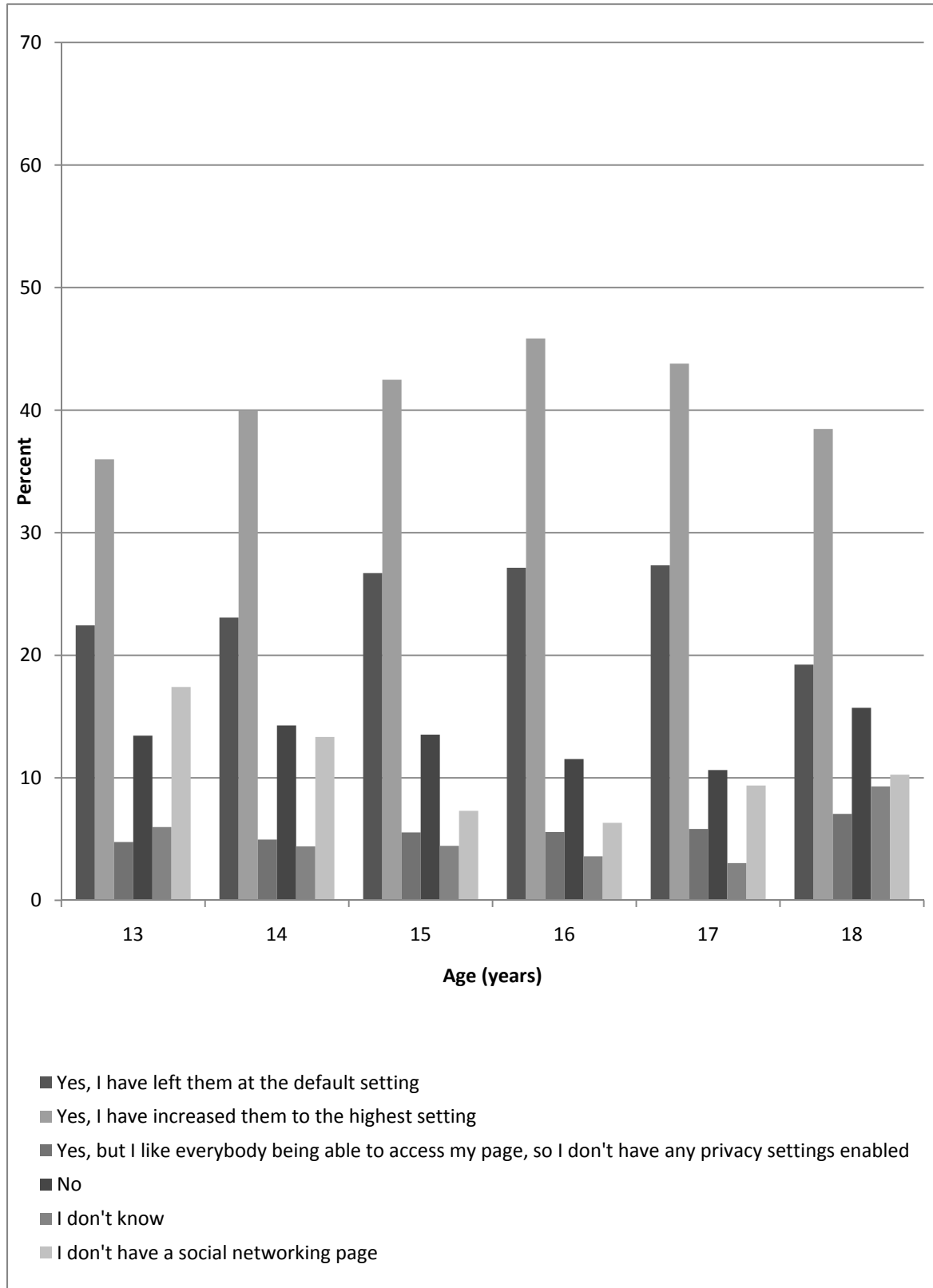
Figure 5.2b Have you explored the privacy settings on your social networking pages? (*Male*)

Table 5.1 Have you explored the privacy settings on your social networking pages?

	Sex	Yes, I have increased them to the highest setting		Yes, I have left them at the default setting		Yes, but I like everybody being able to access my page, so I don't have any enabled		I don't have a social networking page		I don't know		No	
		%	#	%	#	%	#	%	#	%	#	%	#
13 Years	M	36.0	680	22.4	424	4.8	90	17.4	329	6.0	113	13.4	254
	F	49.1	1207	18.0	443	3.3	82	15.1	370	6.4	158	8.0	196
14 Years	M	40.0	644	23.1	372	5.0	80	13.3	215	4.4	71	14.3	230
	F	58.8	1166	15.6	309	2.9	57	10.9	217	4.5	90	7.2	143
15 Years	M	42.5	506	26.7	318	5.5	66	7.3	87	4.5	53	13.5	161
	F	62.2	855	16.6	228	3.1	42	9.1	125	3.1	42	6.0	82
16 Years	M	45.8	370	27.1	219	5.6	45	6.3	51	3.6	29	11.5	93
	F	66.4	663	16.5	165	2.1	21	7.0	70	2.3	23	5.6	56
17 Years	M	43.8	173	27.3	108	5.8	23	9.4	37	3.0	12	10.6	42
	F	68.0	386	17.1	97	1.9	11	7.6	43	0.9	5	4.6	26
18 Years	M	38.5	120	19.2	60	7.1	22	10.3	32	9.3	29	15.7	49
	F	34.8	90	19.7	51	6.9	18	11.2	29	10.0	26	17.4	45

5.24 Figures 5.3a and 5.3b show the levels of concern about cyber-safety of those that have left their privacy settings at the default level. Similarly, Figure 5.4 shows that the majority of those respondents who have left their privacy settings on default, have not felt unsafe online.

Figure 5.3a Of those with privacy settings left at default, are they worried about their safety online?
(Female)

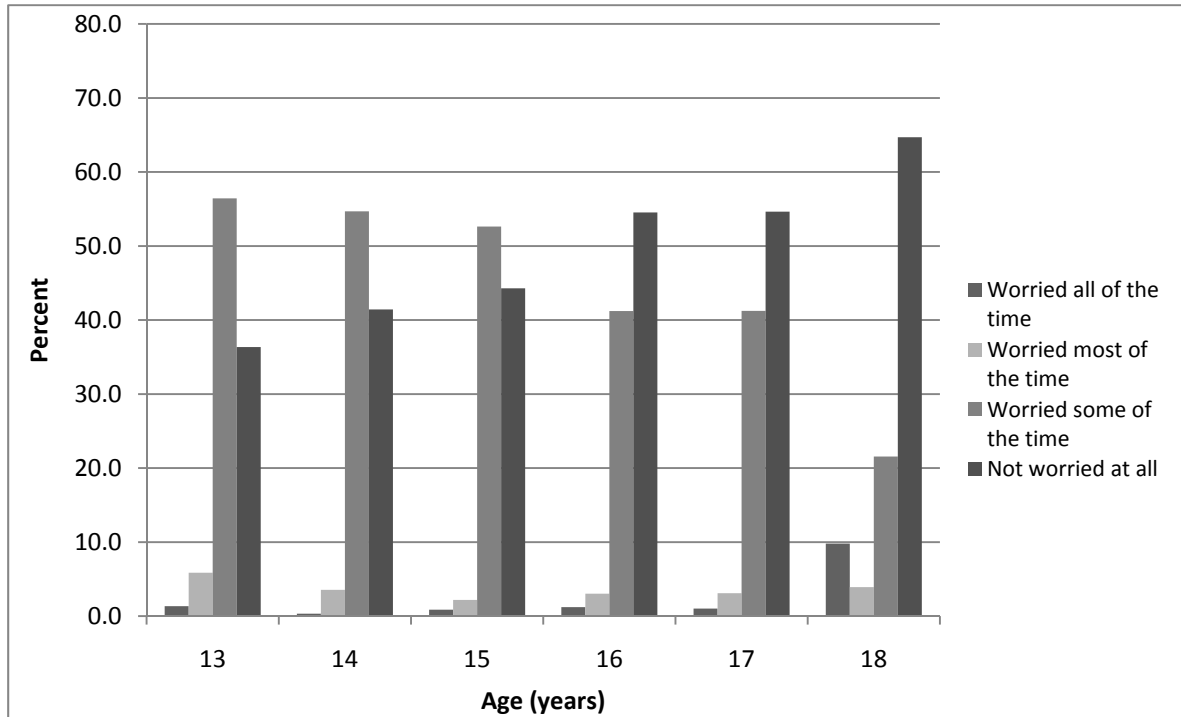


Figure 5.3b Of those with privacy settings left at default, are they worried about their safety online?
(Male)

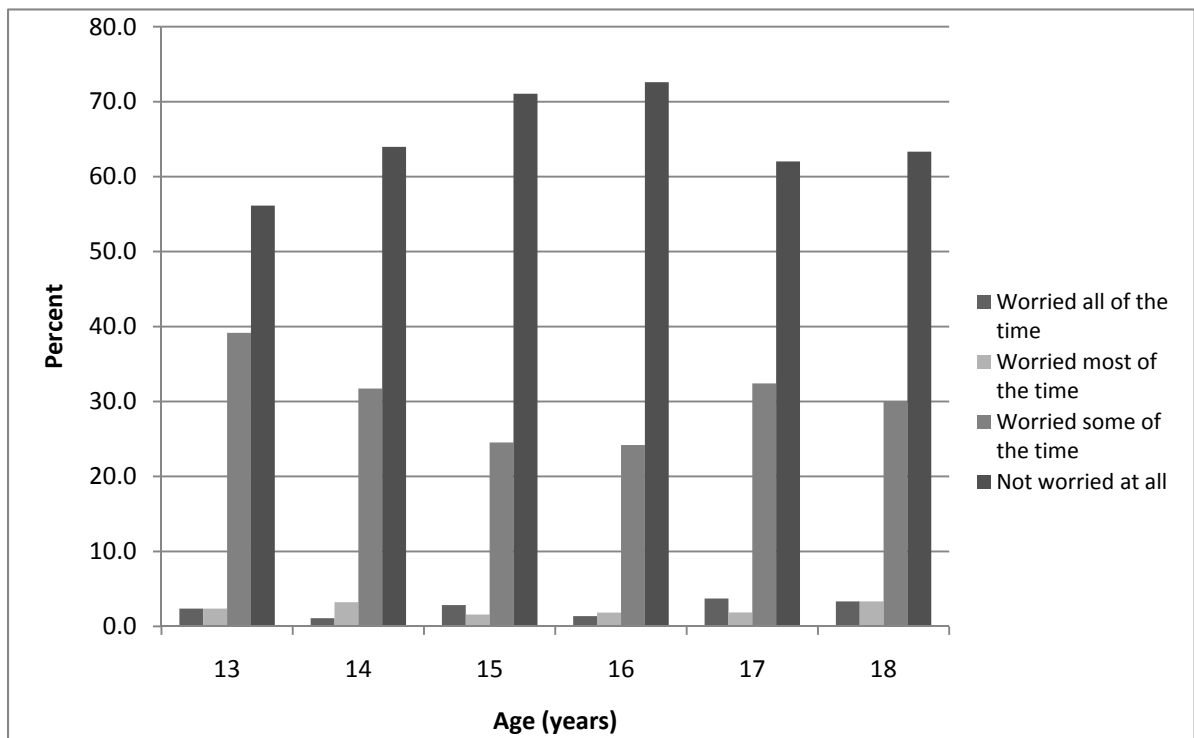
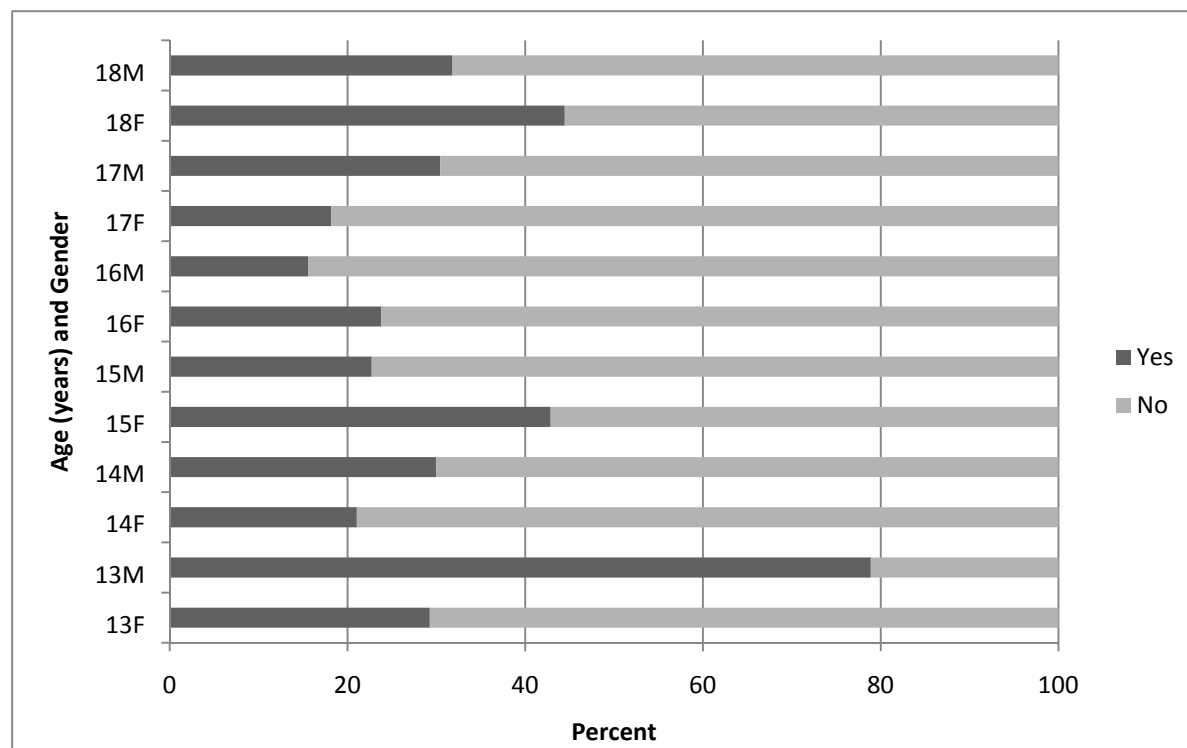


Figure 5.4 Of those with no privacy settings, have they felt unsafe online?



5.25 Canada's Privacy Commissioner investigated Facebook's privacy settings and found serious gaps in its handling of default settings that there was no privacy for anyone joining it. This resulted in changes to Facebook's privacy settings so that users had more control over personal information.²⁵ The Youth Affairs Council of South Australia suggested that:

websites frequented by children and young people often have privacy policies that are wordy and difficult to understand. YACSA would strongly support AYAC's proposal that the government implement strategies to promote the use of youth-friendly, plain language privacy policies for online services, so young people can make an informed decision about disclosing their personal information.²⁶

25 Victorian Privacy Commissioner: Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, pp. CS71, 79; *Submission 59*, p. 7; Mrs Tiffany Downing, South Australian Office of Youth, *Transcript of Evidence*, 3 February 2011, p. CS25.

26 Youth Affairs Council of South Australia, *Supplementary Submission 25.1*, pp. 16-17.

5.26 Ms Candice Jansz has found the default for privacy settings is an 'opt out' manner and they are constantly changing. She also commented on the capacity of young people to keep up with these changes:

What is heartening is that young people are now illustrating considerable cognitive adaptations to the online environment, and take steps to actively manage their own privacy and safety, whilst still reaping the benefits of these powerful technologies.²⁷

5.27 Privacy settings must be in 'very plain language – that is they are simple, short, clear and to the point'.²⁸ Further, representatives from the South Australian Office of Youth similarly commented:

It would also be helpful if, when you set up an account, there were more prompts around setting up your privacy before you can finalise that, so that you have to do it as part of your setup.²⁹

5.28 Facebook, however, pointed out that:

there are many more pop-ups and direct engagement with users to tell them that if you click on this you need to see your privacy settings: 'click here'. There is much more engagement and, in fact, Facebook was the only site in history to ever take all of its users – I think this was about a year ago – and send them a message that said, 'You cannot continue to use Facebook unless you review your privacy settings, make adjustments that you want, and confirm.' That is something that is unheard of on the internet. I think that there is much more user engagement on Facebook. In fact, Facebook has also allowed users to vote on the privacy policy and vote on the terms of service.³⁰

5.29 The results of a survey in 2007 by the Office of the Privacy Commissioner suggested that awareness of privacy had increased since 2004. Younger respondents, aged 18 to 24, continue to be less aware of their privacy rights than older respondents. The survey also showed that 50 percent of respondents were more concerned about providing information over the Internet than they had been two years earlier. However, a higher

27 Ms Candice Jansz, *Submission 44*, p. 4.

28 Dr Russell Smith, Principal Criminologist, Manager Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS12.

29 Ms Suellen Priest, Policy and Program Officer, Office of Youth SA, *Transcript of Evidence*, 3 February 2011, p. CS26.

30 Hon Mozelle Thompson, Advisory Board and Policy Adviser, Facebook, *Transcript of Evidence*, 21 March 2011, pp. CS7-8.

proportion of respondents aged 18 to 24 claimed to be less concerned than other age groups.³¹ The Australian Youth Affairs Coalition stated:

According to the Office of the Privacy Commissioner, the number of young Australians were concerned about internet privacy has quadrupled in past two years. However factors like peer pressure and incentives (such as quizzes, prizes or discounts) lead young people to disclose personal information online. AYAC believes education and transparency are key to supporting and empowering young people.³²

- 5.30 The Office of the Privacy Commissioner survey also indicated that young people were less concerned about disclosing their financial information, and much more likely to disclose personal information to receive a discount, a reward or a prize. Such behaviour, and being less informed about privacy issues, could put them at risk of identity theft.³³
- 5.31 The Victorian Privacy Commissioner believed that young people valued their privacy and were open to understanding and educating themselves about how they can make themselves safer online.³⁴ Recommendations made by a Senate Committee, in a report tabled in April 2011, suggest that all users of the online environment need more education about privacy.³⁵
- 5.32 The Committee supports Recommendation 2 in the Senate Environment and Communications References Committee's report:³⁶ Accordingly, the Committee recommends:

31 Office of the Privacy Commissioner, *Submission 92*, p. 5. See www.privacy.gov.au/publications/rcommunity07.pdf for this survey. Accessed 9 February 2011.

32 Australian Youth Affairs Coalition, *Submission 28*, pp. 9-10, citing Office of Privacy Commissioner (2007) *Community Attitudes to Privacy*, Office of Privacy Commissioner, p. 61.

33 Office of the Privacy Commissioner, *Submission 92*, p. 5; Victorian Privacy Commissioner, *Submission 59*, p. 4.

34 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS69.

35 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

36 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

Recommendation 6

That the Office of the Privacy Commissioner examine the issue of consent in the online context and develop guidelines on the appropriate use of privacy consent forms for online services and the Australian Government seek their adoption by industry.

Identity theft

5.33 Identity theft is a broad concept. It occurs when personal information, such as date of birth, credit card details, driver's licence numbers or passport or other identifying material, is obtained and is used to obtain a benefit or service. The Alannah and Madeline Foundation stated:

Prevalence of identity theft among young people is difficult to establish, as most does not involve criminal activity as such. Indeed a recent ACMA study suggests that young people have 'a high level of awareness of the risks of Internet use particularly when involved in social networking on the Internet'.³⁷

5.34 There have also been reports of social networking accounts being compromised for other purposes including fraud purposes.³⁸ For example, the Attorney-General's Department submitted:

We also know of children and young people who have had experiences of unknown others using their photos and in some cases assuming their identity, resulting in them receiving a detrimental credit rating.³⁹

5.35 It can also include use of an identity to harass or stalk a third person, and therefore activity of this kind can evolve into cyber-stalking.

5.36 While this theft is often associated with financial loss for adults, it can have serious consequences for young people if their information is used to fabricate fake documents, such as passports, or to commit further cyber-crimes.⁴⁰ The Federation of Parents and Citizens' Associations of NSW commented:

37 Alannah and Madeline Foundation, *Submission 22*, p. 27.

38 Attorney-General's Department, *Submission 58*, p. 7.

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

40 Office of the Privacy Commissioner, *Submission 92*, p. 6; Victorian Privacy Commissioner, *Submission 59*, p. 3

Children and adolescents are often not even aware of the meaning of identity theft. They may fill out a profile on the internet pretending to be another student from their class or use another student's photograph without realizing the potential harm that they may cause. It is essential to educate people about possible risks especially with the many pathways available to access the online environment.⁴¹

- 5.37 Comments submitted in free text spaces of the Committee's *Are you safe?* survey indicate that the awareness of young people is growing in Australia. When asked if they had felt unsafe online, the following comment was made:

I feel that identity theft is a huge issue, your name is the only secure piece of information i feel safe with sharing, i used to post other personal information but deleted it once i realised the risk (Male aged 14).

- 5.38 In 2007, the Australian Bureau of Statistics undertook a study of personal fraud with over 14,000 respondents aged over 15 years. The survey found that those from 25 to 34 years had the highest reports of identity theft (4.3 percent) against 2.1 percent of those aged 15 to 24 years. The 2007 Office of the Privacy Commissioner survey of people 18 years and older found that only 2 percent of respondents aged from 18 to 24 years had reported identity theft or fraud, compared with 9 percent of the total sample. While there is no immediate economic value in stealing a child's identity, once that person is 18 years old that identity becomes valuable. It can be used to apply for a 'proof of age' card, a driver's licence, passport or credit card. There is, therefore, a risk that criminals will collect personal information and wait before using the stolen identity.
- 5.39 Some young people also publicise personal information about parents, siblings and friends, thus exposing other people's information to the risk of identity theft.⁴²
- 5.40 The Australian Bureau of Statistics estimated that 806,000 Australians over the age of 15 had been the victims of personal fraud in the previous year,⁴³ costing nearly \$A1 billion per year.⁴⁴

41 Federation of Parents and Citizens' Associations of New South Wales, *Submission 76*, p. 4.

42 Attorney-General's Department, *Submission 58*, p. 7.

43 Commander Grant Edwards, Acting National Manager, High Tech Crime Operations, Australian Federal Police, *Transcript of Evidence*, 24 March 2011, p. CS3.

44 Attorney-General's Department, *Submission 58*, p. 7.

5.41 Preventing these crimes is also important in reducing the threat of terrorism and other serious criminal activity often based on the use of false or multiple identities.⁴⁵

5.42 In the past decade, there has been increasing awareness of the dangers posed by this abuse, but the Attorney-General's Department noted that there was a 'paucity' of data relating to young people and identity theft.⁴⁶ The Office of Privacy Commissioner added that:

... a range of measures are required to empower individuals to protect themselves in online environments and are essential to promoting effective privacy and cyber safety. These measures can include promoting education and awareness of the:

- risks posed by various ICT environments and interactions;
- measures that can be taken to mitigate risk, whether through technology or individual behaviour; and
- remedies available should something go wrong.⁴⁷

5.43 While the use of a pseudonym can be for constructive purpose for protection,⁴⁸ they can also be used:

... for the purpose of misleading people as distinct from merely covering one's most commonly used identity. I do not think that the incidence of this is vast but the impact of the individual instances can be quite significant. At this point we are talking about the concept of identity fraud. Identity theft goes much further. It is rare; it involves identity fraud being performed so comprehensively that the individual who used to use the identity cannot afford to keep using it.⁴⁹

5.44 As so little is known about their awareness of identity theft, more research is needed to establish how Australian children view privacy, identify their concerns and work with them to develop effective strategies against this abuse.⁵⁰ The following comments were made highlighting the numerous topics requiring more research and development of policy options:

Consideration need to be given to how organisations who work with children can best protect the privacy of children as

45 Attorney-General's Department, *Submission 58*, p. 7.

46 Attorney-General's Department, *Submission 58*, pp. 6- 7.

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

48 Dr Roger Clarke, *Transcript of Evidence*, 21 March 2011, p. CS28.

49 Dr Roger Clarke, *Transcript of Evidence*, 21 March 2011, p. CS29.

50 Victorian Office Child Safety Commissioner, *Submission 30*, p. 5

organisations increasingly use ICT to capture, record and share information about children.⁵¹

Hacking often relates to unique complications specific to the digital age, but may also involve something as timeless as friends betraying one another's trust after sharing their passwords. Either way, the situation requires an appropriate legal, educational and policy framework to deal with these complications.⁵²

With the rise of online social networking sites and instant messaging programs, additional issues related to identity theft such as impersonation and the use of fake accounts for cyber-bullying purposes are becoming increasingly prevalent.⁵³

- 5.45 Since 2005, measures have been taken that were intended to make it more difficult for criminals to create new identities or incorporate fabricated or inaccurate information into false credentials.⁵⁴ However, it is still the case that:

Most networks facilitate users duplicating passwords used elsewhere. When this occurs users are at greater risk in regard to identity theft.⁵⁵

Collection of unnecessary information

- 5.46 In their dealings with organisations, some young people disclose significant amounts of personal information. As has been shown, this can be used for a variety of illegal purposes with possible consequences for those individuals later in their lives.

- 5.47 Inclusion of 'mandatory' fields in online documents was seen as a specific problem: unless they are filled in, it is not possible to complete some online documents.

We need to bear in mind that information collected through the use of mandatory fields is sometimes used for unrelated purposes, such as marketing, statistics, advertisements or even profit motives. Our submission refers to the fact that the sale of information databases is a large industry in the United States. I remind the committee that social networking sites such as

51 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 5.

52 National Children's and Youth Law Centre, *Submission 138*, p. 8.

53 Office of Victorian Privacy Commissioner, *Submission 59*, p. 3.

54 Attorney-General's Department, *Submission 58*, pp. 6, 7.

55 Armorlog International, *Submission 4*, p. 2.

Facebook insist that real people register. Obviously that is for good reason but it does mean that people are again forced to provide quite a lot of personal information. For example, Facebook limit the age of people who use it to 13 years and over, but of course that is a very difficult thing for them to actually verify. The downside of doing a proper verification process would be that people would have to provide even more information. So that is one concern.⁵⁶

- 5.48 Joining social networking sites such as Facebook requires users to provide real names, dates of birth and other personal information. Facebook takes down fake sites very quickly:

Facebook, because it is a real-name culture, attracts a different kind of person. Because people tend to form groups according to family, friends and people they know, there is a certain degree of community policing that goes on. For example, child predators do not necessarily like to go to Facebook because if they have to use their real name or a verified email address you can find them. But there are a group of people who really do not care if you know who they are or not, because it is about power: they want you to know who they are. Now, what a company like Facebook does is use technology to try to root out aliases and fake accounts, and to look at patterns of conversation that indicate bullying or some sort of inappropriate behaviour. But one of the most valuable tools is to allow people within groups to report people who they think are doing bad things, and it is a remarkably effective tool. It is easier to be a bully if you are on text messaging or chat rooms and other things ...⁵⁷

- 5.49 The Deputy Victorian Privacy Commissioner commented on Facebook's policy:

Although this in itself is a bit of a concern for privacy people, they are kind of monitoring the community. People who are genuine friends of someone do realise that the child should not be on there. There is some kind of self-monitoring in a sense happening in

56 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS68.

57 Hon Mozelle Thompson, Chief Privacy Advisor, Facebook, *Transcript of Evidence*, 11 June 2010, p. CS16.

these online communities in the same way that that happens in real world communities.⁵⁸

5.50 The Victorian Privacy Commissioner added that:

Some people actually notify Facebook if they realise that there is a child under 13 clearly using Facebook.⁵⁹

5.51 The Commissioner commented on the requirement for the provision of personal information where, for example:

a young person registers with a social networking website. This may result in the collection of a child's full name, address or associated information: for instance, Facebook's Terms of Service states that real names and information must be used to register an account. Young persons may also be more likely to reveal personal information about themselves to receive a reward or discount - such as is required when signing up for an online game or contest.⁶⁰

5.52 The Commissioner noted that Facebook had 'quite intricate mechanisms' for looking at the information a would-be user has to provide, and this detected some children less than 13 years who seek to join. Anecdotally, there seemed to be users whose language skills do not reveal that they are less than 13 years old.⁶¹

5.53 Commenting more broadly, the Victorian Privacy Commissioner made the point that:

On certain sites such as instant messaging or chat rooms, children may also assume that using the Internet is anonymous and therefore appears 'safe'. This may increase the likelihood of a young person sharing their own personal information with someone they otherwise would not.⁶²

Current Australian privacy legislation contains provisions relating to the collection of personal information. The Victorian

58 Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS74

59 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS74.

60 Office of Victorian Privacy Commissioner, *Submission 59*, p. 4, citing Report of the Child Health Promotion Research Centre, *Review of existing Australian and International Cyber-Safety Research*, May 2009.

61 Victorian Privacy Commissioner: *Submission 59*, pp. 4- 5; Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, p. CS74.

62 Office of Victorian Privacy Commissioner, *Submission 59*, p. 4.

information Privacy Act and Commonwealth Privacy Act requires Victorian and Commonwealth public sector organisations, as well as some private sector organisations, to 'only collect personal information that is necessary for its functions or activities'.⁶³

For organisations interacting and collecting directly from children, organisations should consider whether their current collection notices are reasonably easy to understand so that children are able to exercise their privacy rights and make informed decisions.⁶⁴

5.54 Privacy NSW commented that:

In the case of internet sites which require an agreement to participate (excluding contractual matters) such as social networking sites, the question is therefore whether a child or young person has the capacity in the circumstances to consent to the use ... the capacity to consent should be measured on a sliding scale of factors, such as age, the ability to communicate consent, the individual's understanding of the issue in question, support from parents or other authorised representatives and the context in which the issues arise.⁶⁵

5.55 From an organisational perspective, the Victorian Privacy Commissioner expressed concern at the trend for organisations to collect personal information for unrelated purposes:

Over-collection leaves organisations open to larger and more damaging consequences when the security of a database is breached⁶⁶

5.56 Organisations may not require all the personal information they collect, other than to verify the provider's identity. If this information is not kept securely, it can be lost or disclosed to unauthorised persons. It may be transmitted and stored outside Australia, despite national and State/Territory privacy laws.⁶⁷ The Victorian Privacy Commissioner stated:

The effectiveness of privacy laws are limited in an online environment. Data is increasingly transmitted and stored globally,

63 Office of Victorian Privacy Commissioner, *Submission 59*, p. 5.

64 Office of Victorian Privacy Commissioner, *Submission 59*, p. 3.

65 Privacy NSW, *Submission 61*, p. 3.

66 Office of Victorian Privacy Commissioner, *Submission 59*, p. 5.

67 Victorian Privacy Commissioner: *Submission 59*, p. 6; Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, p. CS68; Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS74.

despite privacy regulation occurring at a state and national jurisdictional level.⁶⁸

5.57 The Alannah and Madeline Foundation noted that:

Privacy is a notion that does not technically exist in the online environment. If a technical system can be built by developers, it may be broken by hackers. However, privacy or the lack of privacy affects the average online user when information is shared and an embarrassing or unflattering incident occurs...

A common complaint in relation to social networking sites is the difficulty of controlling personal information and adjusting the privacy settings. With the growing awareness of the importance of protecting personal information comes an increased expectation of user control over how much other people can view of their digital footprint.⁶⁹

5.58 Material so collected can be used for unrelated purposes, such as marketing, statistics, advertisements, and tends to become increasingly comprehensive. The sale of information databases, compiled from material provided by customers or consumers, is a large and important industry in the United States.⁷⁰

5.59 Privacy laws also impose obligations on an organisation to take reasonable steps to inform individuals of:

- the identity of the organisation that is collecting the information and its contact details;
- the individual's ability to access the information;
- the purpose for which the information is collected;
- to whom the organisation usually discloses the information;
- any law requiring the information to be collected; and
- the main consequences for the individual if the information is not provided.⁷¹

68 Office of Victorian Privacy Commissioner, *Submission 59*, p. 6.

69 Alannah and Madeline Foundation, *Submission 22*, p. 27.

70 Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, p. CS68; Victorian Privacy Commissioner: *Submission 59*, p. 6.

71 Office of Victorian Privacy Commissioner, *Submission 59*, p. 2, citing *Information Privacy Act 2000* (Vic) and *Privacy Act 1988* (Cth).

5.60 In response to questions from the Committee in relation to selling information to third parties for marketing purposes, industry groups provided the following responses. Microsoft stated that did not 'just sell' information without having a business case.⁷² ninemsn stated that it:

has recently signed up to the Australian online behavioural advertising guidelines. That is a cross industry initiative. It is very broadly supported. We have now agreed to abide by certain standards regarding the way that we collect and use that sort of information. One of the key requirements is that we need to disclose where we are collecting behavioural information from and using it for third party online behavioural advertising targeting. There has also been an industry website launch that provides consumers with information about online behavioural advertising practices and will have opt-out capability for consumers to use so that they can opt out of that sort of advertising.⁷³

5.61 Facebook explained that there are companies that engage in data mining and data scraping without the consent of users and stated that:

Facebook does not sell information. It does not provide it to marketers. There are some people who we have seen in the press allege that, but it does not make sense from a business model standpoint. The reason that Facebook is valuable is because it keeps the sanctity of the data that belongs to individuals and if advertisers want to advertise to them, they have to go through Facebook. If they gave away the data or sold it, then Facebook would be less valuable.⁷⁴

5.62 Yahoo!7 added that the legislation requires that personal information be stored securely, therefore, it does not share personal information without the user's consent. It is a signatory to the Australian Best Practice Guidelines for Online Behavioural Advertising.⁷⁵ Yahoo!7 also provides

72 Mr Stuart Strathdee, Chief Security Adviser, Microsoft Australia, *Transcript of Evidence*, 21 March 2011, p. CS16.

73 Ms Jennifer Duxbury, Director, Compliance, Regulatory and Corporate Affairs, ninemsn, *Transcript of Evidence*, 21 March 2011, p. CS16.

74 Hon Mozelle Thompson, Advisory Board and Policy Adviser, Facebook, *Transcript of Evidence*, 21 March 2011, p. CS17.

75 Ms Samantha Yorke, Legal Director, Asia Pacific Region, Yahoo!7, *Transcript of Evidence*, 21 March 2011, p. CS17.

the capacity for users to turn off advertising or finetune their preferences.⁷⁶

5.63 Dr Roger Clarke cautioned, however, that:

The word 'selling' is a trap in the questioner's mouth. We always have to get rid of the word 'selling' when we are asking those kinds of questions and talk about 'transfer under any circumstances'. I do not care whether it is trading, gifting or exchange, because there are many uses of weasel words by organisations that are trying to avoid telling the truth. There is definitely considerable availability through various means of that profile data to many companies other than the company that originally collected the information ... A lawyer can quibble on behalf of the large corporations because they construct their terms in such a way that you have consented to everything that they might ever do.

5.64 The Committee supports Recommendation 3 in the Senate Environment and Communications References Committee's Report.⁷⁷ Accordingly, the Committee recommends:

Recommendation 7

That the Australian Government amend the *Privacy Act 1988 (Cth)* to provide that all Australian organisations which transfer personal information overseas, including small businesses, ensure that the information will be protected in a manner at least equivalent to the protections provided under Australia's privacy framework.

5.65 The Privacy and Data Protection Commissioners are currently considering:

making the organisations more responsible in terms of ... giving more notice, and also controlling, and not forcing children, or anyone really, to give over lots of information. That goes back to the amount of information you have to give to get access. So really those are the basic rules around data protection: only collecting

76 Ms Samantha Yorke, Legal Director, Asia Pacific Region, Yahoo!7, *Transcript of Evidence*, 21 March 2011, p. CS18.

77 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

what is necessary to be able to provide the service, not forcing people to provide more information than is needed to access a particular service, and putting controls on what other organisations get access to that service.⁷⁸

- 5.66 Dr Anthony Bendall referred to the ‘do-not-track’ model where the user can choose not to be tracked for the purposes of behavioural advertising.⁷⁹ Apple also offers technology to block particular types of applications, and these approaches could be applied by parents.⁸⁰ He also said that:

Depending on what you are going to use the information for, you give proper streamlined notice about that and have templates that allow people to use it rather than long legal documents. Notice should be given at the time that you are asking the person to make the decision so that the point at which they decide to provide the information would be the point at which the notice would be given rather than a generic document that they are meant to look at the first time they go online or every time they go online and which can be changed whenever a business likes – which is another practice that some online businesses engage in.⁸¹

- 5.67 The Committee supports Recommendation 4 in the Senate Environment and Communications References Committee’s report.⁸² Accordingly, it recommends:

78 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS73.

79 Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS70, citing the Federal Trade Commissioner’s Report *Protecting consumer privacy in an era of rapid change: a proposed framework for businesses and policymakers*. Released December 2010.

80 Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS73.

81 Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS70.

82 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

Recommendation 8

That the Office of Privacy Commissioner, in consultation with web browser developers, Internet service providers and the advertising industry, and in accordance with proposed amendments to the *Privacy Act 1988 (Cth)*, develop and impose a code which includes a 'Do Not Track' model following consultation with stakeholders.

- 5.68 The Committee supports Recommendation 5 in the Senate Environment and Communications References Committee's report.⁸³ It therefore recommends:

Recommendation 9

That the Australian Government amend the *Privacy Act 1988 (Cth)* to provide that an organisation has an Australian link if it collects information *from* Australia, thereby ensuring that information collected from Australia in the online context is protected by the *Privacy Act 1988 (Cth)*.

- 5.69 The Committee supports Recommendation 6 in the Senate Environment and Communications References Committee's Report.⁸⁴ Accordingly, the Committee recommends:

Recommendation 10

That the Australian Government amend the *Privacy Act 1988 (Cth)* to require all Australian organisations that transfer personal information offshore are fully accountable for protecting the privacy of that information.

- 5.70 The Committee supports Recommendation 6 in the Senate Environment and Communications References Committee's report.⁸⁵ It therefore recommends:

83 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

84 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

Recommendation 11

That the Australian Government consider the enforceability of provisions relating to the transfer of personal information offshore and, if necessary, strengthen the powers of the Australian Privacy Commissioner to enforce adequate protection of offshore data transfers.

- 5.71 The Committee supports Recommendation 7 in the Senate Environment and Communications References Committee's report.⁸⁶ Accordingly, the Committee recommends:

Recommendation 12

That the Australian Government continue to work internationally, and particularly within our region, to develop strong privacy protections for Australians in the online context.

85 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

86 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix

Other significant cyber-safety complexities

- 6.1 In addition to the cyber-threats set out in the two previous chapters, a number of other online concerns were raised in the evidence.
- 6.2 This chapter considers the validity of the term ‘technological-addiction’ and the online promotion of undesirable and/or illegal behaviours and practices, which may include exposure to violent and sexually violent online games as well as sites promoting suicide, self harm, anorexia and drug/alcohol abuse.

‘Technology addictions’

- 6.3 Parents/carers are becoming more aware of the time children spend online.¹ Addiction to various forms of technology is seen by some parents/carers as a problem for some of their adolescents. Gaming is seen as a ‘really big issue’ for many young boys, for whom it is their social networking site.²
- 6.4 For example, a concerned parent wrote about a child who, like some of his friends, is ‘games obsessed; his behaviour in relation to computer gaming looks like addictive behaviour.’ They engage virtually via gaming consoles connected to the Internet. Many of the games are M-rated. The M15 games some children play, despite their ages, were supplied by their parents. They play ‘for many hours each day’, longer when not at school, and ‘live

1 Mr Craig Scroggie, Vice President and Managing Director, Asia Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, p. CS3.

2 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. CS48.

talk' takes place as they play. The well-being of children when they are 'playing' together in such violent environments is a matter for concern.³

- 6.5 The Royal Australian and New Zealand College of Psychiatrists stated that 'problematic Internet use' (PIU) was first described in the late 1990s through case studies and scientific papers. At present, there is no official recognition of PIU by authorities or psychiatrists in the United States, Europe or Australia. China and other East Asian countries, who consider it a major public health concern, recognise it and provide extensive government funds for research and treatment.⁴
- 6.6 Although it is clear that there are significant impacts on some people, the College noted active debate about the recognition and classification of PIU. This included whether it merited inclusion in the forthcoming (2012) Fifth Edition of the Diagnostic and Statistical Manual. The term 'technology addiction' has negative and derogatory connotations, is scientifically incorrect and could lead to panic or undue worry. The College recommended that the term 'problematic Internet use' be used in place of 'technology addiction(s)' wherever possible.⁵
- 6.7 Appearing for the Australian Psychological Society, Dr McGrath confirmed that there is pressure, particularly in Asian journals, for adding 'technology addiction' to the list in the Diagnostic and Statistical Manual. She did not believe that it is a different manifestation, and noted that there did not seem to be any evidence it is widespread.⁶
- 6.8 The Australian Youth Affairs Coalition referred to the promotion and sensationalising of internet addiction in the media and the lack of clinical validity.⁷ Similarly, the Alannah and Madeline Foundation noted that, while there is a large commentary on the subject in the media, there is at present neither sound research evidence nor convincing theoretical support for such a syndrome:

Although a small number of writers and researchers (the commentary particularly from writers in China, Taiwan and Korea) claim that this is an identifiable behavioural syndrome, there is neither sound research evidence nor convincing theoretical support for such a syndrome at this time. It has been suggested

3 Anonymous correspondence received on 14 December 2010.

4 Royal Australian & New Zealand College of Psychiatrists, *Submission 120*, pp. 5, 8.

5 Royal Australian & New Zealand College of Psychiatrists, *Submission 120*, pp. 5, 8.

6 Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, pp. CS63-64.

7 Australian Youth Affairs Coalition, *Submission 28*, p. 6.

that 'internet addiction' is a term that has been promoted and sensationalised by the media but so far has little clinical validity.⁸

- 6.9 Professor Sheryl Hemphill expressed the view that it was not clear how prevalent this addiction was, or whether it did exist.⁹ In its submission, the Murdoch Children's Research Institute drew attention to the debate about its existence, and to the amount of information about 'technology addiction'. It noted that, while further research is required, an array of responses was also required to deal with the problem.¹⁰
- 6.10 The Alannah and Madeline Foundation also noted that there had been speculation that some unique aspects of the Internet may lure people into difficulties that they might otherwise avoid, such as online gambling and accessing pornographic sites. There is no research evidence that a passion for the Internet is long lasting, or that excessive usage is not simply a reflection of other social problems. Moreover, many of the strongest proponents for establishing a separate category of Internet addiction had some commercial interest in doing so. At some later time, however, excessive Internet usage may be given as another example of an Impulse Control Disorder, such as gambling, kleptomania, pyromania, etc.¹¹
- 6.11 While there are examples of young people who become 'addicted' to online activities such as Facebook or online games, it is necessary to be more aware of what they did online rather than blocking or only allowing access to specific sites.¹²
- 6.12 Mr Geordie Guy stated that, when individuals ignore pressing life problems by immersing themselves in online games or other online behaviour, this habit itself does not reflect problems with the online behaviour. Rather, these are symptoms of social problems.¹³
- 6.13 Mr Bruce Arnold believed that the notion of what he called 'cyber-addiction' had been strongly promoted by some therapists, tabloid journalists and totalitarian governments. He suggested that some adolescents had an over-engagement with electronic games or the Internet, in the same way that others over-engage with sport, comics, TV or a range of other activities. He also noted that there is very little

8 Alannah and Madeline Foundation, *Submission 22*, p. 24.

9 Associate Professor Sheryl Hemphill, Senior Research Fellow, Murdoch Children's Research Institute, *Transcript of Evidence*, 9 December 2010, p. CS21.

10 Murdoch Children's Research Institute: *Submission 111*, p. 3.

11 Alannah and Madeline Foundation, *Submission 22*, pp. 25- 26.

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

13 Mr Geordie Guy *Submission 105*, p. 10.

recognition within medical and legal communities of 'television addiction, videogame addiction or cyber-addiction', suggesting that these are essentially 'phantom disorders'.¹⁴

- 6.14 The Internet Industry Association quoted American research that urged proponents of safety education to study the history of youth drug and alcohol abuse prevention. It noted 'striking similarities' in the contexts of the two initiatives and the intensity of public concern. There were 'parallels in the eagerness to prevent Internet victimisation with the early, rushed efforts to prevent youth drug abuse' in the 1970s and 1980s. It was argued that such messages did little to change behaviour.¹⁵
- 6.15 The Consultative Working Group on Cybersafety, however, considered that computer gaming addictions are likely to be significant and have serious implications for Australian society. It stated that over-use of video games is most commonly seen among massive multiplayer online role playing game players, 'who can be somewhat marginalised socially'.¹⁶

Online gambling

- 6.16 While also not included in the Terms of Reference for this Inquiry, access to online gambling raises concerns for young people.
- 6.17 The past ten years has seen greatly increased and sophisticated ways for individuals to gamble, including access to 24-hour gambling through the Internet, mobile phones and interactive television. According to the Australian Psychological Society, there is evidence that young people are significantly more likely to participate in most forms of gambling, except lotteries and bingo, than older people. It believed that under-age gambling is 'particularly common': about 60 percent of those 13 to 17 years old reported gambling at least once a year.¹⁷ While gambling on interactive sites, such as online casinos, is not legal in Australia, use of the Internet for approved gambling on, for example, sporting events is allowed.¹⁸
- 6.18 The Youth Affairs Council of South Australia stated:

14 Mr Bruce Arnold, *Submission 60*, p. 5.

15 Internet Industry Association, *Submission 88*, pp. 5-6.

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

17 Australian Psychological Society, *Submission 90*, p. 11.

18 Mr David d'Lima, South Australia State Officer, Family Voice Australia, *Transcript of Evidence*, 3 February 2011, p. CS53.

In light of this, and the fact that there is still some debate as to whether internet addiction should be a diagnosable condition, YACSA will refrain from offering specific comment on the efficacy or otherwise of potential treatments for internet “addiction.” However, we note with interest developments overseas, for example a dedicated technology addiction clinic in the UK²⁸, and would encourage the government, in conjunction with the non-government sector, to explore these developments as well as any methodologies that specifically confront excessive and damaging technology use in young people.¹⁹

Violence

- 6.19 The Victorian Office of the Child Safety Commissioner noted that the high level of sexualised imagery and violence in computer and online games is currently being considered in the Minister for Home Affairs discussion paper.²⁰ The Alannah and Madeline Foundation commented:

Many children have unrestricted access to violence on the internet, through a variety of media, including videos, and violent games. Recent studies show that increased access to violence normalises this behaviour within young people’s social groups and can in a minority of cases lead to increased levels of violent behaviour.²¹

- 6.20 The Association of Parents and Friends of ACT Schools referred to the lack of ‘shockability’ due to desensitising through exposure.²² Similarly, Ms Catherine Davis from the Australian Education Union commented:

The harm that is being done by the promotion of violence through some of those games, not only violence per se, but also sexual violence in the sorts of computer games that are out there at the moment are mindboggling, and the effect that that has on both boys and girls and issues of online addiction and gaming and those sorts of things should be thrown into the mix today.²³

19 Youth Affairs Council of South Australia, *Supplementary Submission 25.1*, p. 12.

20 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 3.

21 Alannah and Madeline Foundation, *Submission 22*, p. 23.

22 Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS25.

23 Ms Catherine Davis, Federal Women’s Officer, Australian Education Union, *Transcript of Evidence*, 30 June 2010, p. CS25.

- 6.21 Concern was also expressed in relation to online advertising and the games available on line and it was suggested that legislative restrictions be considered.²⁴ The Australian Psychological Society advised:

The evidence strongly suggests that exposure to violent video games is a causal risk factor for increased aggressive behaviour, aggressive cognition, and aggressive affect, and for decreased empathy and pro-social behaviour.²⁵

Online promotion of inappropriate behaviours

- 6.22 Inappropriate social and health behaviours promoted in the online environment can include under-age drinking, drug use, suicide and anorexia.

Online availability of alcohol

- 6.23 NSW considered the issue of underage access to alcohol via the Internet in 2001. To address concerns, reforms were made requiring NSW-based licensees selling liquor over the Internet:

- To display liquor licence numbers prominently on their websites, and in any advertisement connected with Internet sales;
- To display a notice stating that it was an offence to sell, supply or obtain liquor on behalf of someone under 18 years of age;
- Prospective purchasers to supply their dates of birth; and
- Give written instructions to the person delivering the liquor requiring delivery to the adult who placed the order, or to another adult at the premises who undertakes to accept it on behalf of the person who placed the order.

- 6.24 These and other provisions were included in the *Liquor Act 2007* (NSW). NSW liquor laws cannot be used to regulate liquor sellers' activities if they were not located within that State.²⁶

24 Ms Dianne Butland, Executive Member, State Council, Federation of Parents and Citizens Associations of New South Wales, *Transcript of Evidence*, 30 June 2010, p. CS 34.

25 Australian Psychological Society, *Submission 90*, p. 10.

26 NSW Government, *Submission 94*, pp. 11-12.

Online availability of drugs

- 6.25 The Australian Customs and Border Protection Service noted that a range of prohibited goods, including illicit drugs, can be ordered via the online environment, in addition to:
- Guides to using/preparing drugs and expected experiences;
 - Guides on making narcotics with household items, including concealing them and avoiding attention from law enforcement;
 - Detailed instructions on constructing explosive devices and improvised firearms;
 - Use of over-the-counter drugs to produce a desired effect;
 - Techniques for obtaining requirements for the production of narcotics, including theft; and
 - Advice on the use of money transfer services when buying pharmaceuticals overseas.²⁷

Suicide

- 6.26 Although not included in the Inquiry's Terms of Reference, online encouragement of suicide was a concern raised by some participants. Distribution of material that counsels, promotes or provides instruction on methods of suicide is illegal.²⁸
- 6.27 The Alannah and Madeline Foundation noted that pro-suicide sites contain 'more than detailed' information on how to commit suicide. Many incite the reader to 'end the pain', to 'achieve the bliss of death'. Others hector and harass the reader, telling her/him how worthless their life is and how worthwhile it will be to end it.²⁹
- 6.28 Family Voice Australia argued that the basic principles of law should apply to the online environment as they apply to human communities in general. If necessary, the nature of this environment may require specific applications of these principles to ensure that they are applied effectively in a particular context.³⁰

27 Australian Customs and Border Protection Service, *Submission 109*, pp. 4-5.

28 Attorney-General's Department, *Submission 58*, p. 6.

29 Alannah and Madeline Foundation, *Submission 22*, pp. 22-23.

30 Family Voice Australia: *Submission 50*, p. 2.

- 6.29 Family Voice Australia drew attention to the suicide of two young people, in Melbourne in 2007, who had followed detailed instructions from a suicide website in the Netherlands. It believed that if young people were to be protected from harm, it had to be recognised that the online environment internationalised things such as the encouragement or promotion of suicide.³¹
- 6.30 Family Voice Australia are critical of the adequacy of the current 'take-down' orders which do not protect young people from harm on sites hosted overseas, and that Australian laws were 'lagging behind'.³² headspace added that:
- There are potential dangers with tribute pages when a person has suicided. We have found in the situation where a young person has suicided, the tribute page inadvertently glamorises suicide. Some pages also give details of the way the person killed themselves.³³
- 6.31 headspace suggested the establishment of a set of guidelines in relation to the reporting of suicide on-line and especially for social networking sites. headspace suggested this could be an extension of the current Mindframe National Media Initiative.³⁴

Anorexia

- 6.32 Open question forums provide a range of advice from bloggers on a range of subjects, including anorexia and drug usage.³⁵ For example, a simple search via Google leads to 'anorexia tips', and these included 'the thin commandments'.³⁶ The Alannah and Madeline Foundation stated:

Another content risk for children and young people are sites advocating for a range of unhealthy life choices, including pro-anorexia (pro-Ana) sites. A quick search brings up dozens of such sites, many of which offer 'thinspirational' tips such as 'creeds', motivation, tips and tricks and advice on how to stay thin.³⁷

31 Family Voice Australia: *Submission 50*, p. 3; Mr Richard Egan, National Policy Officer, *Transcript of Evidence*, 9 December 2010, p. CS53.

32 Mr Richard Egan, National Policy Officer, Family Voice Australia, *Transcript of Evidence*, 9 December 2010, p. CS53.

33 headspace, *Submission 127*, p. 4.

34 headspace, *Submission 127*, p. 4.

35 Alannah and Madeline Foundation, *Submission 22*, p. 23.

36 Mr David d'Lima, South Australia State Officer, Family Voice Australia, *Transcript of Evidence*, 3 February 2011, p. CS52; Alannah and Madeline Foundation, *Submission 22*, p. 22.

37 Alannah and Madeline Foundation, *Submission 22*, p. 22.

- 6.33 It was also noted that the Internet can provide a source of information assistance and support for people contemplating these behaviours:

Exposure to promotion of inappropriate behaviours can have negative implications for young people but equally the Internet provides a safe space for young people experiencing difficulty to express their views and access support online. Responses to this issue need to focus on helping young people to develop coping mechanisms and be aware of support available from parents and services in the community.³⁸

- 6.34 Internet service providers also have in place some measures in relation to these sites:

Facebook employs a reporting infrastructure to prevent self-harm content on their pages, wherein content is reviewed by the Facebook team and removed if necessary. MySpace also takes proactive steps to prevent self-harm material appearing on its users' profiles and encourages groups to help with recovery from eating disorder problems. MySpace's Terms of Use prohibits material promoting eating disorders and self-harm. MySpace bans and removes content that "promotes or otherwise incites...physical harm against any group or individual." These are just a few examples of how some global companies work to protect children from harmful content online.³⁹

Committee views

- 6.35 It must be recognised that, for most users most of the time, the online environment is a prominent, useful and important part of their lives. In considering any changes to current structures and practices, it is important to seek to reduce risks for the protection of all users, rather than introducing onerous restrictions in an attempt to protect the minority. It is also important to address causes of abuses rather than their symptoms.
- 6.36 To be effective, cooperative national solutions must be devised and implemented. Improvements for all users must be drawn together to involve professionals (such as researchers, teachers, police, youth workers), parents/carers and, most importantly, young people. Above all, best practice must be implemented.

38 Australian Youth Affairs Coalition, *Submission 28*, p. 6.

39 Family Online Safety Institute, *Submission 38*, p. 7.

- 6.37 Conclusions about the means of correcting abuses, and the recommendations that may follow from them, will therefore be addressed later in this Report.

You can share absolutely none of your details on the internet whatsoever, but that will probably detract from your enjoyment of the internet and you won't be able to use it to its full potential. Or, you could share all your details, which is highly risky, but will probably be more useful to you, and your friends. I try to find a balance between these extremes.¹

The decision to post

Information sharing, assessment of risk and the privacy of young people

- 7.1 This chapter presents the Committee's consultations with young people on privacy, risk and the information they share online. As the introductory quote indicates, young people engage in a balancing act: sharing information to form greater social networks while also attempting to maintain their personal security. Through its analysis, it seeks to shed light on how young people decide what information to share and when they feel comfortable doing so. It will also discuss appreciation and mitigation of risks online and the extent to which young Australians are already equipped to respond to dangers online. By gaining an insight into the decision-making processes of young Australians, education programs and awareness campaigns can be appropriately targeted and adapted.
- 7.2 Before discussing the decision-processes of young people, it is important to place their online activities in a broader social-development context. Fundamentally, young people 'post' their information, opinions and

1 Survey respondent, Female aged 17.

activities in order to construct the identity they wish to present to others. Therefore, the links between identity formation and online activities offers important background when gauging young people's appreciation of risks online and their reasons for sharing information.

The Internet and identity

- 7.3 According to the Australian Bureau of Statistics, young Australians are among the highly connected groups in the country.² This age group is also at a critical stage in their personal development, exploring and presenting their public and private identities. The advent of new technologies has presented young people with additional platforms to express themselves and experiment with different aspects of their identity. Further, young people often feel buoyed by the perceived distance and anonymity provided by the Internet.
- 7.4 Throughout the formative teenage-years, there are the contradictory desires to create an authentic identity, and the need for a sense of security –self-protection driven by a desire for acceptance by their peers. This tension is particularly evident in the online environment where the disclosure of personal information (the building blocks of an individual's identity) can be accessed and manipulated by third parties, potentially compromising personal safety and privacy.
- 7.5 A recent ethnographic study of members of Generations X and Y conducted by Dr Hilary Yerbury from the University of Technology, Sydney, commented that young people:
- are willing to display their thoughts, behaviours and actions to bolster their sense of self, and to leave traces of themselves in times and spaces where their embodied selves do not exist. In their discussions of trust and authenticity, they acknowledge that they interpret the characteristics of the other person in order to grant trust or recognise authenticity. By the same token, they are aware that others will interpret their actions and expressions to create another's view of their identity. Thus, sometimes they seek to safeguard their future by being careful about the traces they leave online and to maintain the safety of their offline selves by not

2 Australian Bureau of Statistics, 2006-07: *Household Use of Information Technology Survey*.

divulging the kind of information that would make them vulnerable to unwanted attention from strangers.³

Creating authentic identities online and offline

7.6 Creating one's identity has been described as a process of self-actualisation that includes the moral requirement of being able to act in a way that is 'true to oneself'.⁴ Yet social relations – the reaction of others – are also important. The construction of identity is a complex process:

It is future oriented, involving both psychological and social processes. The psychological processes of transformation interact with the social processes in ever-changing ways. The interactions are further complicated by the influences of particular aspects of life in the twenty-first century that impinge on the development of the sense of self... notably information and communication technologies.⁵

7.7 Young people have a strong sense of self and value authenticity; they expect to find authenticity in others whether online or offline.⁶ Though young people can be tolerant of ambiguity in the identity of others, there is an overarching expectation of sincerity; they believe that it is important to be able to trust in the authenticity of others.⁷ Importantly, these expectations of sincerity and anticipations of authenticity can expose young people to great risks online, particularly predatory conduct.

7.8 However, the *Are you safe?* survey received comments indicating that young people may be willing to compromise their individual authenticity to ensure safety and security online:

ever since i had access to the internet, parents and schools have taught me to never tell the truth on the net for fear of all the dangers (Female aged 17).

3 Yerbury, H. 2010, 'Who to be? Generations X and Y in civil society online', *Youth Studies Australia*, vol. 29, no. 2, p. 31.

4 A Giddens, 1991, *Modernity and self-identity: Self and society in the late modern age*, Stanford University Press, California, pp. 77-79.

5 Yerbury, H. 2010, 'Who to be? Generations X and Y in civil society online', *Youth Studies Australia*, vol. 29, no. 2, p. 31.

6 Yerbury, H. 2010, 'Who to be? Generations X and Y in civil society online', *Youth Studies Australia*, vol. 29, no. 2, p. 28.

7 Yerbury, H. 2010, 'Who to be? Generations X and Y in civil society online', *Youth Studies Australia*, vol. 29, no. 2, p. 28.

Only through your own doing can you reveal yourself online, and if you are really concerned about certain sites then you should create another email address or give false information which won't lead to your identity being revealed (Male aged 17).

On the internet you can basically just use a pseudonym or nickname that has little or no link to yourself to avoid these types of situations and then abandon it if things get too scary (Female aged 17).

- 7.9 In many situations, young people use this 're-set' strategy to protect themselves online. Although this may guard them from certain dangers online, 'abandonment' may not be sufficient to protect their privacy or personal information in all circumstances. These risks are discussed below and in Chapter 5 of this Report.
- 7.10 Many participants in the *Are you safe?* survey commented that they continually assess the authenticity of communications and content they view online. This indicates the positive impact of existing education and awareness programs. The strategies employed by young people to determine the level of risk and authenticity of content and communications is explored further below.

Exploring identity

- 7.11 In the course of its Inquiry, the Committee received a substantial body of evidence detailing how the Internet's perceived anonymity emboldens its users. Jedidiah, a Year 9 student, commented

A lot of people have a sudden change of personality when online – they may create fake accounts, imitate people or be very dissimilar to what they are in real life... Going online gives opportunities for many to experiment and compete for attention.⁸

- 7.12 This point is also discussed by social researchers:

Free from adult regulation, young people's articulation and expression of various parts of their identity to their friends and others supports critical peer-based sociality. Such processes of socialisation are essential for psychosocial development at a time when many young people are consolidating their identities,

8 Jedidiah, *Submission 133*, p. 1.

pulling up roots from their family, striving for independence and developing new types of relationships.⁹

- 7.13 A recent paper by the Cooperative Research Centre for Young People, Technology and Wellbeing commented that the flexibility of social networking and its capacity for individual customisation, allows young people use these services to 'experiment and find legitimacy for their political, ethnic, cultural or sexual identity'.¹⁰
- 7.14 In other studies, young people have also referenced a greater degree of acceptance due to the anonymity provided by new technologies, with one participant noting that he was active in the online environment because he did not feel limited by the reactions of others to ethnicity. The same participant felt that he could meet and engage with people with similar interests and viewpoints in a way that is denied to his embodied self.¹¹
- 7.15 The Committee's High School Forum also facilitated a discussion on the effect of perceived anonymity and distance provided by the online environment. When asked 'How many of you believe that you change your personality? ... When your friends go online do you believe they change their personality?', the majority of the Forum's participants indicated by a show of hands that they felt emboldened by online communications or had noticed a change in the personality of others. The question prompted discussion, with the following comments made by participants:

I think some people, in real life, act differently on Facebook maybe because of their insecurities. I find some people will talk to me on Facebook but will not talk to me in real life. I do not know why that is but maybe it is their insecurities or they feel reluctant to come up to me. They feel more secure on Facebook because it is not a face-to-face situation.¹²

I think that everybody does get a little bit braver on Facebook or when texting because you do not have to physically interact with the person you are communicating with. It does not necessarily

9 Collin, P. *et al*, 2011 *The Benefits of Social Networking Services*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 16.

10 Collin, P. *et al*, 2011 *The Benefits of Social Networking Services*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 16.

11 Yerbury, H. 2010, 'Who to be? Generations X and Y in civil society online', *Youth Studies Australia*, vol. 29, no. 2, p. 28.

12 Hayden, High School Forum Participant, *Transcript of Evidence*, 20 April 2011, p. CS22.

change your personality but it does give you more confidence to behave in a way that you probably would not when face-to-face.¹³

7.16 However, this freedom to experiment with an 'emboldened' identity does cause some concern among young people. Other studies have argued that as young people grow towards maturity, they do 'not want to be held to the actions and beliefs recorded online whilst they are creating their self-identity'.¹⁴ Concerns about 'digital-footprints' are discussed below.

What information do young people share?

Types of information shared

7.17 The previously mentioned, *Click and Connect: Young Australians' Use of Online Social Media* report by the Australian Communications and Media Authority (ACMA) revealed willingness to make personal information public differs greatly. An objective of the *Are you safe?* survey was to further explore this issue and better understand the types of information young people share online. The survey asked participants about their willingness to divulge their:

- name;
- age or birthday;
- address;
- telephone number;
- school attended;
- bank account details;
- holiday plans;
- passwords or email addresses; and
- photos of others.

7.18 Each of these is addressed below.

13 Amanda, High School Forum Participant, *Transcript of Evidence*, 20 April 2011, p. CS22.

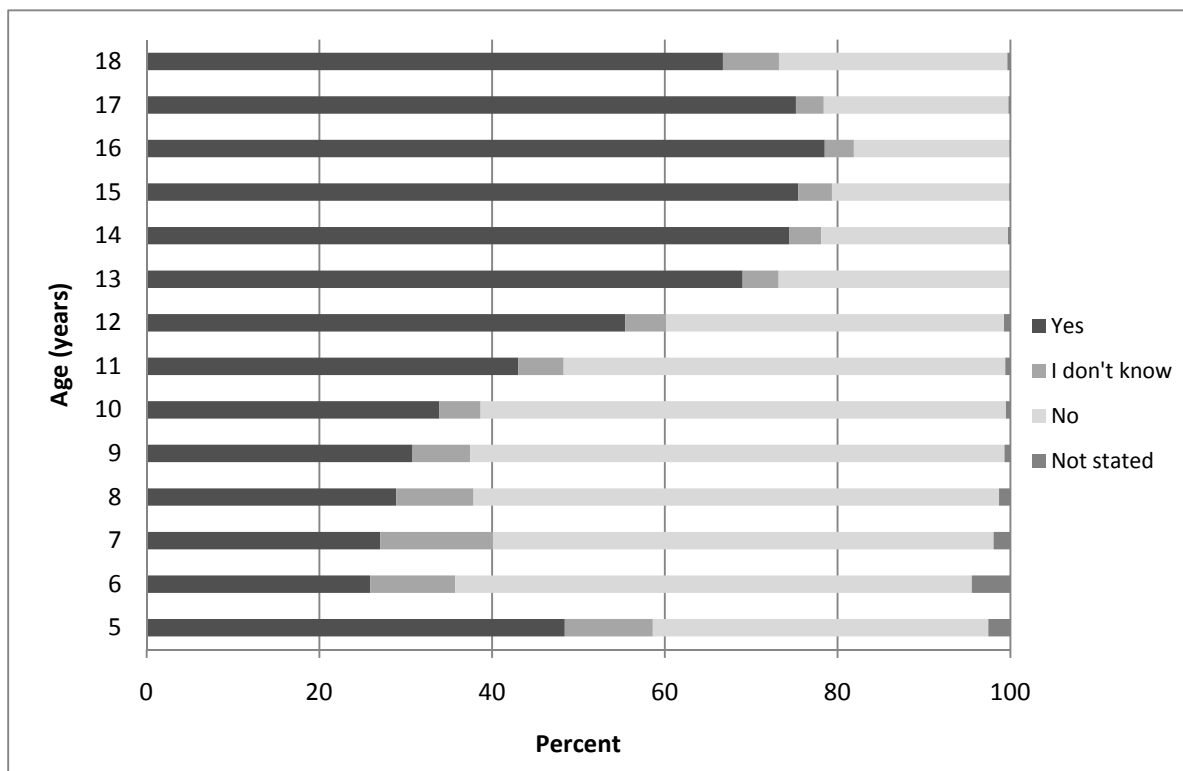
14 Yerbury, H. 2010, 'Who to be? Generations X and Y in civil society online', *Youth Studies Australia*, vol. 29, no. 2.

Name

7.19 The overall majority of participants in the *Are you safe?* survey stated that they share their name online. However, the older the survey’s participants were, the more comfortable they felt to disclose their name online. Research by the Cooperative Research Centre for Young People, Technology and Wellbeing attributed these trends to young people’s desire to both strengthen offline relationships through online communications as well as seek out new online networks.¹⁵

7.20 There was no significant difference between the genders on this question.

Figure 7.1 Do you share your name online? (Age)



15 Collin P, et al, 2011, *The Benefits of Social Networking Services*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 17.

Table 7.1 Do you share your name online?

		Yes		No		I don't know		Not stated		Total
Sex		%	#	%	#	%	#	%	#	#
5 Years	M	46.7	35	42.7	32	10.7	8	0	0	75
	F	50	41	35.4	29	9.8	8	4.9	4	82
6 Years	M	31.3	15	50	24	12.5	6	6.3	3	48
	F	21.9	14	67.2	43	7.8	5	3.1	2	64
7 Years	M	29.1	32	57.3	63	10.9	12	2.7	3	110
	F	24.7	24	58.8	57	15.5	15	1	1	97
8 Years	M	31.4	133	57.3	243	9.4	40	1.9	8	424
	F	26.8	132	63.9	315	8.5	42	0.8	4	493
9 Years	M	33.0	331	59.5	597	7.0	10	0.6	6	1004
	F	28.8	310	64.1	691	6.4	69	0.7	8	1078
10 Years	M	35.0	596	59.8	1017	4.6	79	0.5	9	1701
	F	32.8	590	61.8	1111	4.9	88	0.5	9	1798
11 Years	M	42.0	968	52.5	1211	4.8	110	0.7	16	2305
	F	44.0	1101	49.8	1247	5.7	142	0.5	12	2502
12 Years	M	54.2	1213	41.0	918	4.1	92	0.7	16	2239
	F	56.6	1281	37.2	842	5.4	123	0.8	17	2263
13 Years	M	66.0	1247	31.0	586	3.0	56	0.1	1	1890
	F	71.3	1752	23.5	576	5.1	125	0.1	3	2456
14 Years	M	71.3	1149	25.9	418	2.4	39	0.4	6	1612
	F	76.9	1524	18.1	359	4.8	95	0.2	4	1982
15 Years	M	74.0	881	22.5	268	3.4	41	0.1	1	1191
	F	76.7	1054	19.8	259	4.3	59	0.1	2	1374
16 Years	M	75.8	612	21.3	172	2.7	22	0.1	1	807
	F	80.7	805	15.3	153	3.9	39	0.1	1	998
17 Years	M	75.4	298	22.0	87	2.3	9	0.3	1	395
	F	75.0	426	21.0	119	3.9	22	0.2	1	568
18 Years	M	67.9	212	25.6	80	6.1	19	0.3	1	312
	F	65.3	169	27.4	71	6.9	18	0.4	1	259

- 7.21 Through free text spaces, a substantial number of participants aged 12 years or younger commented they would use their first name, but would be more hesitant in divulging their surname. For example, comments such as those included below were common in participants aged 12 years or younger:

I always confront my parents before joining to a site or giving any info. about myself. They are like pretty protective so I usually make up a birth date if it is compulsory. Never will I tell any real details of myself that could put me in a dangerous position. With my name, first is alright yet second (last name) is strict no no (Female aged 12).

I think it is okay to put your first name because you are not the only person in the world with that name and it would be impossible to find anymore details if they just knew your first name, but never put your last name because it makes it easier for people to track you down (Female aged 12).

- 7.22 Notably, this strategy was not referenced by participants over the age of 13.
- 7.23 The use of nick-names was a common alternative expressed by participants of all ages through the optional free-text spaces. One survey respondent commented:

I think it's OK to put your nick-name up on the web but you shouldn't put your full name ... because they could use that to send you things you don't want [or] hack your private things (Male aged 10).

- 7.24 Research by Australian Communications and Media Authority found that despite privacy concerns, many children and young people in its study claimed they might give their real name if the majority of their peers also used their full name.¹⁶ A comment cited by ACMA illustrates this point:

I have my full name on Facebook. I didn't want to do it but I realised that everyone else and all my friends had.¹⁷

16 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 49.

17 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 49.

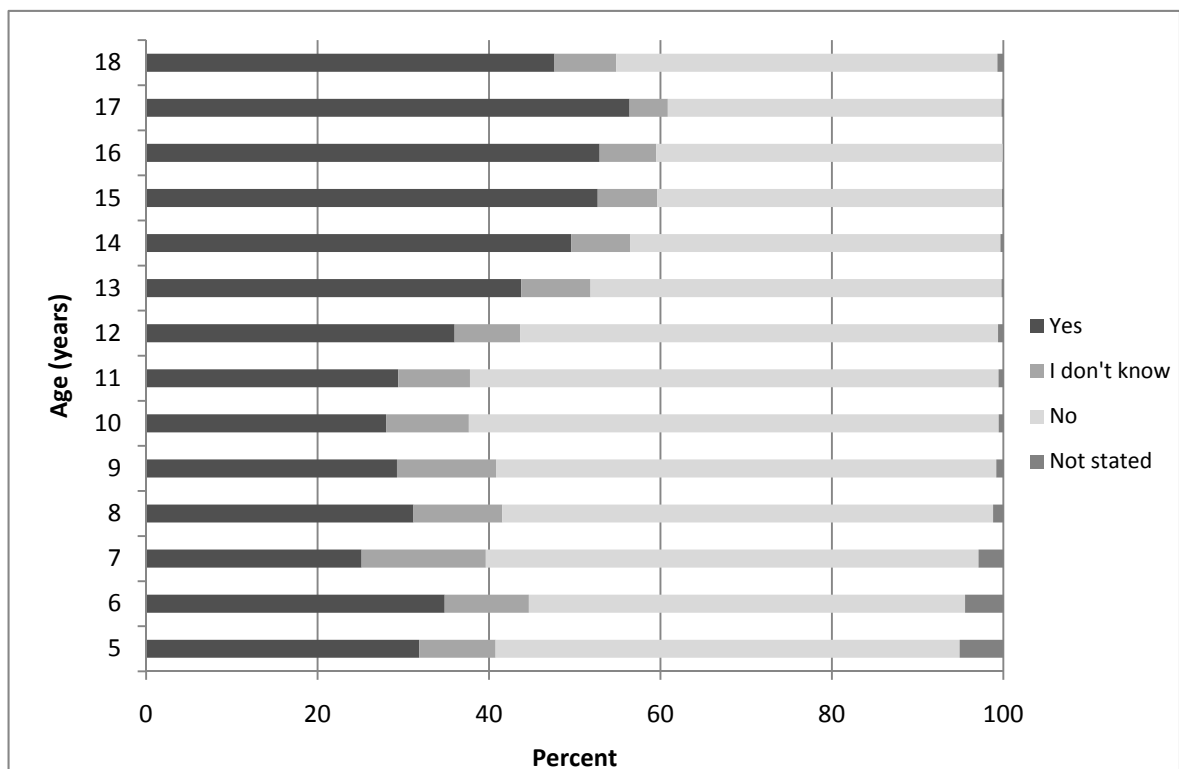
- 7.25 The Committee's consultations revealed some hesitation by some survey respondents, such as:

There are a surprising amount of people on facebook who have posted their mobile, school and networks on their profile-I haven't even put my last name on facebook because I know that people I know will know who I am without my last name-if they don't, then I probably won't add [them] (Female aged 14).

Age or birthday

- 7.26 When asked if they would disclose their age or birthday, results showed that young people are generally hesitant: 51.9 percent of respondents answered that they would not share their age or birthday online.
- 7.27 There were no significant differences between the sexes, but there was an increase in the number of respondents aged 13 years or older that share their age or birthday online (31.0 percent of respondents 12 years or young share their age online, compared to 49.1 percent of respondents aged 13 years or older).

Figure 7.2 Do you share your age or birthday online? (Age)



- 7.28 The survey asked respondents to qualify their answer through free text space at the end of the question. A recurring theme in the comments was that age or birth dates are not perceived to be unique or identifying features. For example, one survey respondent commented:

I strongly believe that it is okay to put your name and age on the internet , because there is other people that have the same name as you and others that have the same age (Female aged 10)

- 7.29 Similarly, some comments by participants indicate a general ambivalence and awareness of the value of this type of information to third parties. For example:

I don't think it matters whether or not I put my age or birthday on it because I no one can trace you through your name or birthday (Male aged 12).

Table 7.2 Do you share your age or birthday online?

	Sex	Yes		No		I don't know		Not stated		Total
		%	#	%	#	%	#	%	#	#
5 Years	M	33.3	25	58.7	44	5.3	4	2.7	2	75
	F	30.5	25	50.0	41	12.2	10	7.3	6	82
6 Years	M	33.3	16	45.8	22	14.6	7	6.3	3	48
	F	35.9	23	54.7	35	6.3	4	3.1	2	64
7 Years	M	24.5	27	54.5	60	16.4	18	4.5	5	110
	F	25.8	25	60.8	59	12.4	12	1.0	1	97
8 Years	M	33.5	142	54.2	230	10.6	45	1.7	7	424
	F	29.2	144	59.8	295	10.1	50	0.8	4	493
9 Years	M	32.9	330	56.8	570	9.6	96	0.8	8	1004
	F	25.9	279	59.8	645	13.5	145	0.8	9	1078
10 Years	M	30.0	511	61.3	1043	8.1	137	0.6	10	1701
	F	26.0	468	62.3	1120	11.2	201	0.5	9	1798
11 Years	M	30.7	707	61.3	1412	7.3	169	0.7	17	2305
	F	28.3	707	62.0	1552	9.3	233	0.4	10	2502
12 Years	M	35.8	801	57.0	1277	6.6	147	0.6	14	2239
	F	36.2	819	54.5	1233	8.7	197	0.6	14	2263
13 Years	M	44.6	842	49.7	940	5.5	104	0.2	4	1890
	F	43.1	1059	46.6	1144	10.1	248	0.2	5	2456
14 Years	M	49.3	794	45.9	740	4.3	69	0.6	9	1612
	F	49.8	988	41.0	812	9.0	179	0.2	3	1982
15 Years	M	53.1	632	42.2	529	4.6	55	0.1	1	1191
	F	52.3	719	38.5	503	9.0	123	0.2	3	1374
16 Years	M	55.8	450	39.2	316	5.1	41	0.0	0	807
	F	50.6	505	41.5	414	7.8	78	0.1	1	998
17 Years	M	58.0	229	38.0	150	3.5	14	0.5	2	395
	F	55.3	314	39.6	225	5.1	29	0.0	0	568
18 Years	M	48.1	150	44.2	138	6.7	21	1.0	3	312
	F	47.1	122	44.8	116	7.7	20	0.4	1	259

Address

7.30 Overall, 93.2 percent of participants answered that they would not divulge their address online. However, there was a peak at both ends of the age sample with increases in those who answered they have disclosed their address online and those who were unsure.

Figure 7.3 Do you share your address online? (Age)

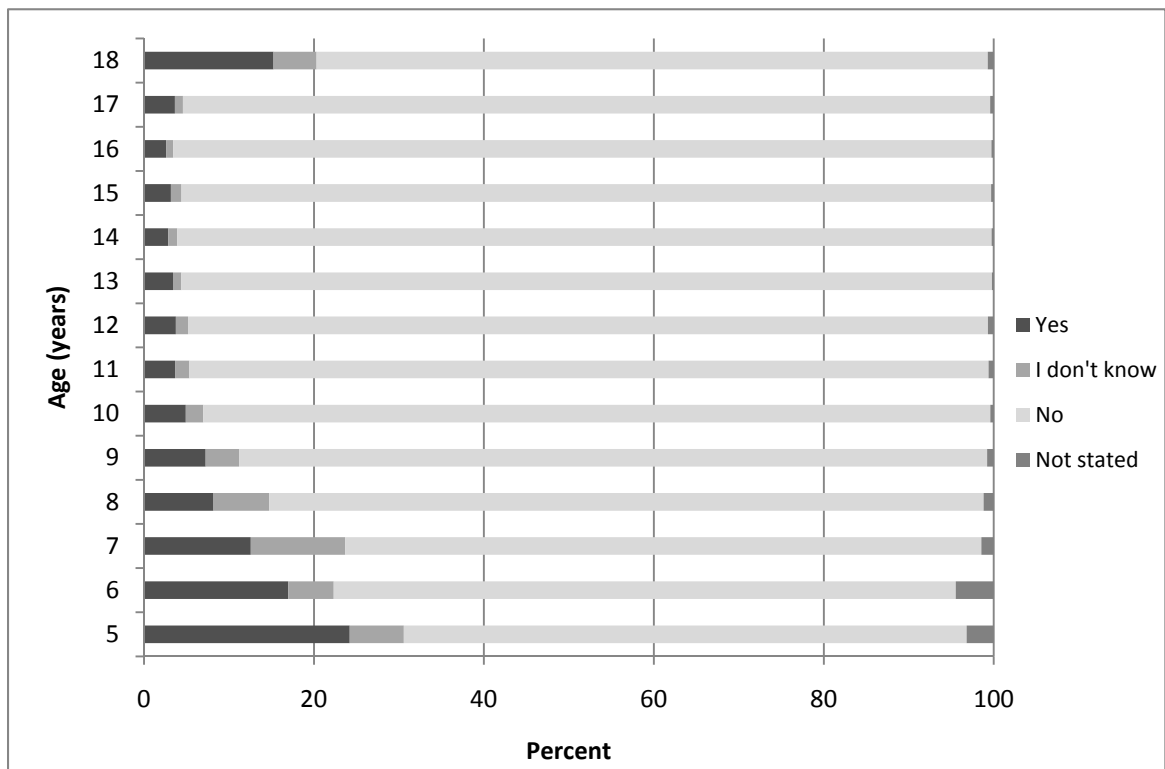


Table 7.3 Do you share your address online?

	Sex	Yes		No		I don't know		Not stated		Total
		%	#	%	#	%	#	%	#	#
5 Years	M	22.7	17	72.0	54	4.0	3	1.3	1	75
	F	25.6	21	61.0	50	8.5	7	4.9	4	82
6 Years	M	16.7	8	70.8	34	6.3	3	6.3	3	48
	F	17.2	11	75.0	48	4.7	3	3.1	2	64
7 Years	M	12.7	14	72.7	80	12.7	14	1.8	2	110
	F	12.4	12	77.3	75	9.3	9	1.0	1	97
8 Years	M	9.4	40	80.7	342	8.3	35	1.7	7	424
	F	7.1	35	87.0	429	5.1	25	0.8	4	493
9 Years	M	9.5	95	84.9	852	4.9	49	0.8	8	1004
	F	5.2	56	91.0	981	3.1	33	0.7	8	1078
10 Years	M	6.3	108	90.6	1541	2.6	45	0.4	7	1701
	F	3.6	64	94.5	1700	1.5	27	0.4	7	1798
11 Years	M	4.2	97	93.2	2148	1.8	42	0.8	18	2305
	F	3.2	79	94.9	2374	1.5	38	0.4	11	2502
12 Years	M	5.3	119	92.2	2065	1.8	40	0.7	15	2239
	F	2.2	50	96.0	2173	1.1	24	0.7	16	2263
13 Years	M	4.8	90	93.6	1769	1.4	27	0.2	4	1890
	F	2.4	58	96.8	2377	0.7	16	0.2	5	2456
14 Years	M	4.3	70	94.1	1517	1.2	19	0.4	6	1612
	F	1.7	33	97.2	1927	1.0	19	0.2	3	1982
15 Years	M	5.1	61	93.0	1108	1.7	20	0.2	2	1191
	F	1.5	20	97.2	1336	0.9	12	0.4	6	1374
16 Years	M	4.5	36	94.2	760	1.2	10	0.1	1	807
	F	1.1	11	98.0	978	0.5	5	0.4	4	998
17 Years	M	7.8	31	89.6	354	1.8	7	0.8	3	395
	F	0.7	4	98.8	561	0.4	2	0.2	1	568
18 Years	M	13.8	43	80.8	252	4.8	15	0.6	2	312
	F	17.0	44	76.8	199	5.4	14	0.8	2	259

Telephone number

7.31 Similar results were found in participants disclosing their telephone numbers online. Overall 90.4 percent of respondents do not disclose their telephone number online, however there was an increase at both ends of the age spectrum.

7.32 Notably, 11.8 percent of participants aged 18 disclose their telephone number online, compared with 5.5 percent of those aged 13 to 17 years.

Figure 7.4 Do you share your telephone number online? (Age)

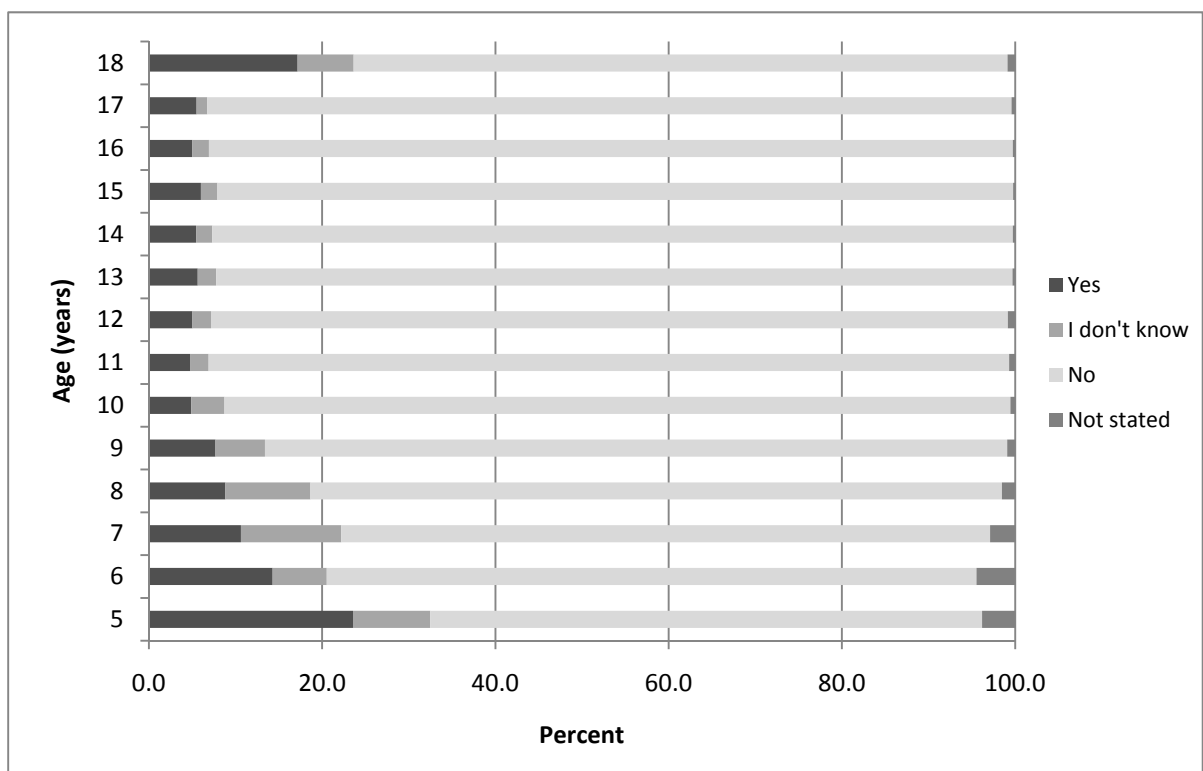


Table 7.4 Do you share your telephone number online?

	Sex	Yes		No		I don't know		Not stated		Total #
		%	#	%	#	%	#	%	#	
5 Years	M	20.0	15	72.0	54	6.7	5	1.3	1	75
	F	26.8	22	56.1	46	11.0	9	6.1	5	82
6 Years	M	8.3	4	79.2	38	6.3	3	6.3	3	48
	F	18.8	12	71.9	46	6.3	4	3.1	2	64
7 Years	M	12.7	14	72.7	80	10.9	12	3.6	4	110
	F	8.2	8	77.3	75	12.4	12	2.1	2	97

8 Years	M	11.3	48	74.1	314	12.3	52	2.4	10	424
	F	6.7	33	84.8	418	7.7	38	0.8	4	493
9 Years	M	9.3	93	82.3	826	7.5	75	1.0	10	1004
	F	6.2	67	88.9	958	4.1	44	0.8	9	1078
10 Years	M	6.1	104	89.2	1518	4.1	70	0.5	9	1701
	F	3.7	67	92.2	1657	3.6	64	0.6	10	1798
11 Years	M	5.8	133	90.4	2084	2.9	67	0.9	21	2305
	F	3.8	95	94.3	2359	1.4	36	0.5	12	2502
12 Years	M	6.9	155	89.5	2005	2.6	59	0.9	20	2239
	F	3.1	71	91.1	2136	1.7	38	0.8	18	2263
13 Years	M	7.5	141	89.5	1692	2.8	52	0.3	5	1890
	F	4.2	104	93.8	2304	1.6	40	0.3	8	2456
14 Years	M	7.8	126	89.4	1441	2.4	38	0.4	7	1612
	F	3.5	70	94.9	1880	1.5	29	0.2	3	1982
15 Years	M	8.6	103	88.8	1058	2.4	29	0.1	1	1191
	F	3.7	51	94.5	1298	1.5	20	0.4	5	1374
16 Years	M	7.9	64	89.7	724	2.2	18	0.1	1	807
	F	2.6	26	95.3	951	1.7	17	0.4	4	998
17 Years	M	9.6	38	87.3	345	2.3	9	0.8	3	393
	F	2.6	15	96.7	549	0.5	3	0.2	1	568
18 Years	M	19.3	48	71.8	186	8.1	21	0.8	2	259
	F	17.2	50	75.5	431	6.5	37	0.9	5	571

School attended

- 7.33 The majority of participants answered that they would not disclose the name of their school online (68.9 percent). There was no significant difference between male and female respondents, though older participants indicated they are more willing to share information about the school they attend online: 16.2 percent of respondents aged 12 years or younger share this information, compared with 32.0 percent of respondents aged 13 years or older.
- 7.34 Of those that do share the name of their school online, many appear to do so to link up with others that attend their school. For example, the following comments were common from those that disclose their school:

sometimes putting information like the school you attend could be dangerous, but its something a lot of people do so that they can identify their peers on facebook (Female aged 14).

Because I am in Year 11, putting this information (Name and School) is quite essential for me to contact past friends and future business opportunities (Male aged 17).

7.35 However, one participant noted a belief that the size of the school would mitigate any risk posed by sharing this information:

I don't think it matters whether or not I put my school ... because even though people can track my school, my school has over 500 people so I don't think I'd have to worry about that (Male aged 12).

Figure 7.5 Do you post the name of your school online? (Age)

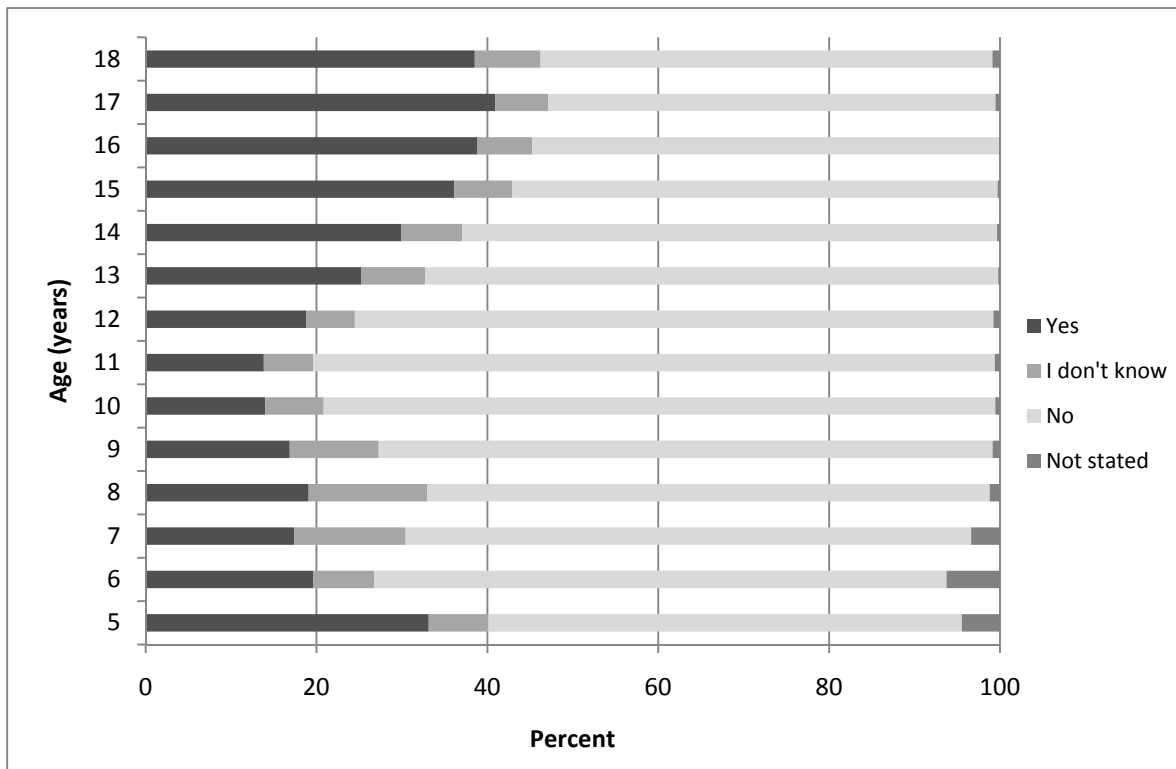


Table 7.5 Do you post the name of your school online?

	Sex	Yes		No		I don't know		Not stated		Total
		%	#	%	#	%	#	%	#	#
5 Years	M	36.0	27	57.3	43	4.0	3	2.7	2	75
	F	30.5	25	53.7	44	9.8	8	6.1	5	82
6 Years	M	14.6	7	62.5	30	14.6	7	8.3	4	48
	F	23.4	15	70.3	45	1.6	1	4.7	3	64
7 Years	M	20.0	22	65.5	72	10.9	12	3.6	4	110
	F	14.4	14	67.0	65	15.5	15	3.1	3	97
8 Years	M	22.2	94	61.6	261	14.6	62	1.7	7	424
	F	16.4	81	69.6	343	13.2	65	0.8	4	493
9 Years	M	20.9	210	67.9	682	10.3	103	0.9	9	1004
	F	13.1	141	75.5	814	10.6	114	0.8	9	1078
10 Years	M	16.1	274	76.3	1298	7.0	119	0.6	10	1701
	F	12.0	216	80.8	1453	6.7	120	0.5	9	1798
11 Years	M	17.0	391	76.8	1770	5.5	127	0.7	17	2305
	F	11.0	274	82.5	2064	6.1	152	0.5	12	2502
12 Years	M	21.3	477	72.6	1625	5.4	120	0.8	17	2239
	F	16.3	368	76.8	1739	6.1	138	0.8	18	2263
13 Years	M	27.8	526	65.7	1241	6.3	119	0.2	4	1890
	F	23.3	572	68.2	1675	8.3	204	0.2	5	2456
14 Years	M	33.9	547	60.2	971	5.3	85	0.6	9	1612
	F	26.7	529	64.5	1278	8.7	172	0.2	3	1982
15 Years	M	42.1	501	52.7	628	5.0	60	0.2	2	1191
	F	30.9	425	60.1	830	8.3	114	0.4	5	1374
16 Years	M	45.6	368	49.1	396	5.3	43	0.0	0	807
	F	33.4	333	59.1	590	7.3	73	0.2	2	998
17 Years	M	48.1	190	45.6	180	5.3	21	1.0	4	395
	F	35.9	204	57.0	342	6.9	39	0.2	1	568
18 Years	M	39.7	124	52.2	163	7.1	22	1.0	3	312
	F	37.1	96	53.7	139	8.5	22	0.8	2	259

Bank account details

- 7.36 An large majority of participants stated they would not share their bank account details online (94.0 percent).
- 7.37 The increase at the age of 18 years might be explained by an increase in those engaging in the digital economy and making purchases online.

Figure 7.6 Do you share your or your family's bank details online? (Age)

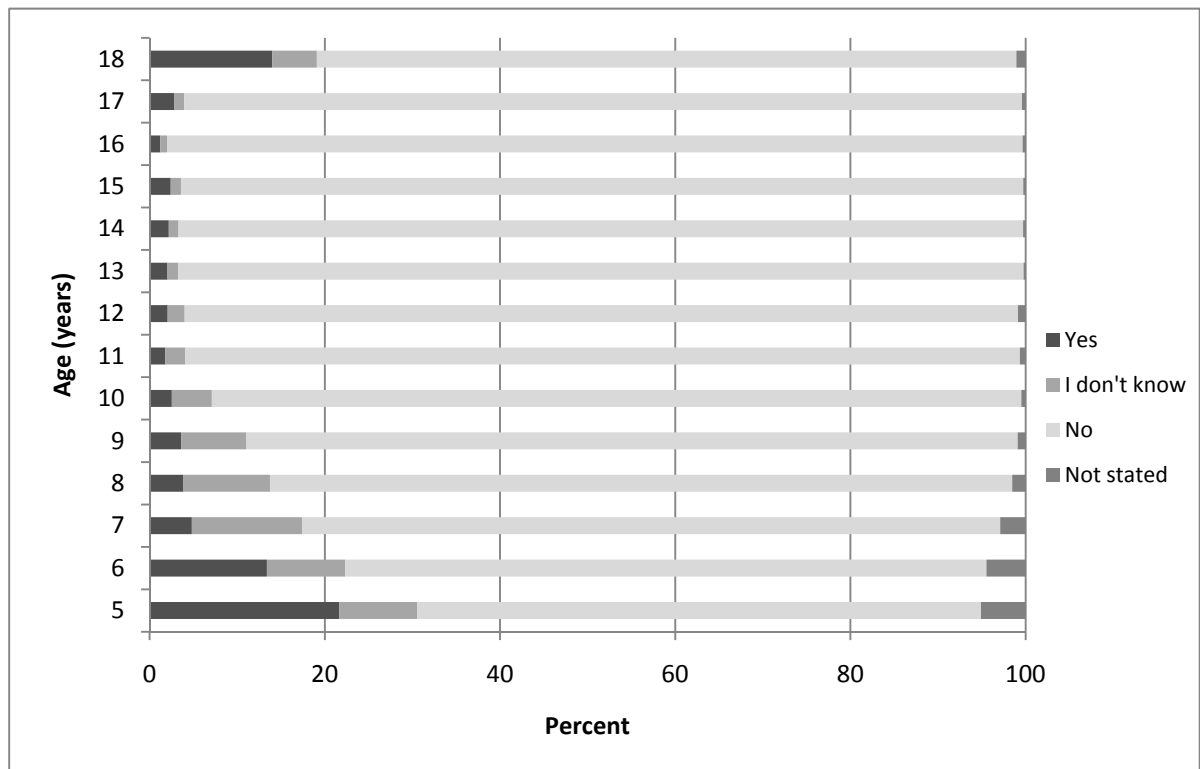


Table 7.6 Do you share your or your family's bank account details online?

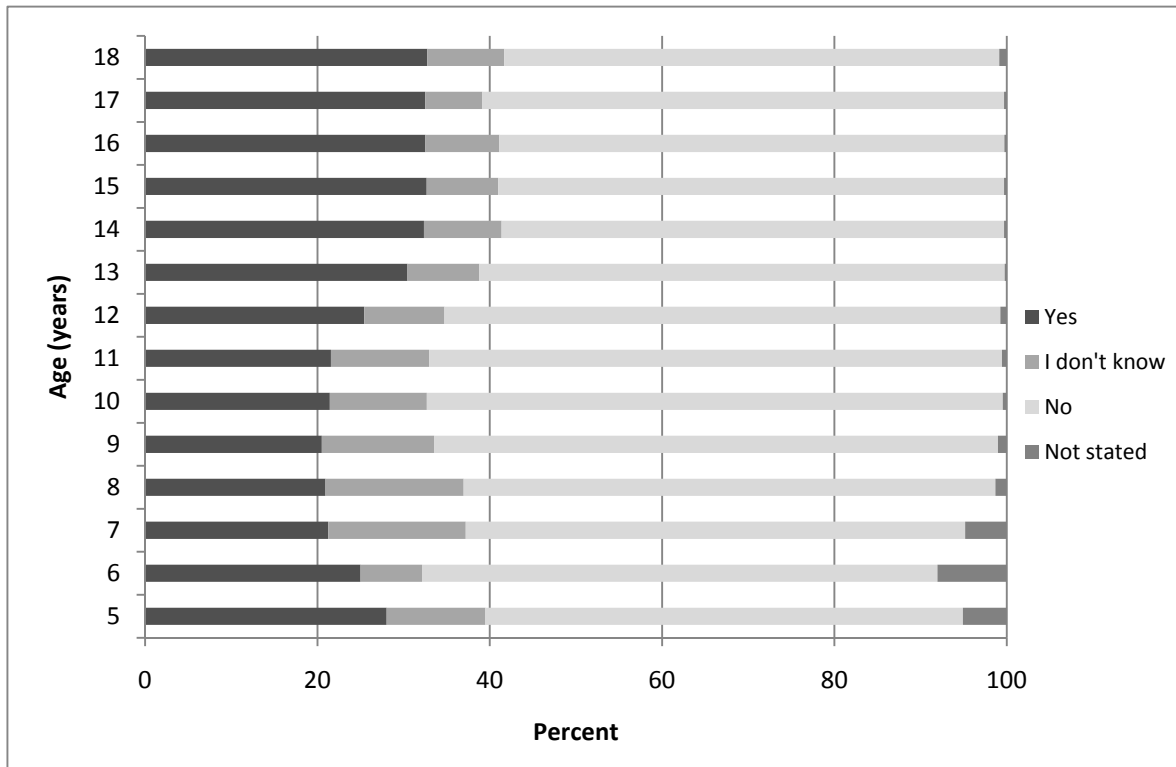
	Sex	Yes		No		I don't know		Not stated		Total #
		%	#	%	#	%	#	%	#	
5 Years	M	18.7	14	70.7	53	6.7	5	4.0	3	75
	F	24.4	20	58.5	48	11.0	9	6.1	5	82
6 Years	M	10.4	5	70.8	34	12.5	6	6.3	3	48
	F	15.6	10	75.0	48	6.3	4	3.1	2	64

7 Years	M	7.3	8	79.1	87	10.0	11	3.6	4	110
	F	2.1	2	80.4	78	15.5	15	2.1	2	97
8 Years	M	5.2	22	80.9	343	11.8	50	2.1	9	424
	F	2.6	13	88.0	434	8.3	41	1.0	5	493
9 Years	M	4.8	48	86.6	869	7.8	78	0.9	9	1004
	F	2.5	27	89.4	964	7.1	77	0.9	10	1078
10 Years	M	2.9	49	91.5	1557	5.1	87	0.5	8	1701
	F	2.2	40	93.2	1676	4.1	73	0.5	9	1798
11 Years	M	2.1	49	94.3	2174	2.6	61	0.9	21	2305
	F	1.4	36	96.2	2406	2.0	50	0.4	10	2502
12 Years	M	2.8	63	93.9	2103	2.4	54	0.8	19	2239
	F	1.3	30	96.3	2180	1.5	33	0.9	20	2263
13 Years	M	2.5	47	95.8	1811	1.5	28	0.2	4	1890
	F	1.7	42	97.1	2384	1.0	24	0.2	6	2456
14 Years	M	3.3	54	94.9	1529	1.4	22	0.4	7	1612
	F	1.3	25	97.7	1936	0.9	18	0.2	3	1982
15 Years	M	3.5	42	94.7	1128	1.6	19	0.2	2	1191
	F	1.5	20	97.4	1338	0.8	11	0.4	5	1374
16 Years	M	1.6	13	97.1	784	1.0	8	0.2	2	807
	F	0.9	9	98.1	979	0.6	6	0.4	4	998
17 Years	M	4.8	19	92.7	366	1.8	7	0.8	3	395
	F	1.4	8	97.7	555	0.7	4	0.2	1	568
18 Years	M	12.2	38	82.4	257	4.5	14	1.0	3	312
	F	16.2	42	76.8	199	5.8	15	1.2	3	259

Holiday plans

7.38 Participants in the survey were divided over disclosing holiday plans. 62.6 percent answered that they would not share holiday plans; 26.8 percent answered they would share holiday plans and 10.0 percent reported they were unsure.

Figure 7.7 Do you share your holiday plans online? (Age)



7.39 Of those that would not disclose their plans, the risk that this would pose was appreciated:

Because youif you tell them you are going on a hoilday and where you live, then when you are away they could go and rob your house (Female aged 11).

7.40 However, other comments received through the free text spaces indicated that young people felt this was ‘exciting news’ that they want to share with their friends:

often we put up things [like] “OMG guys, we’re totally going to Bali for the first week of the holidays!! SO excited!” (Female aged 17).

7.41 Other comments reveal that some young people believe that a risk online may be mitigated by factors in the physical world:

Even if I'm going on a holiday and post it, My house has pretty top notch security so I don't think I'd have to worry (Male aged 12).

7.42 Further, it is possible that the rate of divulging holiday plans is greater than these results indicate. It is possible that young people may unintentionally reveal their holiday plans by posting photos on social networking pages or other online networks which could indicate current or future travel plans, thereby exposing themselves to risks back at home.

Table 7.7 Do you share your holiday plans online?

		Yes		No		I don't know		Not stated		Total
Sex		%	#	%	#	%	#	%	#	#
5 Years	M	28.0	21	58.7	44	9.3	7	4.0	3	75
	F	28.0	23	52.4	43	13.4	11	6.1	5	82
6 Years	M	27.1	13	60.4	29	2.1	1	10.4	5	48
	F	23.4	15	59.4	38	10.9	7	6.3	4	64
7 Years	M	20.9	23	59.1	65	13.6	15	6.4	7	110
	F	21.6	21	56.7	55	18.6	18	3.1	3	97
8 Years	M	22.4	95	59.4	252	16.3	69	1.9	8	424
	F	19.7	97	63.7	314	15.8	78	0.8	4	493
9 Years	M	22.5	226	64.4	647	12.1	121	1.0	10	1004
	F	18.6	201	66.4	716	13.9	150	1.0	11	1078
10 Years	M	21.0	358	67.8	1154	10.6	181	0.5	8	1701
	F	21.8	392	65.9	1185	11.8	213	0.4	8	1798
11 Years	M	21.5	496	68.1	1569	9.7	223	0.7	17	2305
	F	21.6	541	65.0	1627	12.9	324	0.4	10	2502
12 Years	M	23.5	526	67.6	1513	8.1	182	0.8	18	2239
	F	27.4	619	61.5	1392	10.5	237	0.7	15	2263
13 Years	M	29.6	559	63.9	1207	6.3	120	0.2	6	1890
	F	31.1	764	58.8	1443	9.9	243	0.2	4	2456

14 Years	M	31.3	504	61.5	992	6.8	109	0.4	7	1612
	F	33.2	659	55.7	1104	10.8	215	0.2	4	1982
15 Years	M	32.9	392	60.5	720	6.5	78	0.1	1	1191
	F	32.5	446	57.2	786	9.8	135	0.5	7	1374
16 Years	M	34.6	279	59.1	477	6.2	50	0.1	1	807
	F	30.9	308	58.2	581	10.5	105	0.4	4	998
17 Years	M	33.4	132	59.2	234	6.8	27	0.5	2	395
	F	31.9	181	61.4	349	6.5	37	0.2	1	568
18 Years	M	34.0	106	55.8	174	9.6	30	0.6	2	312
	F	31.3	81	59.5	154	8.1	21	1.2	3	259

Passwords

- 7.43 The majority of participants would not disclose their passwords online. However, 5.7 percent stated they would disclose their passwords online, and a further 3.0 percent were unsure.
- 7.44 Possible reasons for divulging this information was provided by ACMA's *Click and Connect* report:

Young people and children claimed they would give someone (usually their best friend) their password in certain circumstances. This may be, for example, if they struggled to remember it, they were not allowed online and they wanted their friend to upload photos from the weekend, or they were no longer using their account and thought someone else might as well make use of it.¹⁸

18 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 49.

Figure 7.8 Do you share your email or passwords online? (Age)

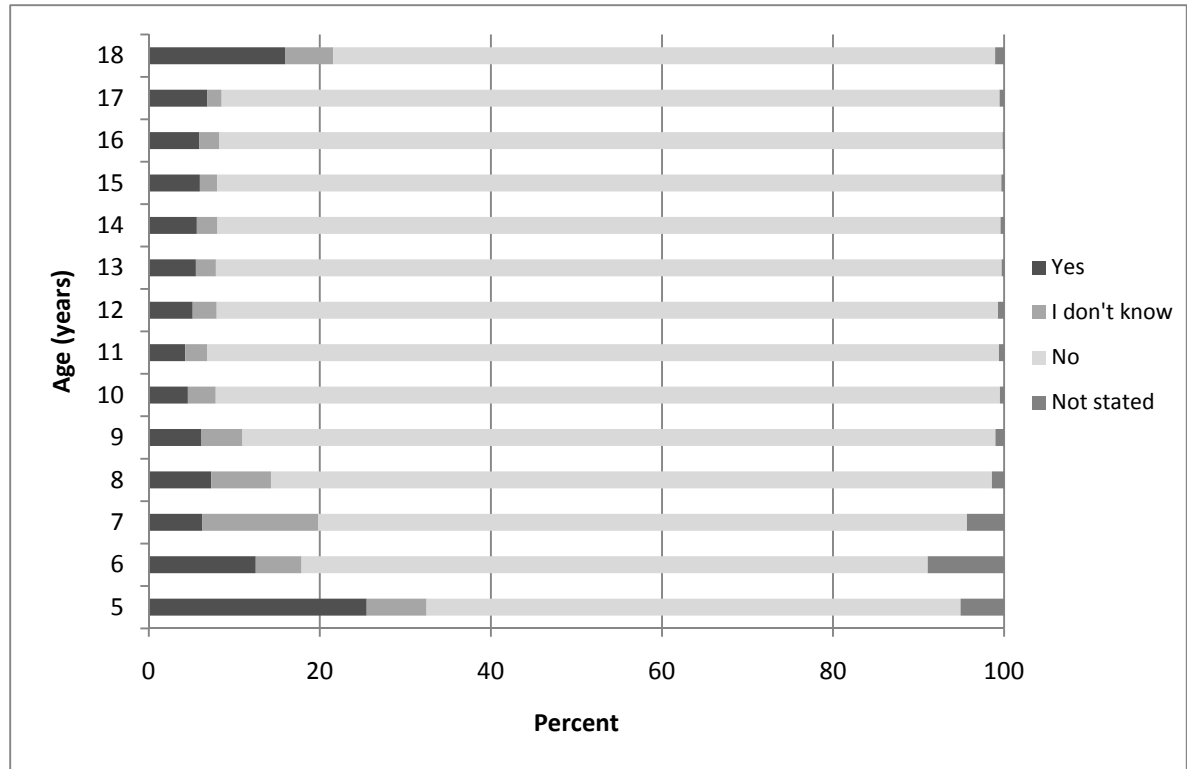


Table 7.8 Do you share your email and passwords online?

	Sex	Yes		No		I don't know		Not stated		Total
		%	#	%	#	%	#	%	#	#
5 Years	M	22.7	17	68.0	51	5.3	4	4.0	3	75
	F	28.0	23	57.3	47	8.5	7	6.1	5	82
6 Years	M	8.3	4	77.1	37	2.1	1	12.5	6	48
	F	15.6	10	70.3	45	7.8	5	6.3	4	64
7 Years	M	8.2	9	74.5	82	11.8	16	5.5	6	110
	F	4.1	4	77.3	75	15.5	15	3.1	3	97
8 Years	M	9.2	39	80.9	343	8.0	34	1.9	8	424
	F	5.7	28	87.2	430	6.1	30	1.0	5	493
9 Years	M	8.2	82	85.0	853	6.0	60	0.9	9	1004
	F	4.2	45	90.9	980	3.8	41	1.1	12	1078

10 Years	M	6.0	102	89.9	1530	3.6	62	0.4	7	1701
	F	3.2	58	93.3	1678	2.9	52	0.6	10	1798
11 Years	M	5.2	119	91.0	2098	3.1	71	0.7	17	2305
	F	3.4	86	94.0	2351	2.1	53	0.5	12	2502
12 Years	M	6.6	147	89.5	2005	3.2	71	0.7	16	2239
	F	3.7	84	93.2	2108	2.4	55	0.7	16	2263
13 Years	M	6.3	119	91.0	1719	2.4	46	0.3	6	1890
	F	4.9	120	92.6	2274	2.3	56	0.2	6	2456
14 Years	M	7.4	119	89.5	1443	2.4	38	0.7	12	1612
	F	4.2	83	93.2	1847	2.5	49	0.2	3	1982
15 Years	M	7.6	90	90.0	1072	2.2	26	0.3	3	1191
	F	4.6	63	93.2	1280	1.9	26	0.4	5	1374
16 Years	M	6.6	53	91.1	735	2.2	18	0.1	1	807
	F	5.3	53	92.0	918	2.5	25	0.2	2	998
17 Years	M	9.6	38	87.1	344	2.5	10	0.8	3	395
	F	4.9	28	93.7	532	1.1	6	0.4	2	568
18 Years	M	15.7	49	78.2	244	5.1	16	1.0	3	312
	F	16.2	42	76.4	198	6.2	16	1.2	3	259

Photos of others

- 7.45 Overall, the majority of participants thought the posting of photos without their permission was not appropriate. The data reflects earlier trends: there are peaks at both ends of the age spectrum, although there was no significant difference between male and female respondents.
- 7.46 The complexities of photo sharing and the types of considerations given by young people when deciding to post a photo is discussed below.

Figure 7.9 Do you post photos of others online? (Age)

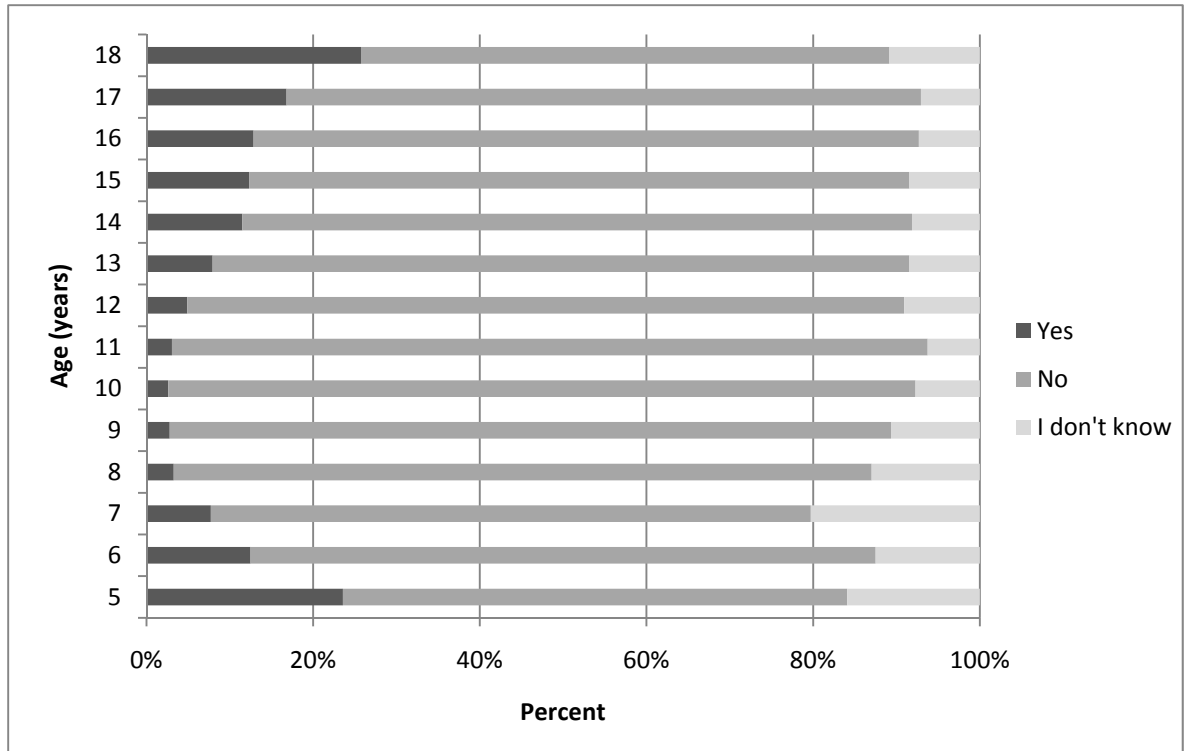


Table 7.9 Do you post photos of others online?

	Sex	Yes		No		I don't know		Not stated		Total #
		%	#	%	#	%	#	%	#	
5 Years	M	25.3	19	61.3	46	9.3	7	4.0	3	75
	F	22.0	18	59.8	49	12.2	10	6.1	5	82
6 Years	M	12.5	6	72.9	35	2.1	1	12.5	6	48
	F	12.5	8	76.6	49	4.7	3	6.3	4	64
7 Years	M	8.2	9	70.9	78	14.5	16	6.4	7	110
	F	7.2	7	73.2	71	15.5	15	4.1	4	97
8 Years	M	3.1	13	84.0	356	9.9	42	3.1	13	424
	F	3.4	17	83.6	412	10.5	52	2.4	12	493
9 Years	M	3.3	33	85.5	858	10.0	100	1.3	13	1004
	F	2.3	25	87.6	944	8.6	93	1.5	16	1078
10 Years	M	3.2	54	88.1	1498	7.1	121	1.6	28	1701
	F	2.1	38	91.2	1639	5.5	99	1.2	22	1798

11 Years	M	3.9	90	90.2	2078	4.6	107	1.3	30	2305
	F	2.3	57	91.2	2281	5.4	135	1.2	29	2502
12 Years	M	5.3	119	85.3	1910	7.7	173	1.7	37	2239
	F	4.5	102	86.7	1962	7.6	173	1.1	26	2263
13 Years	M	7.9	150	85.0	1606	6.3	120	0.7	14	1890
	F	7.9	195	82.6	2028	9.0	220	0.5	13	2456
14 Years	M	12.5	202	81.1	1307	5.6	91	0.7	12	1612
	F	10.7	212	79.7	1580	8.8	175	0.8	15	1982
15 Years	M	14.3	170	77.8	927	7.2	86	0.7	8	1191
	F	10.6	146	80.4	1105	8.2	112	0.8	11	1374
16 Years	M	15.0	121	78.6	634	6.1	49	0.4	3	807
	F	11.1	111	80.9	807	7.2	72	0.8	8	998
17 Years	M	19.7	78	72.2	285	6.8	27	1.3	5	395
	F	14.8	84	78.9	448	5.5	31	0.9	5	568
18 Years	M	25.6	80	64.7	202	8.3	26	1.3	4	312
	F	25.9	67	61.8	160	11.2	29	1.2	3	259

Conclusion

7.47 Divulging personal information forms part of an ‘identity-mosaic’ that young people wish to present to the public. *Click and Connect* found that

Purposeful divulgence of personal details [was] commonplace. Sometimes personal information was divulged without an understanding of the potential consequences of disclosure.¹⁹

7.48 Although young people share their information intentionally, it appears they are not sufficiently aware of the cumulative consequences. Although young people may assign a low level of risk to disclosing a single item of personal information, it appears that they do not evaluate the cumulative

¹⁹ Australian Communications and Media Authority, *Click & Connect: Young Australians’ Use of Online Social Media – Part 1*, 2009, p. 8.

risk of repeatedly doing so. This invites the question: are young people aware of online risks?

Are young people aware of online risks?

7.49 The extent to which young Australians are aware of online risks is not settled with many studies revealing a disconnect between the awareness of a risk existing, and identifying that their actions online may be exposing themselves to that very risk. Indeed, as Mr John Dalgleish commented:

Kids are going to engage in risk behaviours because of their developmental needs to, regardless of what intellectually they know.²⁰

7.50 ACMA's submission argued that young people have a high awareness of cybersafety risks, and identify activities such as 'posting personal information' as high risk behaviour.²¹ Yet, ACMA's research found that of those aged 16 to 17 years,

- 61 percent accept 'friend requests' from people they do not know offline; and
- 78 percent claim to have personal information such as a photograph of themselves on their social networking profile pages, compared to 48 percent of eight to nine year olds.²²

7.51 More broadly across the age spectrum, ACMA found that 17 percent of 12-17 year olds claim that one of their top three reasons for using social networking services is to 'make new friends'.²³

7.52 *Click and Connect* commented that children and young people tend not to identify their behaviour 'in terms of risk, or ascribe a degree to it'.²⁴ However, the *Are you safe?* survey received comments that indicate young people do appreciate risk and actively seek to mitigate those risks based on known options. For example, when asked about the content they share online, the following comments were submitted:

20 Mr John Dalgleish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS15.

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

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

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

24 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 8.

When I realised that literally almost everyone could see what I post on the internet. I then went through all my friends on facebook and realised that there were people I didn't even know, and that really freaked me out, knowing that they could see everything I posted up, as they were on my friends list (Female aged 15).

Many people feel that they are safe when on these [social networking sites] because they only communicate with their friends, however that does not always stop other people from viewing their account (Female aged 15).

I believe that the maximum security features are utilised on social networking, it is okay to use that social media (Male aged 16).

i think that you shouldn't express to much information especially if it is personal or the least bit personal because it is giving away your privacy to others that you don't know. this could be very dangerous (Female aged 11).

- 7.53 Young people who engage in high risk behaviour primarily do so because others do, and therefore their behaviour generally reflects those around them.²⁵ However, other motivations for high risk behaviour have been found to include fun, excitement, curiosity and boredom.²⁶
- 7.54 Yet comments were also made in the *Are you safe?* survey that indicate a possible connection between perceived anonymity and a lack of awareness of risk. One participant commented that 'no one can see me online - i am safe'.²⁷ Anonymity as a perceived safe-guard against risk, though relatively uncommon, is concerning and exposes these young people to extreme risks when online.
- 7.55 Equally dangerous, are the risks that arise when third parties are 'anonymous' or use identities that cannot be verified by others online. For example, when asked what content they share online, a female survey respondent commented:

I like to talk to other young people on the internet. I often use webcams, but unfortunately the other guy's webcam doesn't work. But I know I'm

25 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 49.

26 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 49.

27 Survey respondent, Male aged 14.

safe, because I have talked to these people on the internet before (Female aged 13).

7.56 This respondent exposes herself to predatory dangers discussed in Chapter 4.

7.57 Comments were also made that indicate young people are aware that a general risk exists, but are unaware of the specific dangers the unmitigated risk might bring. When asked about what content they post online, a female survey respondent commented:

can people get on here and look at at this privite stuff.because sometimes i get worried when i'm when i'm on the internet? (Female aged 8).

Risk and anonymity

7.58 Quantitative analysis of the results from the *Are you safe?* survey reveals trends of young people's perceptions of anonymity when online. Almost 29.2 percent of participants aged between five and ten years believe they are anonymous when online. This compares with 21.6 percent of participants aged 11 to 18 years. Perceptions of anonymity overall declined with the age of participants. Significantly, more females aged ten years or younger had greater perceptions of anonymity than their male counterparts, whilst this difference was reversed in the older age group (11 years and older).

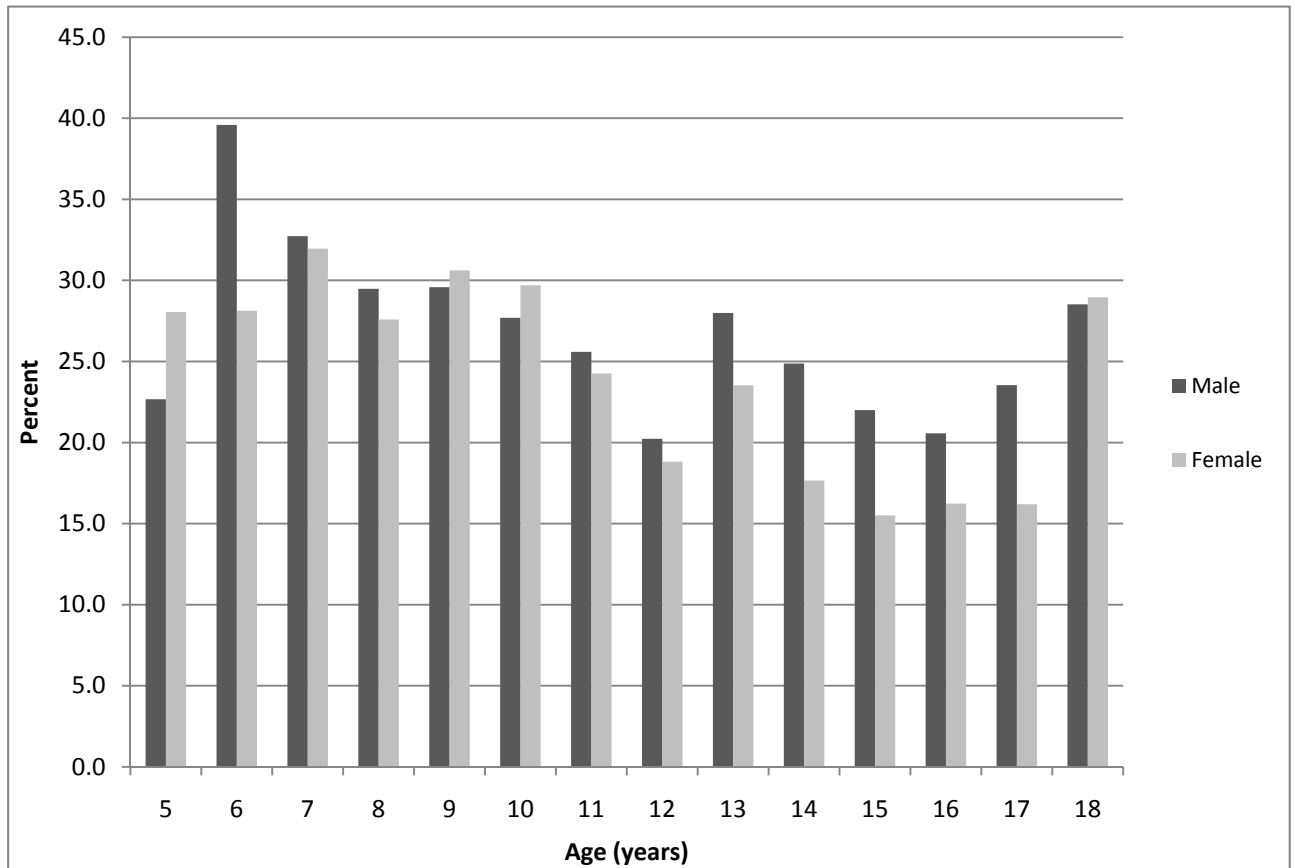
Figure 7.10 Do you think you are anonymous on line? (*Age and gender*)

Table 7.10 Do you think you are anonymous on line?

		Yes	No	Not stated
Sex		%	%	%
5 Years	M	22.7	52.0	25.3
	F	28.0	37.8	34.1
6 Years	M	39.6	39.6	20.8
	F	28.1	54.7	17.2
7 Years	M	32.7	58.2	9.1
	F	32.0	56.7	11.3
8 Years	M	29.5	51.2	19.3
	F	27.6	55.2	17.2
9 Years	M	29.6	48.3	22.1
	F	30.6	51.3	18.1
10 Years	M	27.7	50.0	22.3
	F	29.7	51.9	18.4
11 Years	M	25.6	51.5	22.9
	F	24.3	56.2	19.5
12 Years	M	20.2	55.8	23.9
	F	18.8	63.4	17.8
13 Years	M	28.0	72.0	0.0
	F	23.5	76.5	0.0
14 Years	M	24.9	75.1	0.0
	F	17.7	82.3	0.0
15 Years	M	22.0	78.0	0.0
	F	15.5	84.5	0.0
16 Years	M	20.6	79.4	0.0
	F	16.2	83.8	0.0
17 Years	M	23.5	76.5	0.0
	F	16.2	83.8	0.0
18 Years	M	28.5	71.5	0.0
	F	29.0	71.0	0.0

7.59 Although it cannot be presumed that those believing they are anonymous also believe ‘anonymity’ provides them sufficient protection from online dangers, it is concerning that this percentage of young people still believe they cannot be identified or physically located. This is despite extensive developments in education curricula and safety campaigns by police around the country.

7.60 Of concern are the rates of those that believe they are anonymous online and are not concerned about their safety. Figures 7.11a and 7.11b detail the Committee’s findings from its survey on this question.

Figure 7.11a Of those who believe they are anonymous online, do they feel safe? (Female)

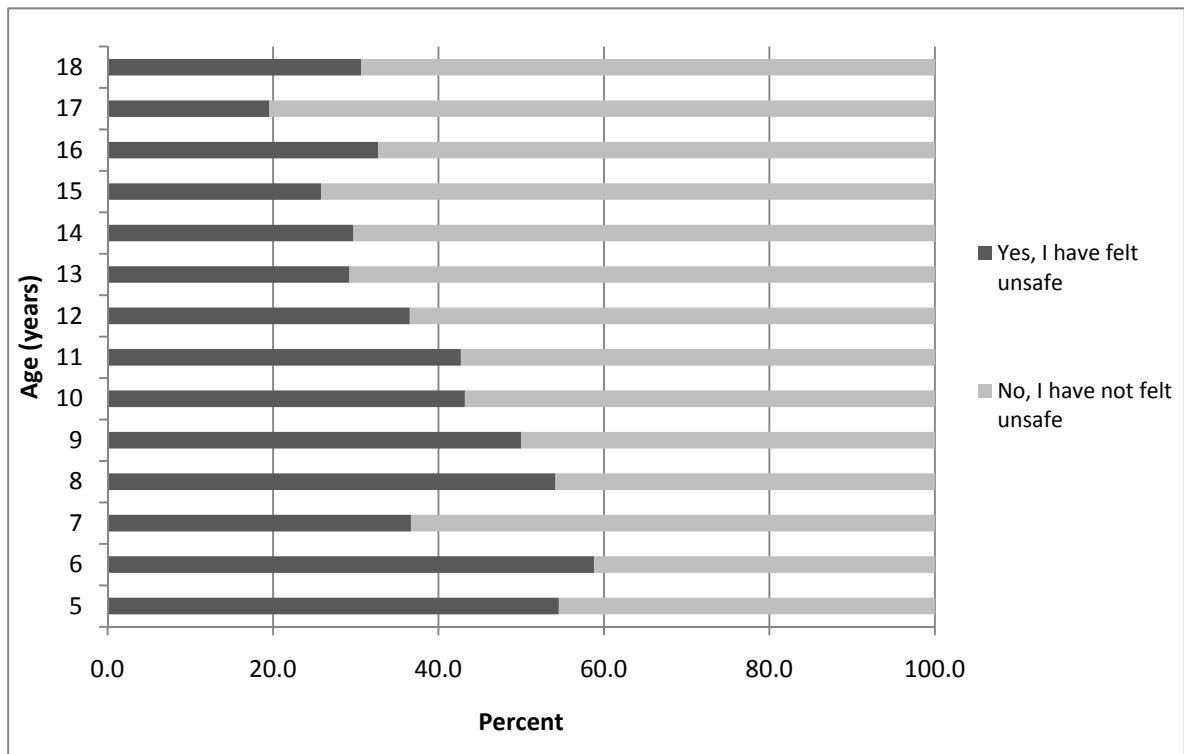
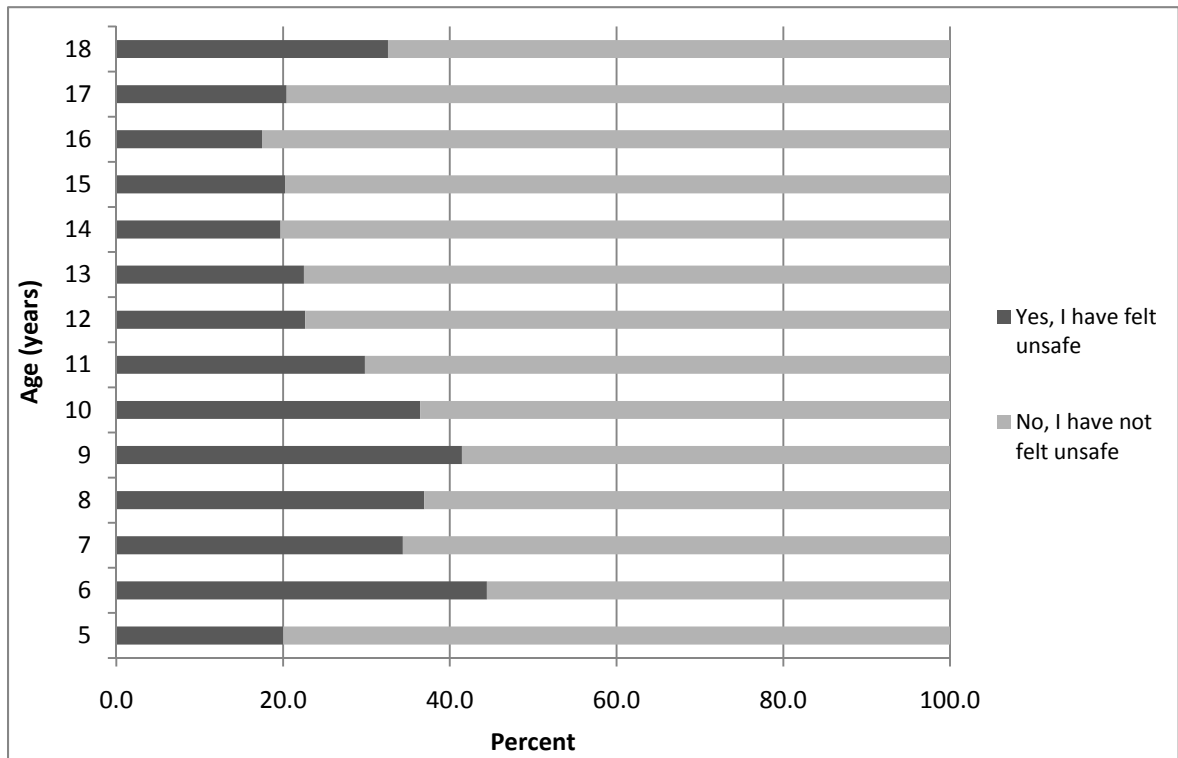


Figure 7.11b Of those who believe they are anonymous online, do they feel safe? (Male)



7.61 The graph below shows the general trend of those that believe they are anonymous when online and tracks their state of worry.

Figure 7.12a Of those who believe they are anonymous, what is their level of concern about online risks? (Aged 12 years and younger)

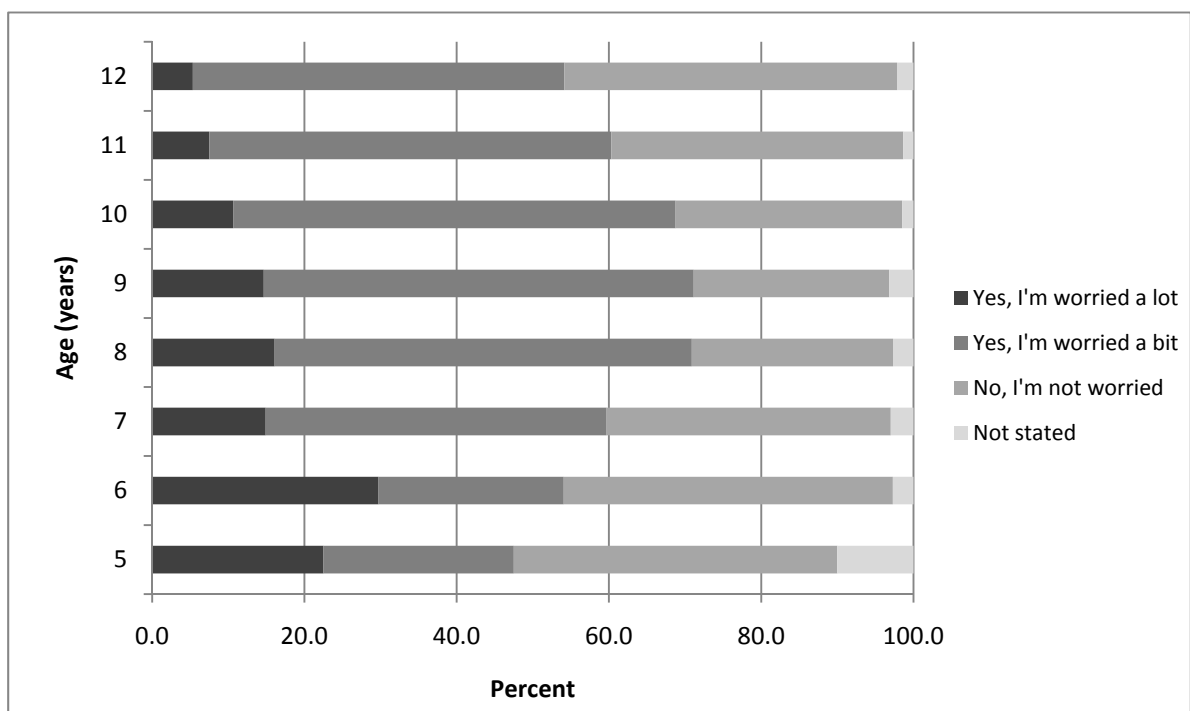
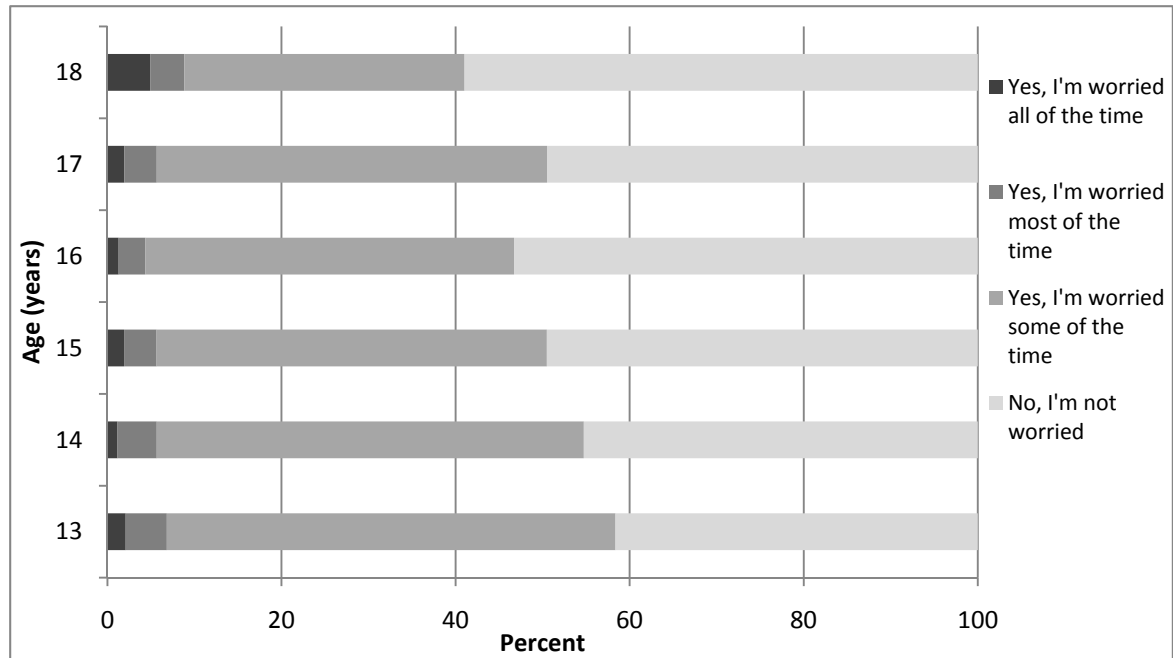


Figure 7.12b Of those who believe they are anonymous, what is their level of concern about online risks? (Aged 13 years and older)



7.62 Children aged between eight and 11 years of age show greater level of concern than those aged five to seven years of age. As might be expected, there is greater concern about safety among females aged 12 years and younger.

7.63 As children aged 12 years and older possibly become more aware of the opportunities for connecting online, they appear to become less concerned with their safety. This is similar to findings by ACMA reported above.

7.64 Although the rate of perceived anonymity appears to decline with age, their level of concern also decreases. If this group believe perceived anonymity is a sufficient mitigation of risk, these young people might be exposing themselves to high levels of risk. Further, these results might indicate that cyber-safety education is not having the desired impact and not reaching its main target audience sufficiently.

Ambivalence

7.65 Though the survey did not ask respondents specifically about their awareness of risk, comments were submitted through free text spaces that indicate a general awareness of a risk, but an ambivalence of the danger it poses. For example when asked about content posted online, the following comments were made:

Often we put up things that we know we shouldn't such as holiday date etc, but we do anyway (Female aged 17).

I know there's all this cyber awareness stuff going on, but its just that its never happened to me or anyone around me. I just don't see it as relevant. I mean, i know the basics, like not posting addresses etc, and i'm not an idiot, so i'm not that worried (Female aged 17).

I accept the fact that the internet can be dangerous, but I'm really complacent about safety issues. I don't really have anything to hide, which is why I'm not worried (Female aged 17).

i think I am pretty careful with what i tell people and put up on the internet. I don't think there's anything that people could use against me. some things may be awkward, but not unsafe (Female aged 14).

- 7.66 The diverse range of awareness and appreciation of risk is not surprising as varying results are also reflected in similar studies. A longitudinal survey of young Australians surveying their awareness and appreciation of risks online would be valuable when seeking to evaluate education programs. Further, examining the rates of perceived anonymity and the strategies that this group employ to safeguard their privacy would reveal the extent to which young people mitigate risks in ways that neither the Committee's survey nor other Australian studies have included.

How and why do young people decide what content to share online?

- 7.67 As in other areas of their lives, young people appear to want to take responsibility for their safety online and have a meaningful and valued input to creating a safer online environment. For example, through free text spaces, participants submitted the following comments in response to a question about information shared online:

Everyone has their own responsibility of what they post on the web, and at our age we should be wise enough to know our limits on what we can post and can't post (Female aged 14).

I believe that if you treat the internet with caution and with the awareness of the dangers of cyber activity, then it is possible to feel quite safe on the internet. I have certainly managed this, simply because I am

well aware of the risks and dangers associated with the internet and familiar in how best to avoid or deal with these in an appropriate manner (Female aged 17).

I know what i should and shouldn't be posting up on the internet. (i.e facebook and msn). I have been warned about the issues that could result, if any of my information were to fall in the wrong hands (Female aged 14).

- 7.68 As presented in the Introduction to this Report, the Committee believes that young people hold the key to their safety online. The remainder of this chapter examines how young people decide what information to share, and the resources they employ to achieve their understanding of safe online practices.
- 7.69 Before examining the tools used by young people, it is again important to note that young people are not a homogenous group. Differences in personality have an important effect on online activities, appreciation of risk and the strategies used to maintain a level of safety and security they each deem appropriate.

Personality, identity and appreciation of risk

- 7.70 It has been commented that young people choose to be open and expressive when online.²⁸ The option of protecting their privacy online can fall by the wayside in favour of wanting to stand out to others online.²⁹ This is most often sought through expressive profile pages, welcoming attention from the opposite sex, and making or accepting friend requests from those with similar interests.³⁰
- 7.71 *Click and Connect* categorised its teenage-participants into five distinct groups based on the level of risk which they expose themselves: active risk-takers; responsible risk-takers; the vulnerably influenced; specialist seekers; and claimed conformists. Although no direct comparisons can be drawn between the *Are you safe?* survey and ACMA's report, this model of segmenting is particularly helpful when seeking to ascertain how young

28 Australian Communications and Media Authority, 2009, *Click & Connect: Young Australians' Use of Online Social Media – Part 1*, p. 5.

29 Australian Communications and Media Authority, 2009, *Click & Connect: Young Australians' Use of Online Social Media – Part 1*, p. 5.

30 Australian Communications and Media Authority, 2009, *Click & Connect: Young Australians' Use of Online Social Media – Part 1*, p. 5.

people decide what content to post online, and how they mitigate known risks.

- 7.72 All types of risk takers identified by ACMA's *Click and Connect* report employ a variety of risk management strategies:
- abiding by the rules or advice given to them;
 - using common sense;
 - learning from experience; and
 - resilience.³¹
- 7.73 The Committee's consultations with young people revealed similar strategies, and its findings particularly point to
- critical thinking and rational deduction;
 - informal learning through experience, by examples or through peer-based exchanges; and
 - formal learning through schools, parents and official programs.
- 7.74 Young people also seek to limit certain online networks so that they can communicate and divulge information to those they trust online, but maintain their privacy from the general online public.
- 7.75 Lastly, young people are also concerned by 'digital footprints' and these concerns can inform their decisions to post information and content online. These factors are discussed below.

Critical thinking and rational deduction

- 7.76 Young people can engage a process of critical thinking and rational deduction when assessing online risks, authenticity of content and its sources. One participant noted that real-life networks inform their decisions when asked about the information they share online:

I probably won't add people as a friend unless we have lots of mutual friends (Female aged 14).

31 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 9.

- 7.77 Additionally, as the following dialogue demonstrates, young people assess the authenticity of their communications with their peers when online:

CHAIR- ...How do you determine whether or not you should be clicking on a link [that appears to be sent to you by 'friends']? [Georgia] said it did not sound like [her] friends, so was that a gut instinct?

Georgia-Yes. It was the way it used all the abbreviations-like the way they spelled 'like' was 'lyk' - and those sorts of things. My friends and I only use full words [when communicating online].

CHAIR-So you can look at the language that it has used. Okay. Would anyone else like to comment on that?

...

Jacqui-You have 'friends' on Facebook, but you do not communicate with them over Facebook. You get the people that you do not actually talk to but you know. Those types of people sending [links to virus' or spam messages] to you. It is like, 'You never talk to me; why are you sending me this?' Or it will be [sent by] more than one person. That is another way you can figure out not to click on it.³²

- 7.78 Submitted in the final free-text space, the following comment demonstrates the use of critical thinking by young people:

If I am asked a question in an online forum, I always think "who is going to read this information - who has access to it". Online safety is all about assessing what you are about to do critically - but that's the important point: it must be before you post or else that information is most likely going to exist forever (Male aged 18).

Informal learning

- 7.79 From a young age, children apply common sense and begin to learn from experiences they encounter themselves, through examples by others and as reported in the media. These behaviours or strategies are acquired as children become more resilient and adept at managing their online experiences.³³ These avenues of informal learning are explored below.

32 High School Forum, *Transcript of Evidence*, 20 April 2011, p. CS8.

33 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 9.

Learning from experience

- 7.80 Often, young people learn to modify behaviour after encountering some unsought experiences online. Moreover, learning from experience and developing resilience is 'usually a phenomenon of increasing age and exposure to being online'.³⁴ Exposure over time to unsought experiences can result in an individual learning how best to handle such situations.³⁵
- 7.81 Indeed, the way children and teens begin to manage risk is often by navigating challenging experiences. In an ACMA study, participants gave examples of making their profile pages private after receiving unwanted comments, not using a webcam with strangers after an incident of indecent exposure, or avoiding downloading suspect files or opening pop-ups after they have had a virus.³⁶
- 7.82 When asked where they learnt about cyber-safety, similar examples emerged through the free-text spaces in the *Are you safe?* survey:

on msn, some girl kept on trying to make me her friend on the internet and she tried it for about a month until I found a way to stop it and I tried to block her but somehow she kept on talking to me and I felt very scared that she wasnt who she said she was and she wasnt the age she posted either... I think msn should make it less easy for random people to start talking to you (Female aged 13).

Personal experience and common sense. I grew up surrounded by technology and learnt on my own (Male aged 16).

- 7.83 Experimenting with risk-averse behaviours were found in the ACMA qualitative study to have an effect on the likelihood of repeat activity:

Engaging in high risk behaviour can have varying levels of impact... Some behaviours have consequences which would deter future repetition. In others, the consequences may not be so severe, and therefore these behaviours may be repeated.³⁷

34 Australian Communications and Media Authority, 2009, *Click & Connect: Young Australians' Use of Online Social Media – Part 1*, p. 53.

35 Australian Communications and Media Authority, 2009, *Click & Connect: Young Australians' Use of Online Social Media – Part 1*, p. 9.

36 Australian Communications and Media Authority, 2009, *Click & Connect: Young Australians' Use of Online Social Media – Part 1*, p. 53.

37 Australian Communications and Media Authority, 2009, *Click & Connect: Young Australians' Use of Online Social Media – Part 1*, p. 49.

Sibling- and peer-based learning

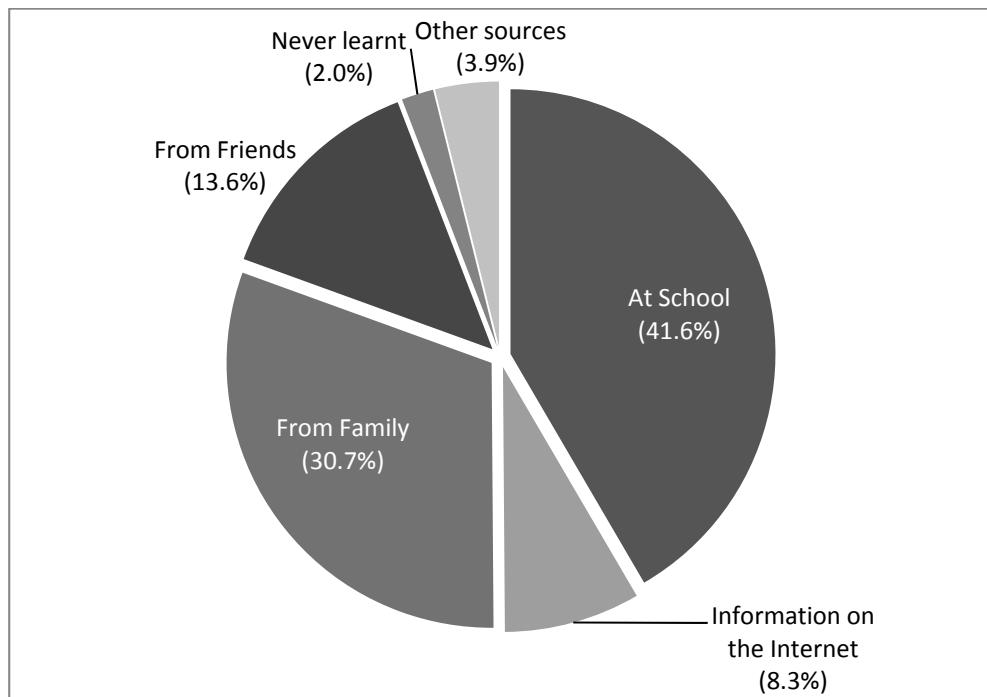
- 7.84 Learning from the experiences of others is an important tool in deciding what content to post online. Most often, young people will learn from each other (their peers) or from their siblings. For example, one respondent explained how they learnt to be safe online:

i sort of learnt by myself, taking examples from others who did the wrong thing, helped me to understand how far i should or should not go (Female aged 15).

just as i grew up, i have older siblings who told me everything about it (Female aged 15).

- 7.85 The role of family and friends in the decision by young people to post information online should not be undervalued. Based on analysis of the results from the Committee's survey, 30.7 percent of young people surveyed identified they primarily learnt about cyber-safety through their family, and an additional 13.6 percent identified that their friends were their primary source of guidance.

Figure 7.13 Where did you learn about cyber-safety?



7.86 This finding highlights the need for these groups to be the carriers of thorough and detailed information, as young people are less likely to reach out to formal portals for assistance.

7.87 ACMA found that older siblings influence risk-taking behaviour by setting the precedent:

[Older siblings] can influence their younger counterparts' behaviour in a number of ways, through allowing them to watch what they do from an early age, and thus advancing their younger sibling's internet capability and social awareness. They often teach them how to use the computer and internet, setting up accounts for younger siblings and setting the level of trust between parent and child. This level of trust often then applies to all younger siblings in the family. For example, if the eldest is seen to demonstrate responsible behaviour online, parents are more likely to be trusting of all their children, however, if they are irresponsible then parents are likely to monitor all of their children more closely.³⁸

7.88 Similar to sibling-based learning, peers influence risk-taking behaviour by setting the social standard:

Trends set by peers include determining what profiles should include, seeking out the next best violent game, determining which online website/forum is best for interacting, and finding and forwarding the next most explicit/shocking material possible.³⁹

7.89 The role of family is further explored in Chapter 10 of this Report.

Common sense

7.90 A considerable number of respondents in the *Are you safe?* survey used the free-text spaces throughout the survey to indicate that deciding what content to post or information to search was largely an exercise in 'common sense', 'common knowledge' or 'general knowledge'. Some of these comments are included below:

Internet personal safety is, in a lot of ways, just a logical extension of
--

38 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 51.

39 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 51.

personal safety in reality. If you do not want someone to phone you, you do not give them your phone number. If you do not want someone to be able to find you or address you directly, you do not give them your name. My initial sense of personal safety in reality can almost definitely be attributed to my family, but as far as on the internet goes, it's COMMON SENSE (Male aged 17).

My common sense, which forms a part of the majority of teenagers, which is why most of them are so annoyed about all of this 'cyber education.' None of it is new, different, or useful. Horror stories you hear about in regards to cyber accidents are just that....accidents. And I understand you are trying to prevent that... but repeating common knowledge at the cost of thousands of dollars is not going to change that (Female aged 13).

You just have to use your common-sense. You wouldn't tell a stranger your personal information or send them raunchy photos. The internet is full of strangers, so just keep personal info to yourself or you'll end up in trouble (Female aged 16).

- 7.91 The identification by young people that they employ 'common sense' is indicative that they are absorbing a level of cyber-safe practices that they have received from a young age, and therefore do not identify that these skills are anything out of the ordinary.

Learning by examples reported in media or featured in television shows

- 7.92 Another source that is impacting on the internal decision-making processes of young Australians includes learning through examples reported in the media or cases that might be featured in television shows.
- 7.93 More specifically, comments made by respondents in the *Are you safe?* survey referenced news stories. For example, a female aged 13 commented that in addition to other sources she learnt about cyber-safety through 'the bad publicity on the media about people getting stalked and bullied and harassed on the internet'.⁴⁰
- 7.94 Similarly, young people are becoming more aware of online dangers and learning methods of managing online risks through popular television programs or movies that feature cyber-safety or cyber-bullying in their storylines. Notably, a 17-year old male survey respondent commented that he learnt about cyber-safety through media:

40 Survey respondent, Female aged 15.

on television programs or movies - i knew how to rotect your facebook page or how stupid it is to put info about yourself up on the interent for strangers to see (Male aged 17).

- 7.95 However, a few respondents were eager to comment that media reporting of cyber-bullying and cyber-safety more generally has led both parents and schools to overstate threats online. In response to the same question, the following comments were made:

Reports on Channel 7 news and A current affair etc has meant taht my parents are super concerned about my safety online. Sometimes they want to sit beside me whilst they actually watch my ever click! Sure bad thigns can happen online, but i believe that we've had so much education at school i can know what to click and when to post (Male aged 16).

I learnt about the actual dangers of what can happen if you disclose too much info online through the news. We learnt about cyber-safety at school, but not so mcuh on [how] little information is needed for a stranger to track you down (Female aged 14).

Formal learning

- 7.96 The results of the *Are you safe?* survey mirror that of other studies: a higher number of young people learn cyber-safety through formal channels.

- 7.97 Most young people 'claim to follow the 'basic' safety advice there have been given, yet it was also noted that young people find that exceptions to these rules are quite common.⁴¹ *Click and Connect* commented that:

Abiding by the rules and applying commonsense are relatively easy strategies which tend to be used by the eight to 10-year-olds. Methods this age group might use to mitigate risk would be giving only parents their password, scanning downloadable files, and reporting someone who is behaving inappropriately or offensive material they come across online.⁴²

- 7.98 Further, young people appear to use the general rules of personal safety to ensure their digital self is also protected. The following comments were

41 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 53.

42 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 9.

submitted through free text spaces in response to two different questions in the survey:

Having a sense of an idea how to play safe helps. If you follow what most parents tell their kids and 'Don't talk to stranger' then you should feel safe most of the time. On the internet you can basically just use a pseudonym or nickname that has little or no link to yourself to avoid these types of situations and then abandon it if things get too scary (Male aged 16).

The internet is a public forum so anything that you wouldn't tell random people on the street shouldn't be put up on it (Female aged 15).

- 7.99 There will be more detailed discussion of the role of formal education and discussions with family in Chapters 8 and 10.

Limiting online networks

- 7.100 The Committee's consultations also found that although young people frequently post personal information, they limit the network that is able to view this information. The forums and the context in which material appears, features heavily in the decision-making process of whether the information should be disclosed or remain offline.
- 7.101 Young people commonly enable privacy settings so that their social networking pages, and personal information contained therein, are not available for broad public viewing. Young people will disclose more online if they believe they have limited their online network to a group of people with whom they feel comfortable sharing that information.
- 7.102 In its submission, ACMA commented that its research had shown that the use of privacy settings on profile pages appeared to be greater amongst the older age groups.⁴³ The strategies of limiting online networks as a method of protecting their personal information further expands the analysis in Chapter 5 on privacy and identity theft.
- 7.103 The following comments were made in the *Are you safe?* survey in response to questions about information sharing online:

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

It is important to not display your pages to the public. By doing this you are risking not only your safety but your family and friends. Never take the powers of the internet lightly (Female aged 13).

As long as pictures and emails are only able to be viewed by the people you know, and the people that would most likely already have your email, then it is okay. The same can be said for schools. If the school that I am attending is only able to be seen by the people who attend my school, or otherwise know that I attend it, then there is little or no issue (Female aged 15).

I believe you should only post in places where the audience can be limited to just your friends, e.g. social networking. I also believe that if you are posting in public places, only post information if you would be happy to have the same information in a newspaper, it's a good way of gauging whether to post information or not (Male aged 18).

We go on Facebook but some of us, including me, set out profiles to friends only so that random strangers can't see our profiles! When we post something onto Facebook, it doesn't go out for the whole world to see! Please understand this! (Female aged 13).

Sites that i might have published photos of my friends or my birthday are completely excluded to the general public, you have to be my friend to see those things. I have chosen who can see those things and if there is somebody i don't know i don't make the silly mistake of accepting their request (Female aged 15).

i think if you have a site that you can communicate with your friends your page should be on private, so only your friends can see so no one who u dont know can see information about you or anyone (Female aged 10).

i think if you have good privacy settings and dont talk or add people you dont know then facebook, msn and myspace are fine (Female aged 12).

7.104 *Click and Connect* made some general comments about the use of privacy settings to limit the network of users online who can view and access the personal information of others. It commented that:

Privacy controls are important in providing young people with the choice to protect themselves. While most young people understand that internet safety is primarily their responsibility, many believe web providers have a duty to allow website users to be safe, and give the choice not to disclose personal information. ...

The privacy controls that were valued included the choice of either a public or private webpage, the choice to hide their age, ... and the choice to show either their real name or an alias.⁴⁴

Disclosing information to expand networks

- 7.105 Despite many young people limiting their social networks online in order to enhance their privacy, some respondents commented that they specifically disclose their information online so that they expand their social networks. For example the following comments were made by respondents to explain their answers regarding information sharing:

sometimes putting information like the school you attend could be dangerous, but its something a lot of people do so that they can identify their peers on facebook (Female aged 14).

Putting information on facebook is quite essential for me to contact past friends and hook up with people who have similar interests (Male aged 17).

- 7.106 Sharing such information appears to increase as young people reach their mid- to late-teen years.

- 7.107 Though sharing information of this kind can expose users to significant risks online, some young people who participated in the survey wanted to demonstrate that they saw this as a risk, but believed in the importance of trusting others online. For example, respondent to questions on what information they share online, one respondent commented:

My parents say that i should put up the name of my school on my social networking pages or bcome friends with people i don't know in real life. But i would be missing out on too many other good things on the net - it places too much emphaisis on the dangers. We need to stike a better balance - know the risks, but if there are opportunites that would outweigh the risk, i will always pursue them (Male aged 16).

44 Australian Communications and Media Authority, *Click & Connect: Young Australians' Use of Online Social Media - Part 1*, 2009, p. 54.

Digital footprints

- 7.108 The decision of some young people to post content is also influenced by concerns about their digital footprints. More specifically, young people are aware of the risks brought by the longevity of uploaded content, as well as the transfer of ownership to the site administrators, and the fact that information can never be permanently deleted.

Longevity of the life of posted content

- 7.109 The Committee's consultations with young people revealed that young people hold concerns about the lasting effect that their online activities might have in the future.
- 7.110 Respondents made the following comments in response to questions about personal content posted online.

... if you were to put a photo up on the internet, you have to consider the fact that people in the workforce will also have access to these photos, so if you want to get your dream job make sure you only put photos you are willing for your future employers to see (Female aged 15).

[Posting] anything online could be dangerous. Putting things online about yourself or others is not safe no matter how safe you think it is and when you delete something it is always going to be online in a way (Female aged 12).

I know that any information that you put up on the web is there, and staying there. What I mean by this is that every time you write something, you are leaving an 'electronic footprint'. This may show users what websites you have been on, etc (Female aged 12).

- 7.111 Similarly, the High School Forum discussed topic of digital footprints with some insights:

CHAIR- Fast forward 20 or maybe 30 years... think of the worst thing you have ever said, put on there or posted--or that someone has posted about you. How are you going to explain it to your 15-year-old?

Georgia-I have had this discussion with my mum. She tells me how she-I do not think she used the word 'cheated' but how she cheated in her-

CHAIR-You do not have to go into too much detail-just how she did something and how she felt about it.

Georgia-It was really nice to see that she kind of had a human side.

CHAIR-Okay; so that would be your human side, to your teenager.

Georgia-Yes. It was just nice to see that I could relate to her in other forms-like, knowing that she had done some wrong things and that she was not perfect.

CHAIR-And whatever the worst thing was that you had ever done, you would not mind your 15-year-old doing that either? Because they will be coming back to you and saying: 'Well, Mum, you did it.'

Georgia-As long as my 15-year-old was not getting their head stomped in or making someone else feel belittled, I would not have a problem with it.

CHAIR---Okay. Someone else? ...

Jacquie--I have a few points on that. The first is: when you get to there, in 20 or 30 years time, like Georgia said, you will be able to relate. I am not saying that your child is going to say, 'Oh, but you did it.' You have learned. But you can relate. So if it happens you can say: 'I understand your position. I know where you have been. This is what I think is best, not from a mother's point of view but from what I learnt at that age.'

Samantha-I think it is a very hard question to answer when you think of how much we have evolved with technology in the last 15 years and how things have changed - like, it is not just bullying anymore, it is cyberbullying. Things have progressed. It is going to be completely different.

CHAIR-That was just thrown in there to get you thinking about what you are actually putting on there. You look down the track and think, 'One day it might be an employer, or a parent or a child.'

Matt-I think that in the next 20 or 30 years the technology is going to change. Like, now we have iPads and stuff like that; in the next 20 years we could be using some different gadget.

CHAIR.-So this would be so outdated you would not even see it?

Matt-Yes. We would not see it.⁴⁵

- 7.112 Other Australian studies also account young people's concerns in this area. The study by the University of Technology Sydney of online and offline identities refers to one participant who commented that:

I know I can do things online, because I'm a number, so I will sign petitions online, forward emails, stuff like that, but as soon as I can be photographed, identified, that's where I draw the line... if [activities where I can be identified] jeopardise my future, I don't know how valuable they are right now.⁴⁶

- 7.113 The same participant acknowledged that in the future, those online reminders of a self existing in another time and space remain positioned as undeniable 'fact', searchable and removed from the context in which they were first expressed. Thoughtfully, the study noted above commented that:

the persistence of these traces of experimentation online creates a dilemma for young people wishing to experiment with ideas and actions, because they last long after the flesh-and-blood person has disowned them.⁴⁷

Ownership of posted content

- 7.114 Concerns were also expressed about the ownership of posted content. In the Committee's High School Forum, a participant commented:

When you upload photos onto Facebook, Facebook technically owns them. Even if you ask them to remove it, it is permanently on the internet and can be brought back at any time depending on the people who own Facebook. I think there needs to be education or warnings put into place so kids understand what they are doing before they click a button.⁴⁸

- 7.115 Another participant commented that the Internet's informality allows content to be freely adopted or stolen by others:

I take photos as a major hobby, so I am always clicking away. People always say, 'Upload them,' so I do. If they want me to take

45 High School Forum, *Transcript of Evidence*, 20 April 2011, pp. CS25-26.

46 Yerbury, H. 2010, 'Who to be? Generations X and Y in civil society online', *Youth Studies Australia*, vol. 29, no. 2, p. 28.

47 Yerbury, H. 2010, 'Who to be? Generations X and Y in civil society online', *Youth Studies Australia*, vol. 29, no. 2, p. 29.

48 Amanda, High School Forum participant, *Transcript of Evidence*, 20 April 2011, p. CS18.

them down, even though it is a really good photo because I sift through tons of photos, I take it down but I am reluctant. I have other friends who are majorly into photography but I can steal their images too because I really like an image'.⁴⁹

- 7.116 A respondent in the *Are you safe?* survey also raised concerns about his private information 'owned' by social networking sites who may then sell that information to third parties. The following comment was submitted in response to questions about sharing personal information online:

It is rather confronting to think that companies such as Facebook and Acxiom are selling our private information to marketers (Male aged 16).

Inability to delete accounts/information posted etc

- 7.117 Adjacent to the concern of ownership is the concern that posted content, including personal information and opinions expressed, cannot be deleted or permanently removed from the online environment.
- 7.118 Two notable comments were expressed in the survey's free-text spaces by respondents wishing to explain the why they have felt unsafe online:

I signed up in random website (such as Facebook) and then I wanted to delete my account because I didn't feel safe with it but then it didn't delete it but just locking account. (I wanted to delete the account permanently but it won't) Then I felt unsafe about websites (Female aged 15).

It feels like every bit of information you put up on the net, someone else is saving it for their own personal use. And I feel like everything I put up on the internet, even if I delete it, it will never be really deleted (Female aged 14).

Targeted advertising as a result of interests and past activities

- 7.119 Young Australians also appear to be concerned by perceptions of becoming the targets of advertising campaigns. The following dialogue demonstrates these concerns:

Ebru-Another thing on Facebook is that if you talk about certain things-if you like soccer or fashion-an advertisement will come up for things that you are interested in. You click on it and see what it

49 Victoria, High School Forum participant, *Transcript of Evidence*, 20 April 2011, p. CS18.

is about. Obviously, Facebook is becoming worldwide with businesses. Businesses are starting to use it-real estate, restaurants and everything-so kids are seeing more advertising for these kinds of things. I remember when Facebook first became popular that if you swore on Facebook you would get banned for a day or a couple of hours. But I think the rules of Facebook have changed since it first started becoming popular.

CHAIR-Do you think it is the rules or do you think it has become so big that it is too difficult to control?

Ebru-Yes, probably the people of Facebook cannot control what every single adolescent says. People put pictures up on Facebook and they just do not care about it anymore because it is so popular.

Senator BARNETT-So you think that Facebook are either selling or transferring your likes and information about you for commercial benefit or for other reasons? That is what you are saying?

Ebru-Yes.⁵⁰

- 7.120 During the Forum, approximately 30 percent of participants indicated they would rather not be targeted by advertisers, and were concerned about such campaigns.⁵¹

When fun isn't fun anymore: examining the complexities of photo sharing

- 7.121 Photo sharing draws upon many of the issues discussed above and illustrates complexities and nuances of the online environment. This topic is frequently raised in broader public discussion. Media outlets have recently given significant attention to the circulation of photos of women among groups of men online, as well as the role of law enforcement agencies to pursue those that *receive* photos of others.
- 7.122 In the context of young people deciding to post content online, the example of photo sharing demonstrates the risks young people expose themselves to as well as the strategies they employ to reduce risk. It also raises an important discussion of how posting photos of others can create additional concerns of permission, ownership and the ability to control

50 High School Forum, *Transcript of Evidence*, 20 April 2011, p. CS14.

51 High School Forum, *Transcript of Evidence*, 20 April 2011, p. CS14.

one's personal information. Further, posting photos can increase strain on existing relationships when requests are made to remove photos.

- 7.123 The Committee received many comments from survey participants when asked whether they post photos of others online. Survey respondents commented on these general complexities:

Photos, I believe are a contentious issue because people freely put up photos on social networking sites like Facebook without permission and pretty much assume that if you are in a photo you give permission for a large amount of people to see you (Male aged 16).

I havnt been on Facebook for about 3 months but every time when i logged on their would be someone fighting with someone on someones wall or status- stupid photos put up on purpose. for example if a girl was a party and might of been sitting in a position and a camera just so happened to take an awkward shot of her underwear or something- this event is totally innocent but the person who uploads this photo onto the internet is an idiot- this happens a lot. photos which at the time are accidental or the subject might not even known are being taken are being put up on the internet for everyone to see. And what girl wants photos of their underwear all over the internet. this example happens allllloooooottt! (Female aged 16).

- 7.124 The Committee's High School Forum also discussed this issue, with one participant noting the absence of requiring formal permission before posting photos of others in a public forum:

It is interesting that, when a school takes a photo of you, it has to have permission and it is the same everywhere. But a friend can put it up and you can ask them to take it down, but they do not have to because it is on their profile. So even if you do not like that photo and you want them to take it down, they can say no.⁵²

- 7.125 These complexities have led some young people to give specific consideration to the consequences of sharing photos of themselves and others online. Comments made by respondents give examples:

For posting pictures of others without their permission. although it would probably be most appropriate to always get their permission, my rule is usually....if its in some ways inappropriate or might hurt or

52 Samantha, High School Forum participant, *Transcript of Evidence* 20 April 2011, p. CS17.

embarrass this person, i will ask them first, otherwise it shouldnt be an issue and i put it up anyway. i take it down if theyve seen it and then ask me to because they are not comfortable with it (Female aged 15).

I only add photos of others without their permission if they already have lots of photos of themself already, they don't care or if is not an innapropriate picture (Female aged 14).

I think it's ok to put some photos up on the internet if you have the person's permission and also if your willing to have that picture stay on the internet forever (Female aged 14).

In terms of posting photos of others without permission, we often post photos of our friends without their permission as a joke and it is well recieved and comical among our group of friends. However it is never at the expense of another persons feelings, if we feel they will be upset over the photo then we dont post it (Female aged 16).

Requesting the removal of photos

7.126 Throughout the Committee's consultations, comments were made by young Australian's that indicate the pathways they seek to have photos of themselves removed. Generally, young people appear to discuss the matter first with their friend/s who posted the photo, and then send a formal request to the site administrator if progress is not made at the first stage:

Imogen was saying before that if you do not like a photo, talk to the person and they may remove it. But if the situation is not resolved within a few days then... you can report it.⁵³

7.127 Both stages are discussed below.

Approaching friends

7.128 The Committee's High School Forum discussed the experiences of young people when they requested their friends to remove a photo online:

CHAIR - A photograph has gone up and you do not like it. You have asked your friend to take it down. I want to know what you did. Who can we start with?

...

53 Madeline, High School Forum participant, *Transcript of Evidence*, 20 April 2011, p. CS16.

Lauren-There was a picture of me and this person ... from my school. Anyway, I was like to my friend, 'Can you take it down?' and she just did it straightaway, inboxed it. She took it down. ... I explained to her why I wanted it down.

CHAIR--Good. So you gave the information back how it made you feel for whatever reason.

Lauren-Yes.

...

Jacqui-It is more or less: if you want pictures taken down, make sure you do it for other people. Don't be a hypocrite. Don't be expect people to do things for you and not let do it for them... You should take on both people's perspectives. You want it off. They want theirs off even though you like it, so do the same for them.⁵⁴

- 7.129 In response to a question on whether approaching friends was a successful strategy, an extremely low percentage of participants in the High School Forum indicated by a show of hands that the issue was satisfactorily resolved.⁵⁵ Amy, a participant, commented that she compromised and sought an informal resolution independently:

They did not take the photo down, and I said, 'No, it's a really bad photo. I don't like it.' If they did not take it down, I just had to remove the tag so the photo would not come up in my other photos. [The photo] is still in their [album], which was okay for me. I just did not want to see it.⁵⁶

- 7.130 A similar comment was made by another Forum participant, Imogen:

If any of my friends tag me in a photo that I would not want to be tagged in, it is up to me to get rid of that tag and ask my friend to delete that photo off Facebook altogether. I can untag it myself, but if you want the photo to go completely you have to ask your friend. ... I have my privacy. I can have everything private or to just my friends. I think it is important because some people can find a way.⁵⁷

54 High School Forum, *Transcript of Evidence*, 20 April 2011, pp. CS16-18.

55 High School Forum, *Transcript of Evidence*, 20 April 2011, p. CS17.

56 Amy, High School Forum participant, *Transcript of Evidence*, 20 April 2011, p. CS17.

57 Imogen, High School Forum participant, *Transcript of Evidence*, 20 April 2011, p. CS13.

Submitting requests to site administrators

- 7.131 Participants in the Committee's High School Forum discussed formal methods of removing unwanted photos of themselves. A few had previously submitted requests to site administrators. For example:

Ebru-From my experience, if I really did not like the photo and it was something that was unnecessary, I actually reported the person with the photo because you can do that. That is like sending something to Facebook and saying, 'This person has a photo of me that I don't want on their Facebook.' You have friends but they have more friends that you do not have, and word will get around if it is a really silly photo of you at a party out there in public. You have to care about your reputation at the end of the day.

CHAIR-And the future: when your kids see it.

Ebru-Exactly. If we just pop up in 20 years and think, 'I've graduated and it's still there.'⁵⁸

- 7.132 Another participant was tagged in a sexually explicit photo by an unknown third party:

Peter-I got tagged once by a pornographic picture. I saw it and did not really like it. I reported it [to Facebook].⁵⁹

- 7.133 Forum participants expressed a general frustration with the reporting processes to site administrators:

One of the problems is that when you report something you want to get a personal response such as: 'Your problem has been brought up. We have looked at it and we have found more cases.' But for people who report, either they do not get looked at or they do not get feedback at all. So you do not know what is going and you do not know if it is going to happen again. I think it is best that you should get feedback-no matter what. You should get feedback knowing that it has been brought up, otherwise it might happen again and you would not know. If you report something you want it to be dealt with, otherwise there is no point reporting it. ... you want to know that someone has looked at the problem not only on your behalf but also on behalf of other people.⁶⁰

58 High School Forum, *Transcript of Evidence*, 20 April 2011, pp. CS16-18.

59 High School Forum. *Transcript of Evidence*, 20 April 2011, p. CS8.

60 Jacqui, High School Forum participant, *Transcript of Evidence*, 20 April 2011, p. CS10.

- 7.134 Young people's ideas on how the online environment can be made safer are explored in more detail in Chapter 18.

Conclusion

- 7.135 This Chapter has sought to detail the awareness and appreciation of risks of young people and reveal their decision-making processes when posting content online.
- 7.136 The resources and strategies employed by young people when deciding to post online demonstrate that young people truly are 'digital natives', whilst older generations have had to learn a 'new' set of rules and technologies that were previously foreign. This difference gives great weight to the exchange of learning that can occur between the generations: young people have much to learn from adults about the value of personal information and personal safety; whilst adults have much to learn from young people about their experiences and their social online currency that underpins their engagement with new technologies.

PART 3

Educational Strategies

Schools

- 8.1 Young people engage the online environment to the extent that their online lives blend seamlessly with their lives offline.¹ An equally seamless approach should be taken to cyber-safety, including education, law enforcement, international cooperation, appropriate products and parental/carer supervision.²
- 8.2 In that context, this chapter examines ways of supporting schools to improve cyber-safety for students and to reduce abuses in the online environment.

Early cyber-safety education

- 8.3 Many participants in this Inquiry stressed the need for cyber-safety education to begin early in life, particularly as the age at which many children now enter the online environment is decreasing.
- 8.4 Educational research shows that early childhood is the key time to develop qualities such as respect, peer support, leadership models and building a sense of community.³ Cyber-safe practices should be developed at home and started with the very young.⁴ The time to reach parents about

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

2 Mr Darren Kane, Director, Corporate Security and Investigations and Officer of Internet Trust and Safety, Telstra Corporation, *Transcript of Evidence*, 8 July 2010, p. CS3.

3 Ms Catherine Davis, Federal Women's Officer, Australian Education Union, *Transcript of Evidence*, 30 June 2010, p. CS15.

4 Dr Barbara Spears, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS17; Mr Robert Knight, Executive Officer, Education, Queensland Catholic Education Commission, *Transcript of Evidence*, 17 March 2011, p. CS24; NSW Secondary Principals' Council, *Submission 32*, p. 4.

this approach is when children are between one and five years old, when they want to do their best for their children. They are receptive and eager to learn about what is going to be best for their children's development.⁵

8.5 Most Australian children are not receiving cyber-safety messages from school until Year 2 (seven or eight years old) when they may have already been online for three years. The recreational use that begins at home, or elsewhere with peer or friendship groups or older siblings, is not necessarily accompanied by the kind of safety messages children need. In particular, it is important that messages are delivered early about the 'permanence, multiplication and circulation' of material put online.⁶

8.6 It was suggested that use of the Internet should be in curriculums from the first year of school, so that it is something that children grow up with and is as common-place as other initiatives such as 'Stranger-Danger'. It was also important that this education happens before children had negative experiences online.⁷

8.7 By the time children are four years old, and certainly by the age of five, teachers can have an indication of those who are engaging in anti-social behaviour. At this age teachers can also identify those whose social difficulties are such that they may not understand the impact of what they might do online. For children judged to be at risk, there is more likelihood of success if targeting their behaviours and attitudes begins early. On the basis that early intervention and prevention is the key to this success, initiatives are being targeted towards pre-school children.⁸

8.8 Further, there has to be a clear understanding in school policy of online ethics and the consequences of breaches.⁹ This can only be achieved if students are introduced to these concepts, and later reminded of them, as part of a program. It was stated by many participants in this Inquiry that

5 Ms Barbara Biggins, Honorary Chief Executive Officer, Australian Council on Children and the Media, *Transcript of Evidence*, 3 February 2011, p. CS49.

6 Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, pp. CS36, 40.

7 ACT Council of Parents' and Citizens' Associations, *Submission 41*, p. 3; Mr Craig Scroggie, Vice President and Managing Director, Pacific Region, Symantec Corporation, *Transcript of Evidence*, 8 July 2010, p. CS8.

8 Dr Helen McGrath: Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS59; School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS36. Associate Professor Karen Vered, Department of Screen and Media, Flinders University, *Transcript of Evidence*, 3 February 2011, p. CS37.

9 Dr Gerald White, Principal Research Fellow, Australian Council for Educational Research, *Transcript of Evidence*, 9 December 2010, p. CS48.

such a program must start when a child first enrolls in school, and be continually reinforced throughout their education.

Roles of schools

- 8.9 Schools are complex, busy, diverse and demanding places for students, teachers and parents/carers. They are microcosms of their environments, reflecting the societies and cultural contexts in which they are placed. They have increasingly crowded curriculums, and are being asked by governments to take on more topics. Teachers are expected to do more and more without necessarily being provided with additional resources. Each new task brings responsibility and accountability to parents/carers, students and to government.¹⁰
- 8.10 Schools are the key places to work with young people and encourage them to make changes to improve their own safety and online ethics. However, schools have been reported to only have a 30 percent influence over what is learnt: 70 percent is outside that realm of influence. Principals are responsible for the safety of their students and the staff within schools, and this extends in many places outside their boundaries to the local community. Thus, Principals Australia argued, cyber-safety has to be a whole-of-community issue.¹¹

Duty of care

- 8.11 Schools are important in providing young people with interpersonal, technological and conflict resolution skills.¹² Further, there is a 'huge need' to recognise that they are dealing with the whole social and emotional development of their students.¹³
- 8.12 The Alannah and Madeline Foundation referred to the duty of care to create a safe environment for students and staff.¹⁴ Cyber-safety is part of this expectation, and Professor Hemphill of the Murdoch Children's

10 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 43; Mr Mark Anghel, Assistant Secretary, Legal Services, Queensland Teachers' Union, *Transcript of Evidence*, 17 March 2011, p. CS1

11 Mr Jeremy Hurley, Manager, National Education Agenda, Principals Australia, *Transcript of Evidence*, 11 June 2010, p. CS9.

12 Murdoch Children's Research Institute, *Submission 111*, p. 4.

13 Ms Dianne Butland, Executive Member, Federation of Parents and Citizens Associations of NSW, *Transcript of Evidence*, 30 June 2010, p. CS37.

14 Alannah and Madeline Foundation, *Submission 22*, p. 11.

Research Institute suggested that schools had to go back to their policies on bullying to ensure that these, and any training for staff, covered cyber-bullying explicitly.¹⁵

- 8.13 The nature of technology means that there is a great deal more responsibility on schools to resolve cyber-safety matters.¹⁶ There has been 'a significant increase' in the time spent by senior executive and welfare officers in schools dealing with these issues. The time that can be spent counselling young people appropriately can be 'extraordinary'. This is particularly so if restorative justice programs are included.¹⁷
- 8.14 It is important for greater clarity be given on the question of the responsibility of schools for student behaviour outside of school hours. The NSW Secondary Principal's Council stated that it was 'not appropriate' for schools to spend such significant resources dealing with out-of-hours communications that lead to student-to-student, or family, conflict. Nor, it believed, should the consequences of such communications be the sole responsibility of schools.¹⁸
- 8.15 The Federation of Parents and Citizens' Associations of NSW stated:
- Some schools have reportedly buried their heads in the sand with regards to the issues around online bullying and its repercussions. They have suggested that, as the incident didn't happen at school, the school is not accountable and shouldn't get involved. However, where children are bullied, using any form of technology, the repercussions are often felt the following day at school.¹⁹
- 8.16 It is unclear how much schools are hampered by the 'often unrealistic fear' of being sued. If schools are required to sign up to provide everything

15 Associate Professor Sheryl Hemphill, Senior Research Fellow, *Transcript of Evidence*, 9 December 2010, p. CS26; Associate Professor Marilyn Campbell, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS16. Murdoch Children's Research Institute: *Submission 111*, p. 5.

16 Ms Catherine Davis, Federal Women's Officer, Australian Education Union, *Transcript of Evidence*, 30 June 2010, p. CS4; Mr Philip Lewis, Chair, Association of Principals of Catholic Secondary Schools (SA), *Transcript of Evidence*, 3 February 2011, p. CS3.

17 NSW Secondary Principal's Council, *Submission 32*, p. 3; Mr Chris Watt, Federal Secretary, Independent Education Union of Australia, *Transcript of Evidence*, 30 June 2010, pp. CS14-15.

18 NSW Secondary Principal's Council, *Submission 32*, p. 3; See also Ms Kelly Vennus, Programs and Training Officer, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS11; Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2010, p. CS31.

19 Federation of Parents and Citizens' Associations of New South Wales, *Submission 76*, p. 3.

relating to cyber-safety, it was pointed out that they could be subject to litigation at a later time.²⁰

- 8.17 Powers of suspension and exclusion provide a discretionary point of entry for principals in South Australia to talk about their concerns and the dangers in situations. Some parents are very protective of their boundaries, so that it is difficult for principals to talk about the behaviour of children in out-of-school hours. Such actions can be viewed by parents as matters outside the purview of school principals.²¹
- 8.18 As a result of the pervasiveness of technology and its impact on schools, two State education departments changed their policies on out-of-hours occurrences.
- 8.19 South Australia has changed its legislation to give principals authority to take action over behaviour that may occur away from the school or outside school hours. Action can be taken at the time of, or after an event affecting the wellbeing of another student, teacher or member of the school community. Principals are empowered to suspend or expel students who act in such a manner.²² The system in South Australia appears to be working productively, and authorities in other States have evidently expressed some frustration that they do not have similar processes.²³ NSW has also changed legislation to clarify that schools are responsible for occurrences outside their premises and out-of-hours.²⁴
- 8.20 This accepted duty of care that schools owe students is complicated by the 24 hour/seven days per week nature of technology. Where it used to be relatively easy to identify bullying behaviour in the schoolyard, the challenge for teachers is now what happens between 3pm and 9am, or over weekends.²⁵ There is legislation in the United Kingdom that provides

20 Australian University Cyberbullying Research Alliance: *Submission 62*, p. 29; Dr Barbara Spears, *Transcript of Evidence*, 3 February 2011, p. CS16.

21 Mr Greg Cox, Department of Education and Children's Services, SA, *Transcript of Evidence*, 3 February 2011, pp. CS72-73.

22 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, pp. CS16, 30; Mr Greg Cox, Department of Education and Children's Services, SA, *Transcript of Evidence*, 3 February 2011, p. CS69.

23 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS30.

24 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS16; Mr Greg Cox, Department of Education and Children's Services, SA, *Transcript of Evidence*, 3 February 2011, p. CS68.

25 Mr Chris Watt, Federal Secretary, Independent Education Union of Australia, *Transcript of Evidence*, 30 June 2010, p. CS15; Ms Georgie Ferrari, Chief Executive Officer, Youth Affairs Council of Victoria, *Transcript of Evidence*, 11 June 2010, p. CS33.

schools with the authority to address student misbehaviour for 24 hours/seven days, wherever it occurs.²⁶

Suspension and Expulsion of School Students - Procedures specifically recognise that behaviour that may warrant suspension includes “hostile behaviour directed towards students, members of staff or other persons including verbal abuse and abuse transmitted electronically such as by email or SMS text message”.²⁷

- 8.21 As previously mentioned however, the New South Wales Secondary Principals Council expressed the view that it was ‘not appropriate’ that schools spend such significant staff resources dealing with communications generated out-of-hours.²⁸
- 8.22 If responsibility is to be taken for students’ actions outside school hours, and for the measure to be effective, it will be necessary to ensure that the necessary resources are available, and that the appropriate educational unions are involved in the process.

Recommendation 13

That the Attorney-General, as a matter of priority, work with State and Territory counterparts to develop a nationally consistent legislative approach to add certainty to the authority of schools to deal with incidents of inappropriate student behaviour to other students out of school hours.

National Safe Schools Framework

- 8.23 The National Safe Schools Framework (NSSF) was originally endorsed by all Australian Ministers for Education in 2003. It included an agreed set of national principles to promote safe and supportive school environments,

26 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS12

27 New South Wales Secondary Principals Council, *Submission 32*, p. 3.

28 Mr Jeremy Hurley, Manager, National Education Program, Principals Australia, *Transcript of Evidence*, 11 June 2010, p. CS9. New South Wales Secondary Principals’ Council, *Submission 32*, p. 3.

and appropriate responses schools could adopt to address bullying, harassment, violence, child abuse and neglect.²⁹

- 8.24 As a result of a review, the revised NSSF was endorsed in December 2010 by the Ministerial Council of Education, Early Childhood Development and Youth Affairs. Ministers undertook to implement the Framework in all jurisdictions and use it to inform the development of safe and supportive school policies. The NSSF was launched on 18 March 2011, to coincide with the National Day of Action against Bullying and Violence, and is available to all Australian primary and secondary schools.
- 8.25 The NSSF is supported by a comprehensive and practical online resource manual. This includes an audit tool that assists schools to make informed judgements about what they are doing well, and to identify gaps in existing policies and procedures.
- 8.26 All Australian schools are encouraged to use this Framework as a basis for developing approaches to address bullying. It recognises that sustainable approaches are required to reduce bullying in the long-term.
- 8.27 The NSSF is 'highly regarded' by Australian and international researchers and practitioners, and is the only national Framework of its kind in the world. Cross-cultural collaboration and effective working relationships across all jurisdictions, and with other key stakeholders, underpin the success of the NSSF.

Curriculums and programs

- 8.28 The Ministerial Council for Employment, Education, Training and Youth Affairs, comprising Ministers for Education and Training, has previously stated the goals for education in Australia. The *Melbourne Declaration on Educational Goals for Young Australians* (2008) provides a mandate and guide for schools about curriculums. It made four important points about information and communications technologies (ICT):
- young people need to be highly skilled in its use;
 - schooling should also support the development of skills in areas such as social interaction, cross-disciplinary thinking and the use of digital media that will be essential in all 21st century occupations;

29 Material in this section was drawn from Department of Education, Employment and Workplace Relations, *Submission 135*, pp. 7-8.

- successful learners have essential literacy and numeracy skills, and are creative and productive users of technology as a foundation for success in learning areas; and
 - for further learning, curriculums will include practical knowledge and skills development in areas such as ICT and design and technology.³⁰
- 8.29 The Australian Council of Educational Research noted that the generally low adoption of ICT, especially in the middle secondary years, is 'by no means' specific to Australia. It did not signal a lack of interest to the use of ICT in curriculums. One study nominated technological reliability, limited access and limited bandwidth as barriers to greater uptake of ICT in these years.³¹
- 8.30 The Queensland Catholic Education Commission suggested that ICT programs tended to lack credibility because they are not seen as part of the mainstream curriculum. Concerns were also expressed about 'bolt-on subjects' that students generally see as down-time.³²
- 8.31 Symantec Corporation recommended that a national approach is required so that cyber-safety is included in a standardised, mandatory curriculum. The Queensland Teachers Union also observed that if there was to be an effective campaign on cyber-safety, it had to be appropriately funded and resourced, and not just 'forced' on to the ever-increasing curriculum.³³
- 8.32 The Australian Parents Council advised that:
- schools have been at the forefront of efforts to incorporate principles of resilience and well-being in their students in the offline environment through a number of programs and cross curriculum initiatives over past years. So perhaps it is not a change of the culture of schools that is needed but the expansion of
-

30 Australian Council of Educational Research, *Submission 20*, pp. 3-4 citing the Ministerial Council for Employment, Education, Training, and Youth Affairs (MCEETYA), 2008, *Melbourne Declaration on Educational Goals for Young Australians*. Melbourne: MCEETYA. Retrieved May 20, 2010, from http://www.curriculum.edu.au/verve/resources/National_Declaration_on_the_Educational_Goals_for_Young_Australians.pdf. This body has been replaced by the Ministerial Council of Education, Early Childhood Development and Youth Affairs.

31 Australian Council of Educational Research, *Submission 20*, p. 7.

32 Mr Robert Knight, Executive Officer, Education, Queensland Catholic Education Commission, *Transcript of Evidence*, 17 March 2011, p. CS30; Mr Mark Anghel, Assistant Secretary, Legal Services, Welfare, Queensland Teachers Union, *Transcript of Evidence*, 17 March 2011, p. CS8.

33 Queensland Teachers Union: *Submission 21*, p. 1; Mr Mark Anghel, Assistant Secretary, Legal Services, Welfare, Queensland Teachers Union, *Transcript of Evidence*, 17 March 2011, pp. CS1, 8.

existing prevention and intervention strategies that have proven successful in offline environments to promote cyber safety.³⁴

8.33 Including ICT material in any curriculum is complicated by the lack of data on trends, successfulness of intervention programs, restorative justice initiatives and perpetrator rehabilitation. Research in such areas would inform the development of prevention strategies, as well as a national curriculum.³⁵

8.34 The Australian Curriculum, Assessment and Reporting Authority (ACARA) is developing the Australian Curriculum. With particular reference to cyber-safety, it has been identified that students will develop ICT competence when they apply social and ethical protocols to operate and manage emerging technologies.

8.35 Conceptual statements are being prepared by the ACARA for publication to support teachers and schools wishing to use them to assist the development of their teaching and learning programs. Each document will include:

- the conceptual framework, evidence and references for the capability; and
- a continuum of learning, showing development across bands of year levels.

8.36 For competence in ICT, this work will include descriptions of developments expected of students at the end of Years 2, 6 and 10.³⁶

Partnerships with the Australian Communications and Media Authority

8.37 The South Australian Commission for Catholic Schools acknowledged the work of the Australian Communications and Media Authority (ACMA) in:

providing access to free, high quality cyber-safety training through the *Cyber-Safety Outreach Professional Development for Educators* program and the *Internet Safety Awareness Presentations* to students, teaching staff and parents in school communities ... Feedback from Catholic school communities is consistently favourable about the relevance and usefulness of the training and resources.³⁷

34 Australian Parents Council, *Submission 10*, p. 4.

35 Australian Secondary Principals' Association, *Submission 33*, p. 3.

36 Australian Curriculum, Assessment and Reporting Authority, *Submission 119*, pp. 1-2.

37 South Australian Commission for Catholic Schools, *Submission 9*, p. 3.

- 8.38 Further, on 16 May 2011, ACMA launched the *Connect.ed* interactive e-learning program for teachers that buttresses the professional development seminars.³⁸

Probably the single biggest driver for take-up of our professional development workshops for teachers has been their concern about issues relating to cyberbullying and also, in a very personal way, if they are legally responsible for that.³⁹

- 8.39 The role of ACMA is addressed in Chapter 1.

Technological approaches

- 8.40 A number of schools are employing technological approaches to assist them to address cyber-safety issues. Secondary schools in particular are using a dedicated email system where concerns about an individual's cyber-safety, or that of others, can be reported anonymously.

- 8.41 A Queensland high school has online counselling, appointments to see the counsellor can be made online, and there is also a chat facility.⁴⁰ The Australian Education Union called for the number of, and resources available to school counsellors be increased so to better assist students:

There can never be guarantees against malicious behaviour, but many risks which are simply borne of ignorance can be significantly reduced if children are educated properly in the use of technologies.⁴¹

- 8.42 The use of mobile phones is restricted at some schools, and banning them has been suggested as a way of reducing cyber-bullying.⁴² However, this would be a challenge for schools and there is little evidence supporting this strategy. Professor Phillip Slee of the Australian University Cyberbullying Research Alliance stated that 'robust research' had found

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

39 Ms Andree Wright, Acting General Manager, Consumer, Content and Citizen Division, ACMA, *Transcript of Evidence*, 3 March 2011, p. CS19.

40 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS30.

41 Australian Education Union, Tasmanian Branch, *Submission 137*, pp. 1-2

42 Association of Independent Schools of SA, *Submission 19*, p. 8.

that it was not at all effective in dealing with abuses such as cyber-bullying.⁴³

- 8.43 In evidence submitted to the Committee, at least one Australian school enforces a policy whereby the school surveys a number of students' mobile phones every week to see what sites they have accessed. Sanctions are imposed if a student has deliberately gone onto sites that are not acceptable under school policies.⁴⁴
- 8.44 Some schools use filters on their local networks. However, these can be bypassed easily by using proxy sites. The Organisation of Economic Co-operation and Development found that using a 'lock down' approach kept students safe at school but they were more vulnerable overall.⁴⁵ Research has shown that 'lock-down' systems are less effective in helping students to learn to use the Internet safely and responsibly. While they kept them safe at school, students from such schools are 'more vulnerable overall'.
- 8.45 Some Australian education systems already have 'Acceptable Use' Agreements with students, and breaches can include disciplinary action.
- 8.46 According to the Alannah and Madeline Foundation, schools with effective behaviour management systems and vigilant supervision of computer use provide another layer of support. It believed that Australian schools are lagging behind in producing robust 'Acceptable Use' policies that reach beyond the school to include parents/carers and the wider community.⁴⁶
- 8.47 The Australian Parents Council discussed the broader effort required:
- Parents need to be informed of the current online and digital environment and the relative dangers of predators online, sexting, cyber bullying and the technology available to guard against inappropriate content material, such as hate sites. They need to be aware of issues of cyber crime, computer security, identity theft: the consequences and sanctions which may be imposed for bad or

43 Professor Philip Slee, *Transcript of Evidence*, 3 February 2011, p. CS12; Australian University Cyberbullying Research Alliance: *Submission 62*, p. 27. See also Associate Professor Sheryl Hemphill, Senior Research Fellow, Murdoch Child Research Institute, *Transcript of Evidence*, 9 December 2010, p. CS26.

44 Dr Gerald White, Principal Research Fellow, Australian Council of Educational Research, *Transcript of Evidence*, 9 December 2010, p. CS48.

45 Australian Council of Education Research, *Submission 20*, p. 7 citing Organisation of Economic Co-operation and Development (2010) *Are the New Millennium Learners making the Grade? Technology use and educational performance in PISA*, Paris CERI, OECD.

46 Alannah and Madeline Foundation: *Submission 22*, p. 8; Dr Judith Slocombe, Chief Executive Officer, *Transcript of Evidence*, 11 June 2010, p. CS37.

criminal behaviours and the ways in which inappropriate use of technology can interfere with other important activities and responsibilities in the lives of their young people.⁴⁷

8.48 Netbox Blue also recommend promoting and enforcing Acceptable Use policies, as

- The creation of an acceptable policy framework and its communication to all stakeholders - students, teachers, parents and carers;
- Education for all stakeholders on minimising known risks, or dealing with them if presented with a situation that places them at risk – focusing on working with students, teachers, parents and carers;
- Technology enforcement – in and outside the school network on all school owned equipment; and
- Regular reviews of attempts to breach such policy frameworks to improve education and to manage individual behavioural issues.⁴⁸

8.49 As already noted, Roar Educate believed that ‘sensationalist’ reporting has shaped the national response to cyber-safety incidents. It also believed that, to protect students, the first instinct of schools has been to ‘lock down’. Within their ‘sandbox environments’, they have been slow to encourage the use of Web 2.0 tools. Roar Educated stated that this environment seems to have reduced the need for engagement about cyber-safety across school communities: students, teachers and parents/carers.⁴⁹

8.50 The Alannah and Madeline Foundation would like to see the introduction of a user-friendly toolkit in text and online versions be made available to all schools to assist with the measurement and the effectiveness of cyber-safety policies and the whole of community approach.⁵⁰

8.51 The Director of the South Australian Office of Youth commented that:

We found that young people probably were not that interested in getting information from schools about how to engage with social networking. They were more aware of how to use and engage with those sites than their teachers and even their parents were. One of our views in the Office for Youth is that education exists

47 Australian Parents Council, *Submission 10*, pp. 2-3.

48 Netbox Blue, *Submission 17*, p. 4.

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

50 Alannah and Madeline Foundation, *Submission 22*, p. 12.

outside the school system. We would like to see a greater emphasis on engaging with other community organisations, sporting clubs and youth development programs as well as parents to better engage and educate young people because they are more likely through research to listen to their friends, parents and relatives rather than schoolteachers.⁵¹

- 8.52 The role of schools, parents/carers and the wider community is inextricably linked. Research by the British Office for Standards in Education, Children's Services and Skills revealed that the most effective schools have a well-considered approach to keeping students safe online and helping them to take responsibility for their own safety. Successful schools have a multi-layered managed approach, involving students, parents and teachers, where there are fewer inaccessible sites.
- 8.53 There are many cyber-safety programs, but not all have been taken up. For example, it was suggested that while the 2009 National Safe Schools Framework went out to every Australian school, 'about 80 percent' did not take it up because there was no way for them to implement it. The Alannah and Madeline Foundation also expressed concern that while schools might have anti-bullying policies, they may not be implemented.⁵²
- 8.54 Other cyber-safety programs and initiatives are available, and have been referred to in this Report, but it is not clear how many of them have been appropriately evaluated and accredited.⁵³ Strategies that could be employed by the whole of school community are addressed in Chapter 10.

Coordination

- 8.55 Time-poor teachers may benefit from having material accessible from a central on line resource. Netbox Blue consider that schools could be encouraged to adopt available solutions if a central body was established to:
- provide advice and online collateral, papers, policies and best practice examples to schools;

51 Mrs Tiffany Downing, Director, Office of Youth SA, *Transcript of Evidence*, 3 February 2011, pp. CS19-20.

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

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

- provide certification for providers within each ‘pillar’, such as the Family Friendly Filter scheme;
- establish a clear set of standards for a school to have achieved to fulfil their duty of care;
- establish a national certification standard for schools in providing a cyber-safe environment for students;
- promote the program to all schools and encourage them via incentives to benefit for adherence to the standards, and
- establish an ongoing review of the standards and an annual re-accreditation.⁵⁴

8.56 The NSW Secondary Principals’ Council suggest that assistance to schools should:

- include a clear legal definition of ‘cyber-bullying’;
- include consistent State and Federal legislation, and
- provide guidelines regarding the actual legislation governing cyber-bullying and how it affects young people.⁵⁵

Accreditation

8.57 Given the nature and pervasiveness of the online world, in a context where warnings and filters have limited efficacy, the most effective approach to cyber safety is to build good teaching and learning experiences into classrooms.⁵⁶

8.58 To ensure quality and consistency across jurisdictions, educational standards for cyber-safety education need to be developed.⁵⁷ Standards need to be developed by the Australian Government for cyber-safety, and the safe, responsible use of digital technologies. Such standards should prevail across all Departments and agencies, to provide ‘a beacon for the non-government sector’.⁵⁸

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

55 NSW Secondary Principals Council, *Submission 32*, p. 5.

56 Australian Education Union, Tasmanian Branch, *Submission 137*, p. 2.

57 Australian Education Union, Tasmanian Branch, *Submission 137*, p. 2.

58 Australian Education Union, Tasmanian Branch, *Submission 137*, p. 3.

Committee views

- 8.59 While many different policies and programs have been put in place to deal with cyber-safety issues, allocation of resources is an issue for all schools. The continuing pressure on curriculums must also be recognised, because it is clearly not simply a matter of adding topics without displacing or reducing times for other, existing items.
- 8.60 Cyber-safety is, however, of such importance to the education and future of young people that the effectiveness of the current approach(es) needs to be analysed.
- 8.61 There is no doubt that awareness of threats to the safety of young people in the online environment has grown, within schools and in the community generally. Perhaps because of media interest, this is especially true of cyber-bullying. Many responses to cyber-safety problems developed and implemented across Australia were revealed during this Inquiry.
- 8.62 The dedication with which solutions have been sought to reduce the risks to those, particularly young people, using the online environment cannot be faulted. While authorities in all jurisdictions are justifiably proud of their cyber-safety programs, there are two measures that can be taken to reduce online threats to users, especially young people.
- 8.63 The first and most important of these was addressed by many participants in this Inquiry: a national cyber-safety education program, devised and implemented with the cooperation of all Australian jurisdictions. The introduction of such a program must be accompanied by a second measure: an extension of the role and powers of ACMA. These proposals will be addressed in Chapter 19.
- 8.64 Many parents/carers are not involved in cyber-safety issues as individuals or via the schools to which their young people go because they lack two things: time and knowledge and/or confidence about the online environment. Their involvement is vital to reducing the incidence of abuses in the online environment. Ways to give them confidence, and extend their knowledge of cyber-safety issues will be addressed in Chapter 10.
- 8.65 At least one important measure can and needs to be taken by schools. 'Acceptable Use' Agreements and supporting policies covering the use of the technology supplied to their students is an area that schools need to address. These Agreements are not always backed by procedures that are followed consistently, or even widely known and understood.

- 8.66 For such Agreements to be effective, they must be:
- clear about the rights and responsibilities of users, especially penalties for breaches of conditions of use;
 - signed by students and parents/carers;
 - preceded by information sessions on cyber-safety, perhaps presented wholly or partially by the young people themselves, and
 - supported by policies that are known and understood by all staff and students, so that they can be implemented promptly, effectively and consistently.
- 8.67 As noted above, the Australian Curriculum, Assessment and Reporting Authority is developing the Australian Curriculum. Together with the revised National Safe Schools Framework, there is progress in the development of national core standards in education in this country.
- 8.68 The Ministerial Council of Education, Early Childhood Development and Youth Affairs is the appropriate forum to guide national action towards such core standards for courses in cyber-safety. Using the revised National Safe Schools Framework, it is in a position to encourage the introduction of core standards, including the development of national 'Acceptable Use' agreements, that will assist schools to deal with threats to their students and staff from the online environment.

Recommendation 14

That the Minister for School Education, Early Childhood and Youth propose to the Ministerial Council of Education, Early Childhood Development and Youth Affairs:

- to develop national core standards for cyber-safety education in schools,
- to adopt a national scheme to encourage all Australian schools to introduce 'Acceptable Use' Agreements governing access to the online environment by their students, together with the necessary supporting policies, and
- to encourage all Australian schools to familiarise students, teachers, and parents with the ThinkUknow program, and the Cyber-Safety Help Button and other resources of the Australian Communications and Media Authority to promote the cyber-safety message.

Recommendation 15

That the Minister for School Education, Early Childhood and Youth and the Minister for Broadband, Communications and the Digital Economy consider extending the Australian Communications and Media Authority's *Connect-ED* program and other training programs to non-administration staff in Australian schools including school librarians, chaplains and counsellors.

Teachers

Professional development of teachers

- 9.1 At the 4th Biennial Conference of the Australian National Centre Against Bullying in 2010, training of teachers was one of the ten steps recommended to increase cyber-safety and reduce bullying across the community.¹
- 9.2 The *Australian Covert Bullying Prevalence Study* showed that:
- ... the majority of staff (67%) felt other teachers at their school needed more training to enhance their skills to deal with a range of issues related to covert bullying, such as dealing with incidents or addressing covert (including cyber bullying) within the curriculum... Of great concern, of those young people who were cyber bullied and informed an adult, 45% of them reported that things either stayed the same or got worse. This reflects the need expressed by school staff for further training in how to deal with bullying, in particular cyber bullying ²
- 9.3 Many schools already have comprehensive cyber-safety programs and policies in place. These should include external presentations from cyber-safety and childhood development experts to allow teachers to ask about

1 Mental Health Council of Australia, *Submission 52*, p. 6. See also <http://www.ncab.org.au/ConferenceInfo/>, *Navigating the Maze: cybersafety and wellbeing solutions for schools* conference.

2 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 15 citing Cross *et al*, 2009, the *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, Edith Cowan University.

their own learning environment. Lessons learnt by such means can then be translated into individual teaching practices.³

- 9.4 As part of registrations in South Australia, teachers are required to complete training in Responding to Abuse and Neglect Education and Care, including cyber-safety elements, and this must be updated every three years.⁴
- 9.5 While all teachers are not necessarily experts in the subject, provided that they relate well to their students, they can play important roles in conveying messages about cyber-safety. Specific training is required to teach this material, particularly at secondary level. To do this effectively funding and resources are required, especially for continuing professional development.⁵
- 9.6 To reduce the impact of bullying, it is important to help victims find ways to develop positive connections with peers and a trusted adult. The NSW Government noted that there was evidence that teachers can help promote positive relationships by:
- establishing networks of buddies;
 - establishing circles of support;
 - creating peer mentors; and
 - finding ways to highlight the child's talent for others to see.⁶
- 9.7 The Australian Council of Educational Research referred to a study that noted the professional development of teachers needed to address attitudes and perceptions as well as development of technological skills.
- 9.8 The two issues emerging 'consistently' from literature and research are:
- a lack of teacher confidence, and
 - the need for professional development of teachers in information and communication technology (ICT).
- 9.9 This Council argued that these matters need to be addressed if schools are to be supported to implement online safety instruction and assist students to develop appropriate online behaviours. Professional development focused on teachers' perceptions about the use of ICT in the curriculum
-

3 Ms Candice Jansz, *Submission 44*, p. 5.

4 Mr Greg Cox, Department of Education and Children's Services, SA, *Transcript of Evidence*, 3 February 2011, p. CS69.

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

6 NSW Government, *Submission 94*, p. 26.

has to be addressed, as do technological skills coaching needs at the school level.

- 9.10 Confident teachers familiar with the uses and concerns about the use of ICT will be better able to assist students to develop effective online safety strategies.⁷ The Australian Council for Educational Research commented that, the 'professional development of teachers needs to address attitudes and perceptions as well as technological skill development'.⁸
- 9.11 Reference has already been made to the fact that curriculums are already overloaded, and to the difficulty of including additional items. To deliver an over-burdened curriculum, collegiality and collaboration are important for teachers. Lack of time and resources can have impacts on their behaviour to students, and such things as performance pay and additional requirements imposed from outside can also have their effects.⁹

Pre-service teacher education

- 9.12 Many participants in the Inquiry drew attention to the importance of the education of teachers before they begin their service.
- 9.13 It appears that the greatest concern for newly graduating teachers is their ability to deal with parents/carers. Another key concern is that they feel that they do not get enough support about behaviour management, either during their education or in their first few years as teachers.¹⁰
- 9.14 Experienced teachers are being replaced by more recent graduates already operating in the online environment and who are, for the most part, savvy and skilled. A 2010 survey of pre-service teachers on their understanding of bullying and cyber-bullying revealed that two-thirds of the participants felt 'confident and competent' to deal with these issues because they understand the online environment.¹¹

7 Australian Council of Educational Research, *Submission 20*, pp. 7-8.

8 Australian Council of Education Research, *Submission 20*, p. 7, citing Pierce R and Ball L, 2009, 'Perceptions that may affect teacher's intentions to use technology in secondary mathematics classes' *Educational Studies in Mathematics* 71(3): 299-317.

9 Ms Catherine Davis, Federal Women's Officer, Australian Education Union, *Transcript of Evidence*, 30 June 2010, p. CS15.

10 *Transcript of Evidence*, 30 June 2010, p. CS20: Ms Kate Lyttle, Secretary, Australian Parents' Council; Ms Catherine Davis, Federal Women's Officer, Australian Education Union.

11 Dr Barbara Spears: Senior Lecturer, School of Education, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS38 (and see Australian University Cyberbullying Research Alliance, *Submission 62*, p. 24, for some results of this survey.) Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS17.

- 9.15 The Australian University Cyberbullying Research Alliance noted, however, that the role that pre-service teacher education can play in a 'whole-of-school' approach to cyber-safety is often omitted. The Alliance also referred to another study which showed that pre-service teachers were reflecting advice and strategies which young people do not use and to which they do listen. When asked what advice they would give to students who were being bullied, 96 percent of pre-service teachers said that it would be to seek help, to tell a teacher or a parent/carer.¹²
- 9.16 Throughout the Committee's inquiry, a need was seen for teacher training in Australia to include cyber-safety units as part of pre-service teacher education. Units of this kind should include a component addressing awareness and skills for preventing and managing bullying.¹³
- 9.17 In January 2011, the Australian Communications and Media Authority rolled out its Pre-Service Teacher Training program. This is built on its successful face-to-face Professional Development for Educators workshops. It will equip final year student teachers with the skills, knowledge and classroom resources to help their students stay safe online. This pioneering program consists of a lecture and a tutorial, and 18 universities have confirmed bookings to the end of June 2011.¹⁴
- 9.18 The demand for speakers from the Authority, however, exceeds its capacity to deliver:
- There are other programs available but these can be very costly (prohibitively so) and the content may or may not be as good as anybody can purport to be an expert in the field and there is no regulatory body.¹⁵

12 Australian University Cyberbullying Research Alliance: *Submission 62*, pp. 24- 25; Dr Barbara Spears, *Transcript of Evidence*, 3 February 2011, pp. CS14-15.

13 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS33; Alannah and Madeline Foundation, *Submission 22*, p. 5.

14 Australian Communications and Media Authority: *Submission 80*, p. 2; Ms Andree Wright, Acting General Manager, Digital Economy Division, *Transcript of Evidence*, 3 March 2011, p. CS3. See Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS61, for the success of its programs for teachers.

15 Parents Victoria Inc, *Submission 143*, p. 3.

Recommendation 16

That the Minister for Tertiary Education, Skills, Jobs and Workplace Relations and the Minister for Broadband, Communications and the Digital Economy work together to ensure that sufficient funding is available to ensure the Australian Communications and Media Authority can provide the necessary training for professional development of Australian teachers.

Recommendation 17

That the Minister for Tertiary Education, Skills, Jobs and Workplace Relations and the Minister for Broadband, Communications and the Digital Economy encourage all Australian universities providing teacher training courses to ensure that cyber-safety material is incorporated in the core units in their curriculums.

Cyber-bullying of teachers

- 9.19 Cyber-bullying of teachers by students was an issue for several participants in this Inquiry. The anonymity of some online sites allows staff or schools to be the target of inappropriate content.¹⁶ There is an increase in the number of teachers being bullied by students and this can affect their lives, careers and performances because of its public nature.¹⁷
- 9.20 The Australian Teachers Union highlighted the personal and professional attacks on teachers by students using Facebook and Myspace such as the Rate My Teachers sites.¹⁸ The Union is contacted 'regularly' by members who are attacked personally and professionally via websites such as RateMyTeachers and Facebook. Further, the Union has received allegations of students filming classes on mobile phones and uploading videos with disparaging comments onto YouTube.¹⁹

16 NSW Secondary Principals Council, *Submission 32*, p. 3; Mr Mark Anghel, Assistant Secretary, Legal Services, Welfare, Queensland Teachers Union, *Transcript of Evidence*, 17 March 2011, pp. CS2, 8.

17 Mr Mark Anghel, Assistant Secretary, Legal Services, Welfare, Queensland Teachers Union, *Transcript of Evidence*, 17 March 2011, p. CS1.

18 Australian Education Union, *Submission 11*, p. 9.

19 Australian Education Union, *Submission 11*, p. 9; Ms Diane Butland, Executive Member, Federation of Parents' and Citizen's Associations of NSW, *Transcript of Evidence*, 30 June 2010, p. CS5.

- 9.21 The NSW Secondary Principals Council and the NSW Teachers Federation noted similar conduct:

Cyber-harassment of staff should also be recognised when considering the importance of stakeholders working together. The anonymity of some sites does allow staff or schools to be the targets of inappropriate content. Tracing of the source of the postings would be helpful in preventing these postings in the first place.²⁰

Teachers work well with School Liaison police who reinforce to students the message of Cyberbullying. But investigating cyber-bullying is difficult even for the police.²¹

- 9.22 The Queensland Teachers Union believe that the number of false and defamatory statements made online by students about teachers is increasing. It is 'quite common' for teachers to be accused falsely of being paedophiles and, in one case, a teacher's private address was included on a site. Students have also placed some false profiles of teachers on 'dating' sites.²²
- 9.23 If offenders can be traced, the Queensland Department of Education and Training allows behaviour management policies at schools to be used and this can range from suspension to expulsion from school.²³
- 9.24 The Union noted that it had 'very little success' in having material removed from the RateMyTeachers site. While it advises its members about inappropriate material on such sites, because of the complexity and cost of taking legal action, it has never proceeded against anyone for defamatory remarks.²⁴
- 9.25 There continue to be ethical and legal issues about the presence online of educators and the blurring of the teacher/student relationship. Teachers are still unclear about the legal requirements and implications of cyber-safety.²⁵ Some teachers are ignorant about the need for appropriate

20 NSW Secondary Principals Council, *Submission 32*, p. 3.

21 NSW Teachers Federation, *Submission 73*, p. 4

22 Queensland Teachers Union: *Submission 21*, p. 1; Mr Mark Anghel, Queensland Teachers Union, Assistant Secretary, Legal Services, Welfare, *Transcript of Evidence*, 17 March 2011, p. CS2.

23 Mr Mark Anghel, Queensland Teachers Union, Assistant Secretary, Legal Services, Welfare, *Transcript of Evidence*, 17 March 2011, pp. CS2, 5.

24 Mr Mark Anghel, Queensland Teachers Union, Assistant Secretary, Legal Services, Welfare, *Transcript of Evidence*, 17 March 2011, pp. CS3, 5, 6.

25 Queensland Catholic Education Commission: *Submission 67*, p. 5.

relationships with their students and do not understand the possible implications, for example, of sending a student a text message.²⁶

- 9.26 There is a view that there is limited redress for teachers, and students in some cases, because Internet service providers (ISPs) are unwilling or unable to remove material in a timely manner. Unless posted messages are defamatory within the existing law, or contravene communications regulations, the perpetrators can continue to operate and inflict significant harm by damaging the reputation of individual teachers and school communities.²⁷ Mr Michael Wilkinson from the Queensland Catholic Education Commission stated:

Increasingly profiles of teachers were being uploaded by students with all sorts of very negative and close to defamatory comments, but never crossing the line so that legal action could be taken. Through the student protection person in Toowoomba Catholic Education, we pursued that at some length to see if we could have the site taken down. It was taken down, and then it was up 48 hours later.²⁸

- 9.27 The Systems Administrators' Guild of Australia noted that there is anecdotal evidence that academics are being bullied by their students. While they are comparatively easy to block, via emails, as social networking sites are not yet much used for teaching.²⁹
- 9.28 The Tasmanian Department of Education provides guidance to schools where teachers are aggrieved by material that might be put on RateMyTeachers by, for example, contacting the person responsible for posting it or the site itself.³⁰
- 9.29 Netbox Blue suggested a central legal counsel be established to provide advice to schools therefore providing access to the best advice and consistency across schools.³¹

26 Australian Education Union, *Submission 11*, p. 9; Mr Michael Wilkinson, Executive Secretary, *Transcript of Evidence*, 17 March 2011, p. CS29; Mr Mark Anghel, Assistant Secretary, Legal Services, Welfare, Queensland Teachers Union, *Transcript of Evidence*, 17 March 2011, p. CS4.

27 Mr Michael Wilkinson, Executive Secretary, *Transcript of Evidence*, 17 March 2011, pp. CS29, 30; Queensland Catholic Education Commission: *Submission 67*, p. 2.

28 Mr Michael Wilkinson, Executive Secretary, Queensland Catholic Education Commission, *Transcript of Evidence*, 17 March 2011, p. CS30.

29 Ms Donna Ashelford, Board Member, National Management Committee, System Administrators' Guild of Australia, *Transcript of Evidence*, 17 March 2011, p. CS69.

30 Mr Trevor Hill, Department of Education, Tasmania, *Transcript of Evidence*, 20 April 2011, pp. CS6-7.

31 Netbox Blue, *Submission 17*, p. 6.

- 9.30 To combat cyber-bullying of teachers and support them, a 'reputation management' position has been established in the Queensland Department of Education and Training. The occupant has good contacts with State police and the Australian Federal Police, as well as with Facebook. The Department noted that relationships with Facebook and Google means that inappropriate material can be removed 'fairly quickly'.³²

Recommendation 18

That the Minister for School Education, Early Childhood and Youth establish a position similar to Queensland's 'reputation management' position to provide nationally consistent advice to teachers who are being cyber-bullied by students about the role and processes of the Australian Communications and Media Authority, law enforcement agencies and Internet service providers in facilitating the removal of inappropriate material.

- 9.31 The Association of Independent Schools of South Australia called for a 'readily available, simple and easy to understand explanation of the changing online environment for parents and schools to access'.³³ The Association further commented that,

Pre-service and in-service teachers be given additional support and training on online safety, responsible use of technology and online security and privacy. Many teachers would benefit from greater support and advice to recognise and manage incidents of cyber harm ... A greater suite of resources that can be used within the curriculum to teach students about the social and emotional consequences of Cyberbullying and inappropriate behaviours that are regularly reviewed.³⁴

32 Mr Michael O'Leary, Executive Director, Information and Technologies Branch, Web and Digital Delivery, Department of Education and Training (Qld), *Transcript of Evidence*, 17 March 2011, p. CS82.

33 Association of Independent Schools of South Australia, *Submission 19*, p. 4.

34 Association of Independent Schools of South Australia, *Submission 19*, p. 14.

Mandatory reporting

9.32 Mandatory reporting is required in some situations:

Currently in South Australia, mandatory reporting requirements exist for teachers and others in relation to suspected physical, emotional and sexual abuse and neglect. This could be extended to include online maltreatment or abuse, though this would require extensive consultation and negotiation with states. Any variation to the mandatory reporting laws would need to be supported by adequate funded training of teachers to recognise and report incidents of cyber-harm.³⁵

9.33 The NSW Teachers Federation called for clarification in relation to the decision as to whether or not law enforcement agencies should be contacted:

[The] Federation does nonetheless strongly support clarification of the role and responsibilities of school staff ... The Coroner in the Wildman case also called for revision of “policies so as to provide practical and clear guidance to senior staff as to the circumstances in which police should be called to deal with “...³⁶

9.34 Dr Helen McGrath added that if a system of mandatory reporting is introduced it may ‘do more harm than good’, as ‘you will not even know if the child has a mental health disorder and you do not know if it comes from bullying.’³⁷

Training accreditation

9.35 The Australian Council of Educational Research referred to a study that differentiated between barriers to use of the online environment. It suggested that the lack of teacher competence and confidence, resistance to change and ‘negative attitudes’ were ‘major barriers’ that could be attributed to teachers. Lack of time, lack of effective training and lack of accessibility and technical support could be attributed to schools.³⁸

35 Association of Independent Schools of South Australia, *Submission 19*, p. 16.

36 NSW Teachers Federation, *Submission 73*, p. 3.

37 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS32.

38 Australian Council of Educational Research, *Submission 20*, p. 7.

- 9.36 Teacher accreditation was also discussed by the Australian Psychological Society:

Teachers should be provided with regular training and support about how to appropriately understand and respond to cyber risks. This includes the capacity to build in cyber-safety as part of the broader curriculum, encouraging pro-social behaviours as part of general classroom management techniques and more specifically being able to respond to inappropriate internet use.³⁹

- 9.37 Such a program would be more effective if it could be provided online, and if it was open to both teachers and students.

Recommendation 19

That the Minister for School Education, Early Childhood and Youth and the Minister for Broadband, Communications and the Digital Economy investigate funding a national, online training program for teachers and students that addresses bullying and cyber-bullying, and is validated by national accreditation.

Whole-of-school community

- 10.1 The promotion of cyber-safety is inescapably a broad community issue. The need for a whole-of-school approach is demonstrated by the assertion from Principals Australia that schools have only 30 percent influence over young people's education.¹
- 10.2 The Australian Council of Educational Research also supported the idea of a multi-layered approach, involving schools, parents/carers and the community, to manage online safety effectively. The central role of this approach is to improve the confidence of teachers to use the Internet; to model appropriate behaviour, and to require school policies in cyber-safety, and safety generally.²
- 10.3 Research from the American Online Safety and Technology Working Group reported that a multi-layered approach is required from schools, parents/carers and the community to establish accepted online behaviour, and that young people need to be taught digital literacy skills.³
- 10.4 An example of a whole-of-school approach is the NSW Government implementation of *MindMatters*: a whole-of-school approach to mental health promotion. It includes modules to foster the development of social and emotional skills, and encourages effective home, school and

1 Mr Jeremy Hurley, Manager, National Education Agenda, Principals Australia, *Transcript of Evidence*, 11 June 2010, p. CS9.

2 Australian Council of Educational Research: *Submission 20*, pp. 7-8; Dr Gerald White, Principal Research Fellow, *Transcript of Evidence*, 9 December 2010, pp. CS41, 46-48, 50. See also Associate Professor Marilyn Campbell: School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS32; Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS9; Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS31.

3 Australian Council of Educational Research, *Submission 20*, pp. 6-7.

community partnerships. Since 2007, cyber-safety has been a focus of the bullying and harassment arm of the project.⁴

- 10.5 While it is not the only such program that has been introduced in Australia, the Australian Council for Educational Research was one of a number of organisations that endorsed the value of the *Cyber-safety and Well-Being Initiative (eSmart Schools Framework, hereafter eSmart)* undertaken by the Alannah and Madeline Foundation. This is an initiative for cultural change and community-based intervention, aimed at creating environments where it is easy and normal for individuals to make smart choices when using technology. *eSmart* focuses on a 'whole-school' approach to cyber-safety problems, and provides a suite of tools to assist schools; it is a culture and behaviour change model targeted at the whole school community and, as such, is not a one-off lesson, unit of work, program or policy that sits in isolation from the day-to-day business of schools.⁵
- 10.6 It was argued that, for it to be effective, a whole-of-school approach had to involve teachers, including those in the pre-service phase, support staff, administrators and parents/carers/carers. This meant professional development, time release and workload management for school staff, especially teachers.⁶

Parents/carers

- 10.7 A member of the ACT Safe Schools Taskforce was quoted as observing that parents/carers must be involved 'at all parts of the journey':

Cybersafety isn't like teaching your child to ride a bike. It's not a skill that you had when you were younger and that you can pass on to your child. It's an area where things are changing so much, so quickly, that as a parent you need constant reiteration and updating and strategies to protect our children.⁷

4 NSW Government, *Submission 94*, p. 23; Mr Jeremy Hurley, Manager, National Educational Agenda, Principals Australia, *Transcript of Evidence*, 11 June 2010, p. CS8.

5 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. CS7.

6 Ms Catherine Davis, Federal Women's Officer, Australian Education Union, *Transcript of Evidence*, 30 June 2010, p. 32.

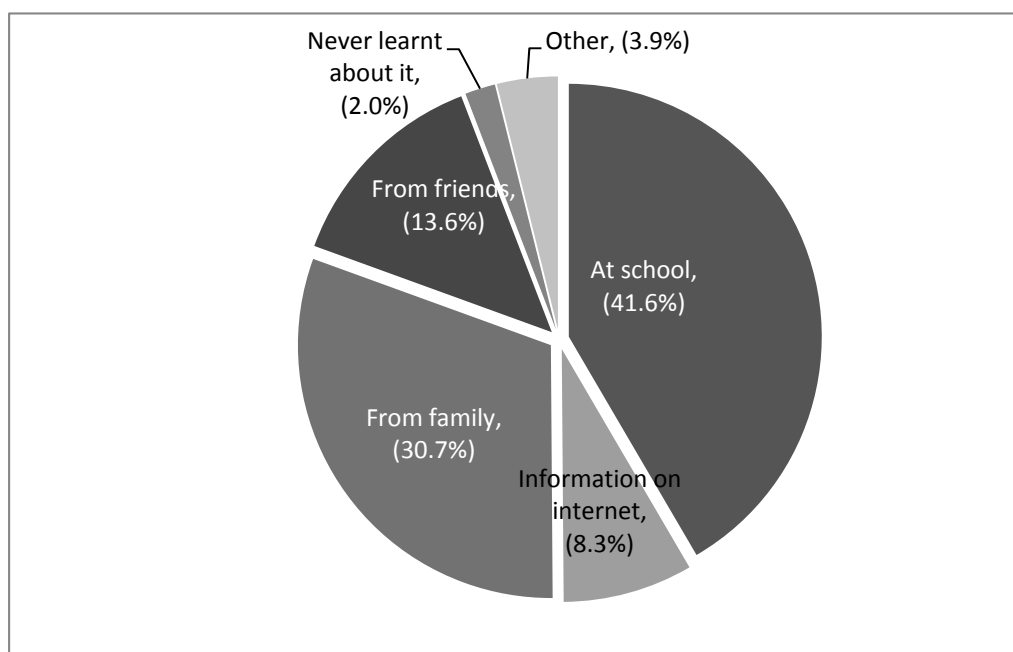
7 See Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS37.

10.8 The Australian Parents Council believed that the element missing from the efforts made to develop consistent 'whole school' approaches to cyber-safety appeared to be the systematic engagement of parents/carers. This was despite the fact that their engagement is essential to those efforts.⁸ Similarly, the Alannah and Madeline Foundation advised that:

Parents, and to a lesser extent teachers, feel overwhelmed and ignorant about what's going on in social networking sites, chat rooms, online gaming and other areas in cyberspace. Teachers believe parents should take a lot more responsibility for their children's behaviour (both online and offline). Parents (and teachers) would like to know more about the virtual spaces young people inhabit, but don't know where to start. Both groups believe their ignorance has led to an unhealthy power shift, so that young people are too easily able to operate 'under the radar', or outside the usual boundaries governing their behaviour.⁹

10.9 The role that parents play in the cyber-safety education of their children cannot be understated. Not only does the family unit play an important educative role, but also a key supportive role when young people face cyber-safety risks and dangers. Figures 10.1 to 10.3 present the results from the Committee's *Are you safe?* survey and provide details of this relationship.

Figure 10.1 Where did you learn about cyber-safety?



8 Australian Parents Council, *Submission 10*, p. 4.

9 Alannah and Madeline Foundation, *Submission 22*, p. 18

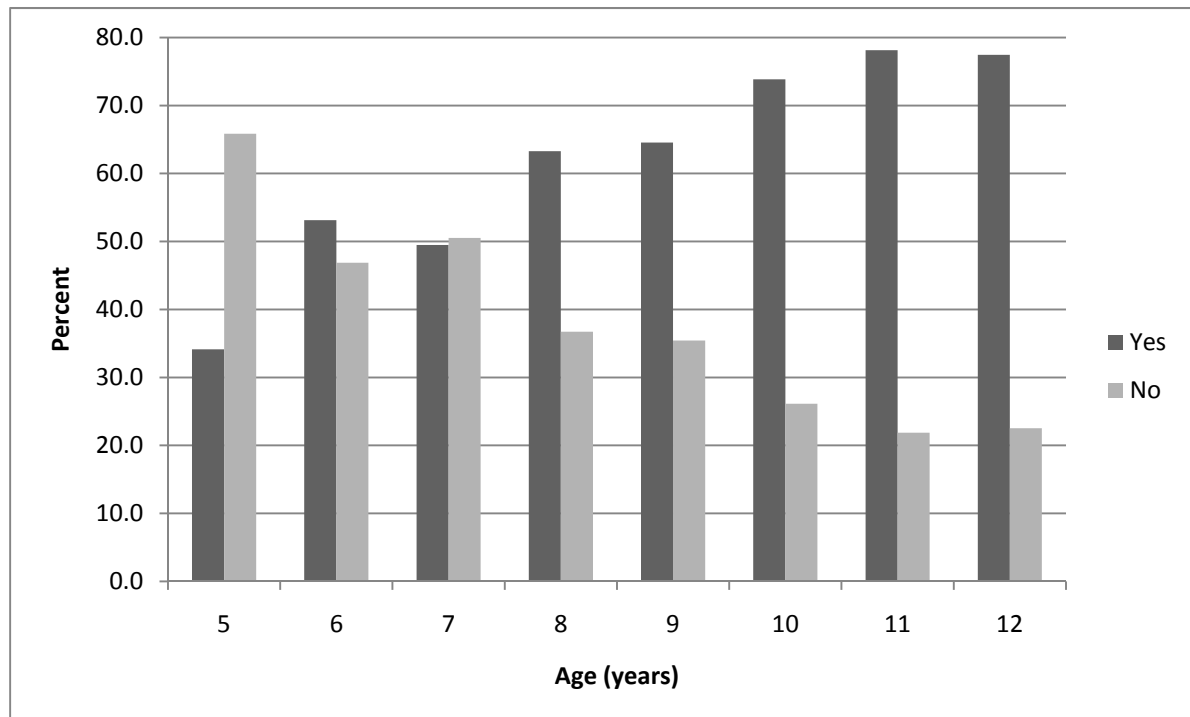
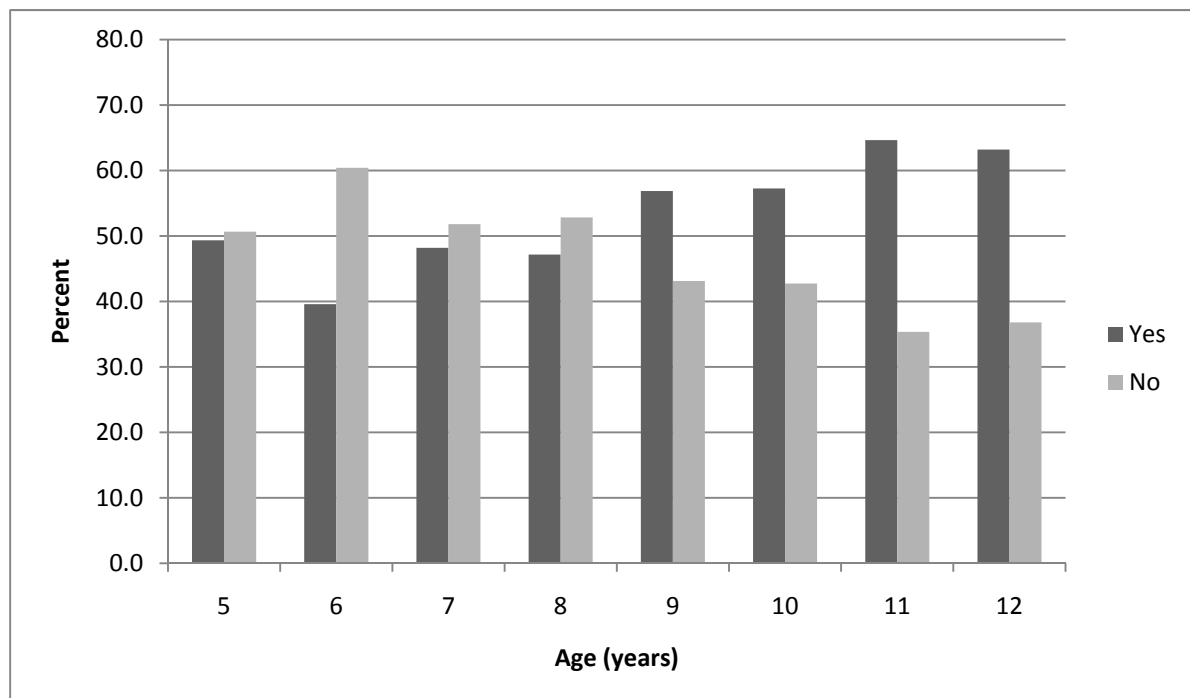
Figure 10.2a Do you talk about cyber-safety with your parents? (*Female aged 12 years and younger*)Figure 10.2b Do you talk about cyber-safety with your parents? (*Male aged 12 years and younger*)

Table 10.1 How frequently does your family talk about cyber-safety?

		Never		Yes, when I ask		Yes, sometimes		Yes, frequently		Total
Sex		%	#	%	#	%	#	%	#	#
13 Years	M	17.7	335	23.9	451	42.4	802	16.0	302	1890
	F	9.2	225	21.3	522	45.2	1111	24.3	598	2456
14 Years	M	23.9	286	22.0	355	40.3	649	13.8	222	1612
	F	10.6	210	19.7	390	48.6	964	21.1	418	1982
15 Years	M	28.3	337	20.0	238	38.9	463	12.8	153	1191
	F	14.3	196	20.2	278	45.3	623	20.2	277	1374
16 Years	M	35.1	283	16.9	136	37.9	306	10.2	82	807
	F	18.2	182	18.8	188	47.8	477	15.1	151	998
17 Years	M	40.5	160	14.2	56	34.4	136	10.9	43	395
	F	23.2	132	17.3	98	45.1	256	14.4	82	568
18 Years	M	39.7	124	15.7	49	29.5	92	15.1	47	312
	F	40.5	105	15.1	39	33.2	86	11.2	29	259

Figure 10.3a How frequently does your family talk about cyber-safety? (*Female aged 13 years and over*)

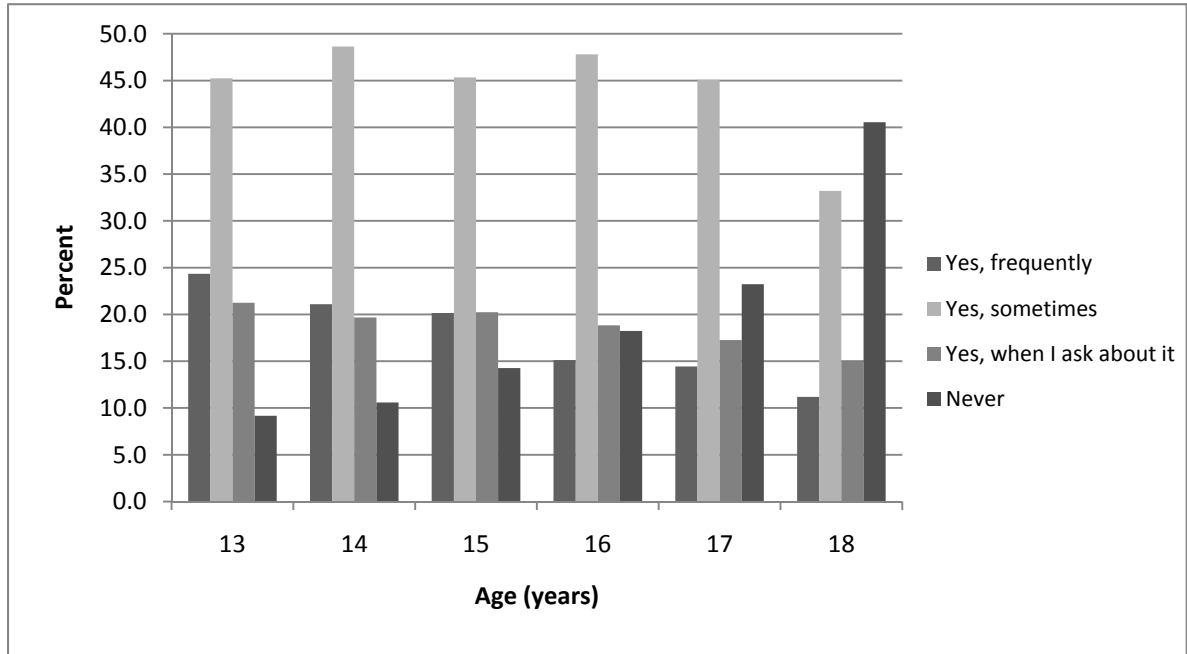
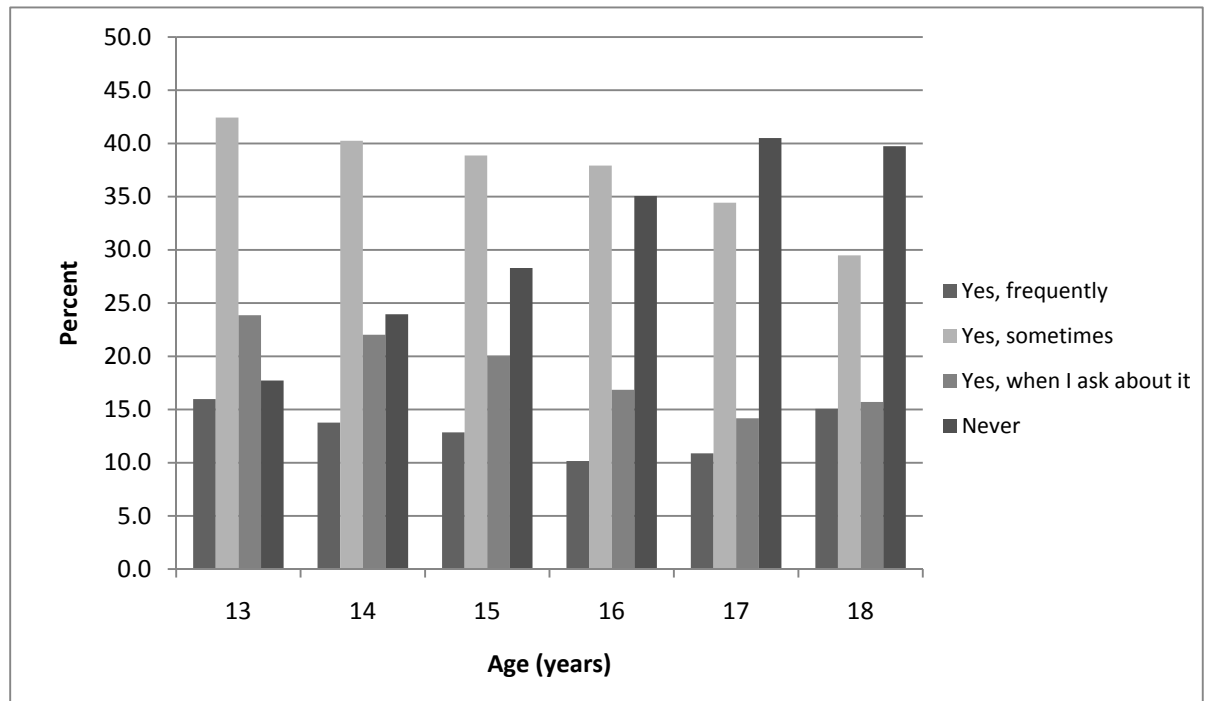


Figure 10.3b How frequently does your family talk about cyber-safety? (*Male aged 13 years and over*)



Information for parents/carers

10.10 The Family Online Safety Institute commented that:

There has never been a time when so many resources have been available for parents, grandparents, teachers, and care-givers to provide protection from online risks. All of the major operating systems and search engines provide family safety settings and mobile operators, social networks, and Internet Service Providers offer tools and settings to help protect families.¹⁰

10.11 The Australian Communications and Media Authority (ACMA) has released *the Cybersmart parents: connecting parents to cybersafety resources*. Dr Helen McGrath commented on the quality of its materials:

The ACMA materials are brilliant. I cannot recommend them highly enough. There are very few resources and presentations that you hear rave reviews about wherever you go. The ACMA materials are raved about. They are terrific to recommend to parents.¹¹

10.12 The ACT Council of P&C Associations believe that parents/carers know that information is available but not necessarily aware of where to go to find it and called for:

the government advertises the ACMA website better to parents/carers as well as other resources and their potential use. It is recommended that television and/or radio advertisement is used, as well as advertising through schools.¹²

10.13 The Victorian Office of the Child Safety Commissioner, however, expressed concern that many of the resources available for parents/carers,

require a high degree of literacy skills and an understanding of English. This inquiry provides an opportunity to explore which parents/carers and carers are not able to use these resources and to make recommendations about how to more effectively empower such parents/carers and carers to support their children.¹³

10 Family Online Safety Institute, *Submission 38*, p. 17.

11 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS19.

12 ACT Council of P&C Associations, *Submission 41*, p. 8.

13 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 5.

- 10.14 The Australian Parents Council emphasised that there is a plethora of information available:

if you were to google 'cybersafety', you would be daunted by the range of information. Parents do not know how to be discretionary about what is worthwhile, what is serious and what is not.¹⁴

- 10.15 The Queensland Secondary Principals Association has found that as 'more and more students are certainly online, more and more parents are certainly online'.¹⁵ Parents/carers, however, use these technologies in vastly different ways from their children, and these differences can cause concern and divisions among families:

Young people used technologies much more holistically; to communicate, learn, socialise, play, research, do homework, and in fact, their on-line life blended seamlessly with their offline life. Parents felt a lack of control because they did not fully understand how their children used technologies and cited threat from predators as their greatest fear ... Children and young people on the other hand were dismissive of their parents' and teachers' fears and cited their biggest issues as slow internet and viruses.¹⁶

- 10.16 Brisbane Catholic Education requires that parents attend cyber-safety information sessions before laptops are distributed under the Digital Education Revolution.¹⁷ These strategies can be effective, as children often want to engage with their parents:

One of the things we know from research in Europe is that children and young people actually want to discuss this issue with their parents but they are put off from doing that because their parents do not have the technological savviness to have that discussion.¹⁸

- 10.17 The NSW Parent's Council added that:

Even though there are numerous websites full of advice to assist parents in ensuring safety along with the obvious benefits of ICT,

14 Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS6.

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

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

17 Ms Anita Smith, Senior Education Officer, Brisbane Catholic Education, *Transcript of Evidence*, 17 March 2011, p. CS24.

18 Mr John Dalglish, Manager, Strategy and Research, BoysTown, *Transcript of Evidence*, 17 March 2011, p. CS15.

this advice is often difficult to put into place and to continue to monitor.¹⁹

10.18 The Alannah and Madeline Foundation is of the view that:

Children and young people on the other hand were dismissive of their parents' and teachers' fears and cited their biggest issues as slow internet and viruses. However, further probing revealed that nearly all young people interviewed had experienced or witnessed cyberbullying and considered it common and extremely unpleasant.²⁰

10.19 The Alannah and Madeline Foundation also believed that:

Young people are less apt to share or disclose with parents who don't appear to understand or care what their children are doing online. Young people can, however, have a key role in educating parents about their lived online experience – one that, it appears, they are keen to assume.²¹

10.20 Parents/carers should also be made aware of the range of available resources that can assist them to manage their children's internet use.²² The Foundation considers that programs should encourage the need to have clear understandings and agreements within the family about acceptable internet and mobile phone usage and to maintain open communication with their children about issues arising.²³

Many children and young people are reluctant to tell their parents about cyberbullying and other forms of online abuse fearing that access to their social networks will be removed. Parents need to be supported to communicate effectively with their children on mobile phone and internet use (gaming, chat rooms, messages, keeping personal details private, voice masking, responding to unwelcome attention, combating addiction).²⁴

10.21 While schools have a role in educating students about cyber-safety, this must be balanced against the main purposes of schooling, the role of

19 NSW Parent's Council, *Submission 43*, p. 3.

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

21 Alannah and Madeline Foundation, *Submission 22*, p. 10.

22 Alannah and Madeline Foundation, *Submission 22*, p. 11.

23 Alannah and Madeline Foundation, *Submission 22*, p. 11.

24 Alannah and Madeline Foundation, *Submission 22*, p. 11.

parents/carers and the responsibility of the community.²⁵ Parents/carers are the primary educators of children, and they:²⁶

need to educate themselves on how to protect their children, and to have greater access to resources and experts to assist with this education. Many school libraries are already working within their schools to offer sessions to parents, and public libraries are reaching out not only to parents but also to the whole community.²⁷

- 10.22 Childnet has developed the *Know IT All for Parents* resource which is interactive and provided available in different formats and languages which has been provided to two million parents in the United Kingdom as of June 2010.²⁸ Similarly, ACMA has now launched the new parent interactive resources in the top five non-English languages: Chinese, Greek, Italian, Vietnamese and Arabic.²⁹

Cyber safety education and training needs to start with parents of preschool aged children ... It needs to be undertaken at a time when parents still might know more about the online world than their child does ... It needs to be part of the requirement of educating children in Australia and be attended by at least one parent of all pre-school aged and school aged children.³⁰

- 10.23 The Australian Parents Council explained that, if material is not in a format appropriate for parents, these resources may not be read:

all too often with initiatives such as this national initiative organisations and government try to do things to and for parents instead of taking an approach of doing it with them. There are often attempts made to communicate with parents which, with all the best intent, try to get a message across but all too often it is not in language that is accessible to parents. Whilst you do not need to talk down to parents, it is a very difficult art to frame stuff up in a language that is accessible to parents across the board without

25 Australian Secondary Principals' Association, *Submission 33*, p. 2.

26 Australian Parents Council, *Submission 10*, p. 1.

27 Australian Library and Information Association, *Submission 16*, p. 12.

28 Childnet International, *Submission 18*, p. 7.

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

30 Name withheld, *Submission 140*, p. 2.

being either patronising or talking at such a simple level that you offend people.³¹

- 10.24 Evidence provided to the Inquiry by ACMA drew attention to the range of its resources that could assist parents/carers to manage their children's internet use.

At the present time we have parents who themselves have had an unhappy or unsatisfactory education, who are fearful of being engaged or unable to engage, who feel disempowered or not valued ... In many ways schools operate very comfortably in middle-class communities and do not serve the needs and interests of those who have not had positive education experiences.³²

- 10.25 The Victorian Office of the Child Safety Commissioner would also like to see work done in relation to collaboration between those with expertise in information and communications technology (ICT) and those caring for vulnerable children to develop strategies to meet the needs of those children.³³

for some parents and caregivers it may be an issue of ignorance and naivety about their child's safety on the internet; however that for most parents and caregivers it was purely a matter of not knowing how to approach the topic ... parents and caregivers need to be educated about the importance of, and "how to", have conversations with their kids about cyber safety.³⁴

- 10.26 The following comments were made by respondents to the Committee's *Are you safe?* survey in response to the ways to improve the cyber-safety of their parents/carers:

parents react very differently to the way teachers would, often dismissing the idea that the bullying is a real issue but a threatening email is immensely scary especially when the person involved had never really felt that anything had come between them face to face. Also it takes a while for young people to realise what a true friend is and build up the courage to cut their losses and join a new friend group where they are accepted (Female aged 17).

31 Mr Ian Dalton, Executive Director, Australian Parents Council, *Transcript of Evidence*, 20 April 2011, p. CS33.

32 Ms Dianne Butland, Executive Member, State Council, Federation of Parents and Citizens Associations of New South Wales, *Transcript of Evidence*, 30 June 2010, pp. CS 17-18.

33 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 5.

34 Centre for Children and Young People, *Submission 31*, p. 2.

Children are heavily influenced by their parents. Educate the parents first and most of all make sure they are being good role models for their kids (Female aged 15).

I would feel safer if I knew my parents could see more that goes on. I tell them but sometimes people put real bad stuff (Female aged 15).

parent education that is detailed enough to include the benefits of social networking to encourage them to get involved as well (Female aged 17).

Parents being more responsible with chn and ICT (Female aged 17).

Parents checking up on what their children are saying online (Female aged 13).

Parents monitoring their children more online and giving them good Internet habits and understanding from a young age (Female aged 16).

parents need to be aware that some of their children are the bully/a nasty child and these children can manipulate them (Female aged 16).

Available technologies

- 10.27 The NSW Secondary Principals Council would like parents/carers to be provided with the tools to manage the online environment at home:

where less rigid filters and controls are often in place.

www.cybersmart.gov.au is a good start but needs wider

advertising to parents and further development and expansion³⁵

- 10.28 There are many free filtering options. Between 40 and 50 percent of parents/carers already use some type of filtering, indicating a level of awareness and adoption.³⁶

- 10.29 The Australian Psychological Society would like to see the establishment of an information and/or referral service to provide advice on best practice technology such as internet filtering systems.³⁷ Similarly, ninemsn commented:

Parents need to be adequately informed as to what products are available and how best to configure and use them in a way most appropriate for their family. ninemsn believes this presents a

35 NSW Secondary Principals Council, *Submission 32*, p. 1.

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

37 Australian Psychological Society, *Submission 90*, p. 25.

valuable opportunity for industry and government to work collaboratively on promoting the availability of these tools. There are some helpful examples of best practice of this cooperative approach emerging from the US and UK.³⁸

10.30 Dr Gerald White commented that it is 'not hard to engage parents in relation to technological devices' and, if you require parents to sign a user access policy, they will be engaged.³⁹ The use of user access agreements provides an opportunity to encourage parents to attend cyber-safety information session.

10.31 Netbox Blue advised that:

Most of these tools are relatively simple to deploy. The question is: which are the right tools that parents/carers should be using? The idea of accrediting tools through things like the IIA and the family friendly filter accreditation I think is really key, so that parents/carers know which tools are going to meet their needs and which tools are not. Getting that message across is perhaps the most important thing. You can do it via expensive advertising on TV or whatever or it could be as simple as sticking leaflets in schoolkids' bags for them to take home.⁴⁰

10.32 Some parents/carers may not worry in the belief that schools will arrange cyber-safety for their young people and are therefore not engaged. They may have an antipathy towards the school, or they do not see that they have a role:

Once you can start to talk to parents/carers and tell them that they have a role and the way that they can fulfil that role – some simple things that they can do to actively engage – the results are quite astounding.⁴¹

10.33 Some parents/carers trust their children and do not see a need for this approach.⁴²

38 ninemsn, *Submission 91*, p. 5.

39 Dr Gerald White, Principal Research Fellow, Australian Council of Educational Research, *Transcript of Evidence*, 9 December 2010, p. CS48.

40 Mr John Pitcher, Netbox Blue, *Transcript of Evidence*, 8 July 2010, pp. CS34.

41 Mr Ian Dalton, Executive Director, Australian Parents Council, *Transcript of Evidence*, 20 April 2011, pp. CS34-35.

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

Parents tend to assume that their children know what they are doing and to think that they are monitoring their children if they have the computer in the same room as they are currently in, but they do not realise that children can downsize the screen if they are doing something wrong and that they might panic and not bring to their parents' attention that something has gone wrong.⁴³

10.34 However, BraveHearts made the point that:

...while it is notionally true that parents and carers must take ultimate responsibility for educating and protecting their children, it is also true that the internet and new communication technologies are becoming increasingly foreign to many parents thus reducing their ability to protect their children. The reality is that more often than not, children know more about the internet and mobile phone technologies than adults do. Continuing calls for parents to educate themselves are falling on the predominately 'out of their depth', baffled and frightened ears of parents and carers.⁴⁴

10.35 The Association of Children's Welfare Agencies stated that parents and carers need access to information to enable them to make informed decisions about cyber-safety issues and this could entail:

- Awareness raising strategies;
- Resources and information on prevalent and emerging cyber-safety issues;
- Resources on how to approach and discuss these issues with children and young people; and
- Information on interventions and supports.⁴⁵

10.36 The desirable outcomes are empowered parents/carers and families that:

- Are able to understand cyber-safety issues and the impact that it has on their child or young person;
- Feel comfortable enough to discuss cyber-safety issues with their child or young person; and

43 Ms Lesley-Anne Ey, Executive Committee Member, Australian Council on Children and the Media, *Transcript of Evidence*, 3 February 2011, p. CS50.

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

45 Association of Children's Welfare Agencies, *Submission 35*, p. 3.

- Know what actions to take or where to go to for more information or support.⁴⁶

10.37 The Family Online Safety Institute emphasised that:

Parents must learn about the risks themselves and then help their children learn how to cope with them ... There is no silver bullet to protect children from the risks of digital media, only a combination of education, awareness, tools, and rules will help guard children from harmful content and empower them to act responsibly online.⁴⁷

10.38 Ongoing education for parents/carers is important to keep them up to date:

The other comment that I have that I think is important is that one-offs do not work, so the learning for parents and the opportunities have to be regular, they have got to be spaced and they have got to be purposeful. The parents are more likely to engage with their school or their child's teacher and indeed the child's learning if they can see a role for themselves. It is really important that the approach is one of partnering, not one of being the expert.⁴⁸

10.39 The ACT Council of P&C Associations suggested further measures to assist parents in keeping up with technology and current trends.⁴⁹ They may not be aware of the resources available and an advertising campaign may increase the level of awareness.⁵⁰

ABS statistics found that most parents/carers were taking steps to protect their child/ren online. 88 percent of ACT families educated their child/ren about safe and appropriate use of the internet, 58 percent of parents/carers had installed content filters while 93 percent said they supervised and monitored their child/ren's use of the internet.⁵¹

46 Association of Children's Welfare Agencies, *Submission 35*, p. 3.

47 Family Online Safety Institute, *Submission 38*, p. 15.

48 Ms Liz Banks, Acting Deputy Secretary, Department of Education, Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS3.

49 ACT Council of P&C Associations, *Submission 41*, p. 3.

50 ACT Council of P&C Associations, *Submission 41*, p. 3.

51 ACT Council of P&C Associations, *Submission 41*, p. 6, citing Australian Bureau of Statistics, 2010, Feature Article 2: 'Children and Cyber-safety' *In fACT: Statistical information on the ACT and region*, No 1308.8, Canberra, ACT.

- 10.40 The Council also suggested annual information sessions for parents to keep up to date.⁵²

... many concerns were raised about the potential threat of cyber-bullying, identity theft, downloading a virus and the risks involved with accessing SNS or chat forums and the potential for their child to talk to someone who is different to who they say they are. Parents seemed to be less concerned about the potential for their child to access sites that encouraged illegal or harmful behaviour or accessing inappropriate material. Interestingly, the most common issue reported by children who used the internet was accessing inappropriate material.⁵³

- 10.41 At the beginning of National Cybersecurity Awareness Week, in June 2011, the Minister for Broadband, Communications and the Digital Economy, Senator the Hon Stephen Conroy, noted that members of the newly formed Teachers' and Parents' Advisory Group on Cybersafety are involved in consultations on how to keep young Australians safe online.⁵⁴

Household media rules

- 10.42 The Alannah and Madeline Foundation is of the view that programs should encourage the need to have clear understandings and agreements within the family about acceptable internet and mobile phone usage and to maintain open communication with their children about issues arising.⁵⁵

Parents need support in engaging with online media such as Facebook, Skype and Twitter right throughout the school years not just voluntary sessions provided by the local council and youth service.⁵⁶

- 10.43 The Communications Law Centre called for:

52 ACT Council of P&C Associations, *Submission 41*, p. 7.

53 ACT Council of P&C Associations, *Submission 41*, p. 7, citing Australian Bureau of Statistics (2010) Feature Article 2: 'Children and Cyber-safety' In *fACT: Statistical information on the ACT and region*, No 1308.8, Canberra, ACT.

54 See www.minister.dbcde.gov.au/media/media_releases/2011/191 of 2 June 2011.

55 Alannah and Madeline Foundation, *Submission 22*, p. 11.

56 Name withheld, *Submission 140*, p. 2.

Educational campaigns specifically in respect of social networking and communications tools available over the internet should be offered to parents and carers of children.⁵⁷

10.44 The Australian Council on Children and the Media commented that:

parents just don't know where to draw the line'. It is not that you do not care or that you do not know what is going on, but you can feel that tug in two directions. You want your child to be modern, to have access to all the best modern technology and to be up with all the information like all their friends are, but you do not want them to be harmed, and finding that balance is something that is really quite difficult. Parents need the best support we can give them, and that really needs to come through information but also through that regulatory back stop – that idea of, 'No, there are some areas that we just do not go in as a society, because we think that children are just far too important and it is not fair or realistic to put all of the burden on parents.⁵⁸

10.45 The Family Online Safety Institute believed that parents/carers should encourage household media rules which set limits on the time spent online and allowable content.⁵⁹

Parents should understand what they are giving permission to when allowing children to access internet sites from Club Penguin to Facebook and everything in between.⁶⁰

10.46 The Communications Law Centre called for additional services :

educating parents on the methods in which children interact, socialise and network over the internet and mobile phones to assist them more effectively to discuss cyber-bullying issues with their children.⁶¹

10.47 A Microsoft Australia survey found that:

Alarmingly, one fifth of all Australian parents surveyed had caught their children looking at inappropriate material online, almost one third had found their children chatting to strangers, 36 percent had caught their kids downloading software without

57 Communications Law Centre, *Submission 63*, p. 4.

58 Ms Lesley-Anne Ey, Executive Committee Member, Australian Council on Children and the Media, *Transcript of Evidence*, 3 February 2011, p. CS49.

59 Family Online Safety Institute, *Submission 38*, p. 15.

60 Name withheld, *Submission 140*, p. 2.

61 Communications Law Centre, *Submission 63*, p. 1.

permission and another 12 percent had found their children handing over personal details.⁶²

- 10.48 In setting the media rules, this will open discussions on what young people are doing online.⁶³ The NSW Primary Principal's Association noted:

The home environment is often a cause for concern. Parents may not be aware of safeguards that can be put in place. These include computers being placed in areas where parents can provide direct supervision, filters such as Net Nanny being installed on home computers, time limits being set related to computer/ internet use, regular open communication between children and parents regarding inappropriate use of the internet and specific issues related to social networking sites.⁶⁴

- 10.49 Parents/carers indicated to the ACT Council of P&C Associations that they 'feel they lack the ability to successfully control their child's online behaviour and activity and believe that their efforts are mostly ineffective.'⁶⁵ The Council suggested that:

parents/carers be provided with easy to understand user guides on sites that are popular among children. For example, parents/carers should be provided access to a user guide on how to change your child's privacy settings on Facebook, how to make a complaint about inappropriate or offensive material on sites such as Facebook or suggestions of appropriate sites that are safe for children to stream video content, as well as other important tips and advice about safe sites and use of a variety of internet sites that are popular among children.⁶⁶

- 10.50 Some information is already available. For example, the Australian Direct Marketing Association provides the following tips for parents:

- Know what your children are doing online – make sure they know how to stay safe and encourage them to tell you if they come across anything suspicious or if anybody says or does something that makes them feel uncomfortable or threatened;
- Get to know the technologies your children are using;

62 Microsoft Australia, *Submission 87*, p. 7.

63 Family Online Safety Institute, *Submission 38*, p. 16.

64 NSW Primary Principal's Association Inc, *Submission 69*, p. 2

65 ACT Council of P&C Associations, *Submission 41*, p. 6.

66 ACT Council of P&C Associations, *Submission 41*, p. 7.

- Discuss the risks with your children and agree on some rules for internet use;
 - Tell your children if they are uncomfortable talking to you they can contact the *Cybersmart Online Helpline* (Kids Helpline) www.cybersmart.gov.au;
 - Place the computer in a family area of the home;
 - Install an internet content filter;
 - Make sure your children know not to share personal information or photos;
 - Report inappropriate, harmful or criminal activities that occur online or via a mobile device to www.thinkuknow.org.au; and
 - Report offensive content to ACMA.⁶⁷
- 10.51 Vodafone also have a digital parenting guides which include how to set up your Facebook privacy settings in four easy steps along with tips on what to do which is a model which could be adapted here.⁶⁸

Involving parents/carers

- 10.52 The ACT Council of P&C Associations called for greater collaboration between schools and parents better to educate parents on how to protect their children online.⁶⁹
- 10.53 ACMA's *Click and Connect* report found that,
- Parents/carers tend to re-enforce the basic internet safety messages with a stronger focus on the issue of predators rather than the broader range of safety issues. Both schools and parents/carers currently appear to work in isolation in informing children about cybersafety, although parents/carers did show interest in a more collaborative approach with schools.⁷⁰

- 10.54 The Tasmanian Department of Education advised:

67 Australian Direct Marketing Association, *Submission 36*, p. 8.

68 Ms Andree Wright, Acting General Manager, Consumer, Content and Citizen Division, Australian Communications Management Authority, *Transcript of Evidence*, 3 March 2011, p. CS15.

69 ACT Council of P&C Associations, *Submission 41*, p. 8.

70 Australian Communications and Media Authority, 2009, *Click and Connect: Young Australians' Use of Online Social Media*, Part 1, p. 10.

... if the child wants the parent to be there they are more likely to come along and in that way you can reach out to some of those parents who would be most at risk in terms of not being able to support their child through acceptable use of technologies. That is the same pattern across a range of issues within education ... which is that being inclusive and supportive to help parents rather than just a big stick or mandating approach is the way to go.⁷¹

- 10.55 The capacity of the school to involve parents/carers may reflect the inherent capabilities of the principals and teachers, rather than on training and support policies.⁷² Some parents/carers would also like to have a greater input:

I recently received a letter requesting my children to fill in an online questionnaire regarding cyber bullying. As parents, we are generally the ones that are required to make the rules and enforce them with relation to our children's online internet usage. I would therefore think that the necessity of having a questionnaire seeking parents/carers views and concerns on this matter would be of equal importance to that of our children's, as we are ultimately the people charged with looking after our children's wellbeing in this respect.⁷³

- 10.56 The Australian Parents Council has found that cyber-safety nights for parents/carers are often very popular, indicating that this is a significant area of concern for them.⁷⁴

Parents are key to preventing cyber-bullying and to addressing it when their children are victims or perpetrators. Many parents/carers miscalculate the amount of time their child spends on the Internet, or are simply unaware of their child's computer usage.⁷⁵

- 10.57 Some schools in America use parent-teacher interviews to set goals and agree on the role of the parent in achieving these goals.

71 Ms Liz Banks, Acting Deputy Secretary, Department of Education, Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS3.

72 Mr Ian Dalton, Executive Director, Australian Parents Council, *Transcript of Evidence*, 20 April 2011, p. CS39.

73 Ms Annette Atkins, *Submission 134*, p. 1.

74 Mr Ian Dalton, Executive Director, Australian Parents Council, *Transcript of Evidence*, 20 April 2011, p. CS37.

75 Simon Fraser University, *Submission 55*, p. 4.

... they are actually engaging with their children's education and establishing an environment of support for their children's learning. They are more than willing to be a part of that and love being a part of it.⁷⁶

- 10.58 Too often, it believed, governments tried to do things to and for parents/carers, instead of doing these things *with* them. While it is difficult to frame communications at appropriate levels, often material is presented in language that is not accessible.⁷⁷
- 10.59 The Australian Parents Council made the point that parental engagement: is not about parents being at the school. You can express that engagement in so many other ways: simply by being interested, by reading the newsletter and by communicating in other ways. We need to bear that in mind when we are looking at an approach. It does not mean being on the premises.⁷⁸
- 10.60 There are some parents/carers who will not come to schools, especially to be informed about technological matters or cyber-safety. This can be because they do not have time, or because they lack knowledge or confidence about the online environment.
- 10.61 Parents/carers can be involved in other ways:
- The New South Wales education department sends around cybertips for parents for the holidays, which I think is a terrific direction as well. There are a few things they can watch and keep an eye on in a positive light.
- SuperClubs Australia also does an interesting thing. That is a private organisation. It is something the Victorian education department adopts. They get the students to interview their parents to find out how much the parents know about cybersafety. This is a primary aged direction to tap into what their parents know and educate their parents as they go. I think that is another clever way of doing it. Again it is going to be the sum of many small moves with parents.⁷⁹

76 Mr Ian Dalton, Executive Director, Australian Parents Council, *Transcript of Evidence*, 20 April 2011, p. CS35.

77 Mr Ian Dalton, Executive Director, Australian Parents Council, *Transcript of Evidence*, 20 April 2011, p. CS33.

78 Ms Kate Lyttle, Secretary, Australian Parents Council, *Transcript of Evidence*, 30 June 2010, p. CS18.

79 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS19.

10.62 The Australian Parents Council suggested that national groups of parents/carers are in a position to tap the significant potential for greater engagement in cyber-safety issues, through:

- conducting a national survey to assist in understanding levels of awareness about cyber-safety risks;
- discovering cyber-safety strategies they are adopting in their homes;
- development of a leaflet for parents/carers incorporating principles of digital citizenship and best practice; and
- a national meeting of parents'/carers' groups to design and distribute a charter as a guide to use of the Internet and digital platforms.⁸⁰

10.63 The Department of Broadband, Communications and the Digital Economy referred to a study that found that about 70 percent of parents/carers are very concerned or fairly concerned about cybersafety.⁸¹ Simon Fraser University reported no correlation between the extent of supervision and the parents' degree of technological knowledge and level of parental concern about cyber-bullying.⁸² Further, a survey by Microsoft Australia found that:

two thirds of Australian parents/carers were concerned about the safety of their kids online, and more than 60 percent of parents/carers allowed their children to surf the net unsupervised and unrestricted at home.⁸³

10.64 It also found that:

- More than two thirds of Australian parents/carers admitted they knew only a few of their children's online friends;
 - Another 11 percent admitted they were totally in the dark, knowing none of their children's online friends;
 - Only half of all parents/carers (58 percent) housed the computer in a public area of the home;
 - 20 percent of parents/carers had not discussed online safety with their children;
 - More than 60 percent of parents/carers were aware their computer had parental control software available – yet less than
-

80 Australian Parents Council, *Submission 10*, p. 5.

81 Mr Simon Cordina, Assistant Secretary, Cyber-safety and Trade Branch, Digital Economy Strategy Division, Department of Broadband, Communications and the Digital Economy *Transcript of Evidence*, 3 March 2011, p. CS18.

82 Simon Fraser University, *Submission 55*, p. 11.

83 Microsoft Australia, *Submission 87*, p. 7.

a third of all parents/carers monitored their children's activity online.⁸⁴

10.65 The Australian Psychological Society suggested that:

... parents/carers are educated and supported to use an internet filter (without relying solely on this strategy), to discuss and use the internet with children and encourage them to evaluate critically information accessed online, to monitor and supervise their child's internet/phone use, and to involve young people in deciding appropriate limits and agreeing on age appropriate consequences.⁸⁵

Conditions of use agreements

10.66 The Australian Parents Council expressed concerns about the level of awareness of the 95 percent of Tasmanian parents signing 'conditions of use' forms for their young people, and what that might mean for their responsibilities as parents. Research was needed about whether they understand what they signed, and why the other 5 percent do not sign these forms.⁸⁶

10.67 The Alannah and Madeline Foundation believed that:

Australian schools also have much ground to make up in producing robust acceptable use policies that reach beyond the school gate to include parents and the wider community.⁸⁷

10.68 Netbox Blue recommend promoting and enforcing 'Acceptable Use' policies:

- The creation of an acceptable policy framework and its communication to all stakeholders - students, teachers, parents and carers;
- Education for all stakeholders on minimising known risks, or dealing with them if presented with a situation that places them at risk, focusing on working with students, teachers, parents and carers;

84 Microsoft Australia, *Submission 87*, p. 7.

85 Australian Psychological Society, *Submission 90*, p. 4.

86 Mr Ian Dalton, Executive Director, Australian Parents Council, *Transcript of Evidence*, 20 April 2011, p. CS38.

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

- Technology enforcement – in and outside the school network on all school owned equipment; and
- Regular reviews of attempts to breach such policy frameworks to improve education and to manage individual behavioural issues.⁸⁸

Parent advisory body

10.69 In Queensland, there is a parent advisory body:

for the Catholic sector, the independent sector and the government sector come together regularly to meet and talk with the Queensland department around issues of concern. My understanding is that they have developed some quite good resources in recent times around cybersafety, so I think they would be worthwhile.⁸⁹

10.70 As has already been noted, the Minister for Broadband, Communications and the Digital Economy has established a Teachers' and Parents' Advisory Group on Cybersafety.⁹⁰

10.71 The Alannah and Madeline Foundation would like to see the introduction of a user-friendly toolkit in text and online versions be made available to all schools to assist with the measurement and the effectiveness of cybersafety policies and the whole of community approach.⁹¹

88 Netbox Blue, *Submission 17*, p. 4.

89 Mr Ian Dalton, Executive Director, Australian Parents Council, *Transcript of Evidence*, 20 April 2011, p. CS36.

90 See paragraph 10.41.

91 Alannah and Madeline Foundation, *Submission 22*, p. 12.

Recommendation 20

That the Minister for School Education, Early Childhood and Youth invite the Ministerial Council of Education, Early Childhood Development and Youth Affairs to formulate a cooperative national approach to the development of a whole-of-school community approach to cyber-safety, and to provide all schools with the necessary information and strategies to measure the effectiveness of their cyber-safety policies.

Peers

- 10.72 While schools can support young people through the provision of information, the encouragement of peer-to-peer education programs can be effective if they hear the facts and evidence from other students.⁹² The Australian Psychological Society believes that:

Teaching positive relationship strategies, empathy skills, the importance of bystander intervention and conflict resolution skills (anger management, problem solving, decision making) in schools is part of a whole school approach to effectively addressing cyber-safety.⁹³

- 10.73 Students at the Committee's High School Forum discussed the important on the role of bystanders in supporting their peers:

Dylan-It depends on what sort of bullying it is. If it is calling a few names and whatnot it is not that bad. It depends on the sort of personality it is. If it gets into violence, depending on how big the person is, some people would fight them.

Senator BARNEIT-Are you saying physically?

Dylan-Yes. It depends how bad it gets. Usually I would fight before I went to the teachers because I do not personally like teachers. That is just my opinion.

Madeline-At our school we are focusing on the bystander at the moment. We are making sure that everybody realises that it is not okay to stand by and just watch. If you see something on Facebook, you should tell a teacher. You do not have to talk to the

92 Parents Victoria Inc, *Submission 143*, p. 3.

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

person who has done the bullying; you can just say 'Hello' or smile at the person who is being bullied. We have a new initiative called One Goal, One Community.

Senator BARNETT-I was going to ask you about that. Can you explain this new initiative?

Madeline-It was brought to us by an old girl from our school who is at Bond University. It is happening in six countries around the world. Everyone gets a sheet and you go round and talk to your family and your family's friends and get them to sign a statement, 'I won't be a bystander and I won't accept bullying.' When you bring back the sheet you get a blue wristband for One Goal, One Community and it shows people that you do not accept bullying. So the people who are doing the bullying will realise, when they see all these people wearing wristbands, that it is not acceptable. The people who are being bullied realise there are people there to stand up for them and support them.

Senator BARNETT-That sounds cool. Do you think the program is working?

Imogen-Yes, it is definitely working. I think we have a strong year 12 community and we look out for the younger grades and ourselves. We are all quite close with our year group coordinator who is also the head of the senior school. He is very involved. If we see anything on Facebook, anything happening in town or anything happening in the playground we go and talk to him and he will have a word. We have also done an online survey, I think it was just in the senior school, that we were all strongly recommended to do. We could do it anonymously and say whether we had experienced any of these kinds of bullying. We could name people if we were not comfortable with going and talking to a teacher face to face.⁹⁴

Concluding comments

10.74 The Australian Psychological Society stressed the importance of the whole-school approach:

It is recommended that schools are encouraged and supported to adopt a whole-school approach to cyber-safety that balances the

94 Imogen, *Transcript of Evidence*, 20 April 2011, pp 18-19.

use of online technologies for creativity and learning in a safe way. Such a policy should be developed in collaboration with students, parents/carers and teachers, have the commitment of the principal (leadership of the school) and be agreed upon by every single member of the school community ...Working in collaboration with parents/carers and students to develop such a policy, making cyber-safety an integral part of student wellbeing practices in schools, and including cyber-safety as part of the curriculum will better ensure the policy's relevance.⁹⁵

10.75 The Australian Psychological Society referred to research by Dr Donna Cross:

... the most promising interventions appear to be those that take a whole-school approach which includes the development of programs aimed at:

- enhancing a positive school climate and ethos which promotes pro-social behaviours
- providing pre-service and in-service training of all school staff to assist them to recognise and respond appropriately to signs of covert bullying
- creating physical environments that limit the invisibility of covert bullying
- increasing the awareness among young people of how group mechanisms work and strengthening their skills in conflict resolution; and
- developing anonymous, peer-led support structures for students to access when they feel uncomfortable.⁹⁶

95 Australian Psychological Society, *Submission 90*, pp. 17, 24.

96 Australian Psychological Society, *Submission 90*, p. 19 citing Cross *et al*, 2009, the *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, Edith Cowan University.

PART 4

Enforcement

Legislative basis

Australian law and the online environment

- 11.1 Responsibility for combating crime in the online environment is shared between the Commonwealth, the States and the Territories. The Commonwealth has responsibility for matters across or outside Australian jurisdictions, while the States and Territories generally have domestic responsibilities.
- 11.2 Appendix E contains additional information on other relevant laws of each State and Territory and those of the Commonwealth.

Australian Government responsibilities

Attorney-General's Department

- 11.3 In May 2010, the Standing Committee of Commonwealth and State/Territory Attorneys-General agreed to establish a National Cyber-Crime Working Group to enable jurisdictions to work cooperatively to combat cyber-crime. Since its first meeting in July 2010, the National Cyber-Crime Working Group has conducted a scoping study of existing mechanisms for reporting online crime. It has also prepared a discussion paper on options to improve current reporting arrangements, including the creation of a centralised online reporting facility. Setting up such a body will be the subject of a feasibility study.¹

¹ Attorney-General's Department: *Submission 58*, pp. 2-3.

- 11.4 This is an example of work being done to consolidate material, so that those in the online environment receive consistent messages delivered centrally about cyber-safety.²
- 11.5 During the 2010 National Cyber Security Awareness Week, the publication *Protecting Yourself Online – What Everyone Needs to Know* was launched. Over 120,000 copies of the book and 270,000 copies of the pamphlet have since been distributed. This material has been updated for National Cyber Security Awareness Week in 2011.³
- 11.6 The Attorney-General’s Department has also produced *ID Theft – Protecting your Identity*. It provides practical strategies for Australians to protect themselves against becoming a victim of identity theft, and what to do if it happens. Since it was launched in 2009, over 60,000 copies have been distributed to individuals and police agencies for use in crime prevention. It is also used in training courses run by the private sector and by non-government organisations.⁴
- 11.7 On 30 April 2010, Australia announced its intention to accede to the Council of Europe *Convention on Cybercrime (2001)*. This is the only multilateral treaty in force that specifically addresses cyber-crime. Its main objective is to pursue a common criminal policy aimed at the protection of society against cyber-crime, through the adoption of appropriate legislation and fostering international cooperation.
- 11.8 The Convention requires participating countries to create offences for certain activities. It establishes procedures to make investigations more efficient, and promotes greater international cooperation using existing regimes, including mutual assistance and police-to-police assistance.
- 11.9 The Department noted that the *Criminal Code Act 1995 (Cth)* already contains comprehensive offences dealing with the misuse of telecommunications, and cyber-crime. These offences were framed in ‘technology-neutral’ language to ensure that they would remain applicable as the online environment evolves. Thus, ‘computer’ was not defined so that offences would encompass such new developments as mobile phones with Internet access. Offences such as hacking into another person’s Facebook account, altering it, or using malicious software to steal personal information, are also included.⁵
-

2 Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch, Attorney-General’s Department, *Transcript of Evidence*, 24 March 2011, p. CS19.

3 Attorney-General’s Department, *Submissions 58*, p. 3.

4 Attorney-General’s Department, *Submission 58.1*, p. 1.

5 Attorney-General’s Department, *Submission 58*, p. 2.

- 11.10 Other offences criminalise the inappropriate use of telecommunications, including the Internet. These offences include using a 'carriage service' in the online environment to menace, harass or cause offence, threats to kill or cause harm to a person, or to use such a service for child pornography.⁶
- 11.11 Further amendments to Australian legislation are required to enable compliance with the Convention, including those which:
- clarify that domestic law enforcement agencies can apply for the preservation of stored communications information;
 - enable the preservation of stored communications and associated telecommunications data at the request of foreign law enforcement agencies, and
 - require confidentiality in relation to the preservation of, access to and disclosure of stored communications and telecommunications data.⁷
- 11.12 The Australian Federal Police (AFP) noted that the Convention provides benefits to law enforcement authorities, as it contains procedures to make investigations more efficient. It also provides systems to facilitate international co-operation, including:
- helping authorities from one country to collect data in another;
 - empowering authorities to request the disclosure of specific computer data;
 - allowing authorities to collect or record traffic data in real-time;
 - establishing a 24 hour/seven days per week network to provide immediate help to investigators, and
 - facilitating extradition and the exchange of information.⁸
- 11.13 However, the Convention cannot be seen as a quick solution to the difficult problem of international evidence and criminal intelligence sharing. The AFP commented that more work needs to be done on ensuring that international law enforcement has the ability to exchange evidence and intelligence in a timely fashion.⁹ The capacity to collect evidence in Australia is arguably more limited than some other jurisdictions.¹⁰

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

7 Attorney-General's Department, *Submission 58*, p. 9.

8 Australian Federal Police, *Submission 64*, p. 14.

9 Australian Federal Police, *Submission 64*, p. 14.

10 Mr Chris Watt, Federal Secretary, Independent Education Union of Australia, *Transcript of Evidence*, 30 June 2010, p. CS14.

Australian Federal Police

- 11.14 The AFP is a member of the Consultative Working Group on Cybersafety. It works closely with other law enforcement and government agencies, industry, non-government organisations, content service providers, banks, education agencies and community groups.
- 11.15 It has a number of roles in cyber-safety issues:
- to target and investigate technology crime including child pornography and paedophile behaviour in the online environment;
 - to provide a police presence in social networking sites, and
 - to contribute to broader prevention strategies such as educational campaigns.¹¹
- 11.16 Specific objectives are to enhance its contribution to combating technology crime impacting Australian families by:
- actively targeting the production and distribution of online child sex exploitation images;
 - creating a hostile environment on the Internet for online offenders through the development of active and innovative methods of informing potential offenders of the risks involved in their activity;
 - increasing research into the evolving digital landscape and emerging threats to better predict trends and capabilities and develop active targeting, prevention and disruption strategies for online crimes, especially those involving child victims;
 - promoting community awareness through active liaison with government and non-government organisations such as educational agencies and community groups;
 - developing and implementing an Australian National Victim Image Library; and
 - developing and implementing a training and welfare strategy to deal with identified risks associated with teams working within the online child sex exploitation arena.¹²

11 Australian Federal Police, *Submission 64*, p. 9.

12 Australian Federal police, *Submission 64*, p. 10.

- 11.17 The AFP is also responsible for the development and implementation of a covert capacity to identify, target and investigate online predators, including:
- purchasing software similar to that used by offenders;
 - purchasing software for the collection of evidence;
 - implementing and maintaining a *covert* and an *overt* police presence on the Internet;
 - purchasing non-government specification hardware from non-government suppliers;
 - maintaining an online presence including warnings in chat rooms relating to potential predatory behaviour, utilising the Virtual Global Taskforce as appropriate, and
 - ‘deterrence initiatives’, such as redirection of all ‘take down’ sites to warning sites requiring the development, implementation and installation of the software required.¹³
- 11.18 Community education remains one of the most important elements of crime prevention. Through initiatives such as *Cybersafety* and the *Thinkuknow* program, the AFP engage with community groups, parents/carers and school-aged children. In the first nine months of 2010/2011, it delivered 51 *Cybersafety* presentations to 8,130 participants, and 118 *ThinkuKnow* presentations to 4,450 participants.¹⁴
- 11.19 *ThinkuKnow* involves presentations by trained volunteers, and a comprehensive website which provides additional information and resources. The themes of ‘Have fun’, ‘Stay in control’ and ‘Report’ form its focus in both the presentations and on the website launched in February 2010. It aims to open lines of communication between parents/carers and children, so that the Internet is as much a topic of discussion as events at school that day. The *ThinkuKnow* button forwards the contact details to the police and this can be followed up.¹⁵
- 11.20 The AFP also embarks on a program of cyber-safety awareness presentations at schools in regional NSW and Victoria, and the ACT. This Youth Education Program is designed to make young people think of the consequences of what they do online. The presentations are backed up by

13 Australian Federal Police, *Submission 64*, p. 10.

14 Commander Grant Edwards, Acting National Manager, High Tech Crime Operations, Australia Federal Police, *Transcript of Evidence*, 24 March 2011, p. CS5, 4.

15 Australian Federal Police, *Submission 64*, p. 22.

Fact Sheets made available on the AFP website, and in hard copy. This program also makes young people aware of the need to protect their images and reputations by being careful of with whom they communicate.¹⁶

- 11.21 Older computer users are also at risk online. The AFP delivers sessions to such users on how they can protect personal and financial information, secure wireless connections and conduct secure banking online.
- 11.22 The AFP is also involved in annual National Cyber Security Awareness Weeks, which demonstrate the importance of working together to achieve a safe online experience for all.¹⁷
- 11.23 Online crime is borderless and evidence can be transitory, highly 'perishable' and often located overseas. A key issue for law enforcement is therefore an effective and efficient legal framework for the exchange of information and evidence with overseas authorities.
- 11.24 There are two ways the AFP can engage with overseas law enforcement agencies for the provision of information:
- on a police-to-police basis, or
 - via the *Mutual Assistance in Criminal Matters Act 1987* (Cth).¹⁸
- 11.25 For evidence to be used, the latter approach is required. While its operations are under review, this Act is based on the historical legal framework and its operations 'can be cumbersome', unlike online technology which acts very quickly.¹⁹
- 11.26 The Virtual Global Taskforce is among the international forums of which the AFP is a member. In December 2009, the AFP became the Chair of this body, made up of police forces from around the world working to fight online child abuse. Its objectives are:
- to make the Internet a safer place;
 - to identify, locate and help children at risk, and
 - to hold perpetrators to account.
- 11.27 The AFP hosted a conference of the Virtual Global Taskforce in December 2010. A key outcome was an agreement for international law enforcement
-

16 Australian Federal Police, *Submission 64*, p. 23.

17 Australian Federal Police, *Submission 64*, p. 24.

18 Australian Federal Police, *Submission 64*, p. 13.

19 Australian Federal Police, *Submission 64*, p. 13.

agencies to work with international industry partners, non-government organisations and the academic sector to find ways of increasing child safety in the online environment, and to remove children from harm. The Virtual Global Taskforce is working towards developing an effective method for the exchange of information and evidence with overseas partners, including sharing international 'hash values' given to identify every child abuse image seized.

11.28 The AFP also has regional alliances via such bodies as the Australia and New Zealand Police Advisory Agency Child Protection Committee, and the Jakarta Centre for Law enforcement Cooperation, to combat online child sex exploitation.²⁰

11.29 The AFP has had a senior member seconded to work in an information and communications technology company in the United States to learn from industry.²¹

11.30 Mr Mark Newton commended the AFP:

The AFP retains world-recognized expertise in tackling criminals who groom children, online and off. Their Online Child Sexual Exploitation Taskforce (OCSET) is capable and effective, and deserves significant expansion ... An adequate response to sexual grooming would be to increase the resources available to the AFP so that they are better able to investigate and arrest child abusers.²²

11.31 As the Australian Institute of Criminology noted, mutual assistance treaties present problems for all trans-national police investigations, so that there is 'probably' a need to improve the speed of undertaking inquiries. Nonetheless, gathering evidence across jurisdictions and conducting prosecutions is 'bound to be difficult'.²³

11.32 Ms Sarah Chidgey from the Attorney-General's Department commented:

In terms of the proposed reforms to mutual assistance in criminal matters laws, as I mentioned, there was the release of a second exposure draft of those reforms. Our consultation period has just run for six weeks; it concluded on 14 March. Those reforms are designed to promote more responsible and flexible measures to

20 Superintendent Bradley Shallies, National Coordinator, Child Protection Operations, Australian Federal Police, *Transcript of Evidence*, 11 June 2010, p. CS40.

21 Superintendent Bradley Shallies, National Coordinator Child Protection Operations, Australian Federal Police, *Transcript of Evidence*, 11 June 2010, p. CS29.

22 Mr Mark Newton, *Submission 15*, p. 8.

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

secure international crime cooperation. Some of the things that those proposed reforms would do are to streamline the process for providing lawfully intercepted material and covertly accessed stored communications, to allow for covert access to stored communications and surveillance devices, and provide existing telecommunications data on a police-to-police basis. It is particularly valuable, as Commander Edwards mentioned, as the police-to-police mechanisms can operate a lot faster than the more formal mutual legal assistance mechanisms.

Finally, those reforms would also enable collection and transmission of prospective telecommunications data. In terms of where that process is at, a number of submissions have been received as part of the consultation process.²⁴

- 11.33 The South Australian Police Force noted that, because applications for assistance must often go to foreign regulators, the current process for the administration of applications under such treaties 'rarely' produces timely investigative outcomes.²⁵ It further commented:

Whilst Facebook have stated that they can respond to a Mutual Assistance request in 10 days, the Attorney-General's office has stated that it will take them at least 6 months to process the request before it is forwarded to Facebook. The uptake in the use of social networking dictates that law enforcement will require content from overseas providers on an ever increasing basis. There is a very real need to improve the process for obtaining information or court outcomes could likely be affected.²⁶

- 11.34 There is a substantial fee incurred for law enforcement agencies requesting details of accounts in situations which are not life threatening.²⁷ Mr Stewart Healley commented:

Reluctance from experience of doing all the investigation work for a brief to have the Offenders Solicitor convince the Magistrate to treat the incident lightly with a warning and no penalty or even dismissed the Charges, reinforcing the Court Message to the Offender "go do what you like" and to the Victim - "SORRY".²⁸

24 Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch, Attorney General's Department, *Transcript of Evidence*, 24 March 2011, p. CS20.

25 South Australia Police Force, *Submission 86*, p. 2.

26 South Australia Police Force, *Supplementary Submission 86.1*, p. 2.

27 Mr Stewart Healley, *Submission 136*, p. 45.

28 Mr Stewart Healley, *Submission 136*, p. 45.

- 11.35 In one situation, the Victorian Police were able to contact an online bully via Facebook in a situation where they could not physically locate them to serve an appropriate warning.²⁹

State and Territory responsibilities

- 11.36 The various codes criminalise some abuses, making them punishable by lengthy periods of imprisonment.

New South Wales

- 11.37 Offences under NSW legislation include:
- Stalking or intimidation intending to cause fear of physical or mental harm. It explicitly catches conduct involving the use of devices such as 'telephone, telephone text messaging, emailing and other technologically assisted means'; and
 - Grooming a child under 16 years of age for unlawful sexual activity. It also makes provision to capture online conduct and similar means of communication.³⁰
- 11.38 The Communications Law Centre noted that NSW is currently the only Australian jurisdiction that explicitly criminalises cyber-bullying by school children. While section 60E of the *Crimes Act 1900* (NSW) makes it an offence when a person 'assaults, stalks, harasses or intimidates' any school staff or student while attending school, it does not cover bullying outside school premises.³¹

Victoria

- 11.39 While Victoria does not directly regulate social networking, under the *Crimes Act 1958* (Vic) it has the power to prosecute crimes which may arise from actions taken on such sites, such as:
- threats to kill;
 - stalking, including repeatedly using the Internet to publish material designed to make someone else apprehensive;

29 Mr Stewart Healley, *Submission 136*, p. 84.

30 NSW Government, *Submission 94*, p. 19.

31 Communications Law Centre, *Submission 63*, p. 6.

- abduction with intent to rape, and
 - sexual penetration of a child under 16 years.³²
- 11.40 A *Personal Safety Intervention Orders Bill* has been introduced. If enacted, this will provide better protection against stalking and behaviours such as bullying and Cyber-bullying.³³
- 11.41 Under amendments made to the *Sex Offenders Registration Act*, registered sex offenders must provide additional persona details such as Internet, instant messaging, Facebook and chat room user names, or any other user names or identity used by the person on the Internet or through other online applications.³⁴

South Australia

- 11.42 South Australian Police noted that the State's laws did not specifically mention the online environment. They are, however, designed to deal with the opportunities that the Internet and other platforms provide for predatory criminal behaviour.³⁵
- 11.43 As cyber-bullying is not a criminal offence, South Australian Police does not maintain statistics of the complaints it received.³⁶ Some of the associated behaviour, such as cyber-stalking and unlawful threats, are criminal and are investigated. Anecdotal evidence suggested that cyber-bullying is rising with the increasing use of technology, although bullying appears to be decreasing in South Australian schools.³⁷
- 11.44 South Australian Police regularly received reports of privacy breaches, generally from concerned parents who were aware of images of their children placed on social networking sites without permission. Because of restrictive legislative provisions, most of these incidents were not criminal. South Australian Police investigated where the intent was to commit a serious offence, such as the posting of intimate images without permission, stalking or identity theft.³⁸

32 Victorian Government, *Submission 112*, p. 5.

33 Victorian Government, *Submission 112*, p. 5.

34 Victorian Government, *Submission 112*, p. 5.

35 South Australia Police, *Submission 86*, p. 1.

36 South Australia Police, *Submission 86*, p. 2.

37 Mr Greg Cox, Director, Student Wellbeing Department of Education and Children's Services, SA, *Transcript of Evidence*, 3 February 2011, p. CS70.

38 South Australia Police, *Submission 86*, p. 2.

- 11.45 Use of social networking sites by young people regularly required South Australian Police to obtain information from sites such as Facebook to identify criminal activity and safeguard children. It also had some concerns about mutual assistance treaties.³⁹
- 11.46 South Australian Police regularly cooperated with other agencies, inside and outside the State, including the Australian Communications and Media Authority (ACMA) and the Australian Competition and Consumer Commission. While material from such bodies was of a high standard, more agencies were developing their own strategies and South Australian Police believed that there was a risk that messages about safety and security in the online environment would become confused.
- 11.47 Through the WatchSA Program, South Australian Police personnel trained in aspects of Internet safety, including issues for parents/carers and adolescents about computer security, scams, etc. The force had developed related packages about the use of technology, including a document on cyber-bullying and e-crime that was distributed to all schools in South Australia in 2009.⁴⁰

Western Australia

- 11.48 There is no specific cyber-bullying legislation in Western Australia but, depending on the case, there may be scope for police involvement as threats and stalking are covered in the State's Criminal Code.⁴¹
- 11.49 Western Australian Police drew attention to the use of technology to identify known images to prevent their distribution on peer-to-peer networks. For it to be successful, this initiative would require the cooperation of ISPs across Australia. If adopted, this technology would automatically be able to filter out child exploitation material.⁴²
- 11.50 Identification of this material is being addressed through a national information technology project which would allow police to compare automatically seizures of child exploitation material against a known data base. This would speed up the assessment of unknown images, potentially identify victims and contact likely offenders.⁴³

39 South Australia Police, *Submission 86*, p. 2.

40 South Australia Police, *Submission 86*, pp. 2-3.

41 Western Australia Office of the Commissioner of Police, *Submission 78*, p. 2.

42 Western Australia Office of the Commissioner of Police, *Submission 78*, pp. 1-2.

43 Western Australia Office of the Commissioner of Police, *Submission 78*, p. 2.

- 11.51 Law enforcement agencies have been built around traditional physical or imaginary boundaries and dealing with the physical world. Western Australian Police noted, however, that the online environment had broken these boundaries between jurisdictions, both nationally and internationally.
- 11.52 There has also been fragmentation of agencies across Australia, and within agencies, so that ACMA used one cyber-safety program (*CyberSmart*) and the AFP another (*ThinkUKnow*). The reporting of online offences is fragmented between the West Australian Crime Squad, ACMA and the AFP. Western Australian Police also drew attention to duplications and gaps in services offered by existing agencies, citing different approaches to investigation of online offences by State police forces.⁴⁴
- 11.53 In Western Australia, although there is scope for further reductions, this fragmentation had been partially addressed, as its Online Exploitation Squad is now co-located with the AFP's Child Protection team.⁴⁵
- 11.54 Within Western Australian Police, the Office of Crime Prevention is exploring the role of crime prevention officers in cyber-safety, while for operational reasons the Online Child Exploitation Squad has retreated from cyber-safety presentations.
- 11.55 Related to fragmentation is the fact that technological advances within the online environment are outstripping law enforcement agencies' abilities adequately to resource investigations. The ever-increasing capacities of platforms is a major challenge for police forces, and an argument for a centralised agency within Australia with broad powers to investigate, advocate and act on cyber-safety issues.
- 11.56 The Force believed that there is an argument for a centralised national agency within Australia with broad powers to investigate, advocate and act on cyber-safety issues.⁴⁶

Tasmania

- 11.57 Tasmanian Police regularly engage with school communities in a range of educational campaigns which included general information on online safety. They supported the Tasmanian 2010 Crime Stoppers Youth Challenge which targeted e-safety, in which children examined crime and

44 Western Australia Office of the Commissioner of Police, *Submission 78.1*, p. 1.

45 Western Australia Office of the Commissioner of Police, *Submission 78.1*, p. 1.

46 Western Australia Office of the Commissioner of Police, *Submission 78.1*, p. 2.

community safety-related issues and developed strategies to address them.⁴⁷

- 11.58 While people have been charged with online offences, few cases have involved children. There have been several instances of sexual grooming of children, but the extent of this abuse in the State is difficult to gauge as it is likely that many of these incidents are not reported.⁴⁸
- 11.59 This force did not see cyber-bullying as primarily an issue for police. Where it became stalking, there is a role for law enforcement but, in less serious cases, it is a parental and educational issue because police involvement can make incidents more difficult to resolve.⁴⁹

Sanctions against cyber-bullying

- 11.60 As observed in Chapter 3, there has been little detailed examination of the legal issues associated with bullying, and even less of those involving cyber-bullying. In particular, schools' responsibilities under civil law, and the criminal ramifications of this conduct, are not well understood.⁵⁰
- 11.61 The Attorney-General's Department advised that serious instances of cyber-bullying may constitute an offence under Commonwealth law. It is an offence to use the Internet or a mobile phone in a way that a reasonable person would consider to be menacing, harassing or offensive, and it carries a maximum penalty of three years imprisonment. The Criminal Code sets the age of criminal responsibility for Commonwealth offences at 14 years. A child aged ten years or more, but less than 14 years old, can only be criminally responsible if she/he knows that the conduct is wrong. The onus is on the prosecution to establish awareness of wrongdoing beyond a reasonable doubt.⁵¹
- 11.62 Professor Marilyn Campbell expressed the view that:
- Even though there are not so-called specific anti-cyberbullying laws, there are enough criminal justice laws on cyberstalking, harassment and telecommunications that, if you wanted to criminalise a child's behaviour, the laws are there – except that, as

47 Tasmania Police, *Submission 85*, p. 2.

48 Tasmania Police, *Submission 85*, p. 1.

49 Tasmania Police, *Submission 85*, p. 2.

50 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 27. See Chapter 11.

51 Attorney-General's Department, *Submission 58*, p. 3.

you know, children under 10 are not held criminally responsible for their actions no matter what they do. Between 11 and 14, it is up to the court to decide whether they intended to commit a criminal act. So it is not about knowing it was naughty and knowing it was wrong and responding to something and not thinking before they clicked. It is about whether they intended to commit a criminal act and whether they then went ahead realising that it was a criminal act.⁵²

11.63 She added that:

Where we need to use the law is in civil litigation, and that is not going to be against the kids and not against the parents; that is going to be against the schools because they are the ones that have got the money.⁵³

11.64 The Attorney-General's Department also noted that criminal legislation at State/Territory level allows for the prosecution of harassing, threatening and intimidatory behaviour through a combination of assault, threatening and stalking offences. These jurisdictions can also rely on offences in the Commonwealth Criminal Code which directly address these abuses.⁵⁴

11.65 The Alannah and Madeline Foundation believed that, because the relationship of bullying to cyber-bullying is integral to the abuse, responses would be best focused on behavioural change in the school and beyond. These would be most effective when developed collaboratively, involving school personnel, parents/carers, young people, the Internet industry and the wider community.⁵⁵ The Family Online Safety Institute:

stresses the importance of differentiation between teasing or mean comments and actual criminal harassment. Instead of criminalization, the solutions should include education, empowerment and the use of website tools and services to mitigate the likelihood that children will fall prey to cyberbullying. The Cybersmart Hero program that is being run by the Australian Communications and Media Authority (ACMA) is a good example of a way to engage children in working towards a solution. The Cybersmart Hero program requires children to work together online, with professionals, to solve a real time cyberbullying-

52 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS26.

53 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS26.

54 Attorney-General's Department, *Submission 58*, p. 4.

55 Alannah and Madeline Foundation, *Submission 22*, p. 19.

themed problem. Since it is often children who are witnesses to cyberbullying, this education initiative is vital to lowering these occurrences. It also emphasizes the importance of education rather than criminalization.⁵⁶

- 11.66 The Communications Law Centre noted that Australia's reluctance to legislate more specifically against cyber-bullying is reflected in the United States where some States encompass it in general anti-harassment laws, or within computer crime statutes. The right to freedom of speech is also seen as a barrier to extensive cyber-bullying legislation, as it may curb the bullies' rights.⁵⁷
- 11.67 It also argued that Australian legislation should provide 'clear and adequate recourse', particularly for victims of cyber-bullying.⁵⁸

Sanctions against cyber-stalking

- 11.68 All Australian jurisdictions have laws dealing with cyber-stalking. Victoria and Queensland have explicitly extended the definition of the crime to include the sending of electronic messages.
- 11.69 Mr Stewart Healley commented that:

The anti-stalking legislation has a number of advantages as a means of addressing cyber bullying. First, a wide range of hostile behaviour falls within its ambit which in itself need not be criminal. For example, a threat which is merely implicit rather than explicit would still be caught. Secondly, while there are differences between jurisdictions in relation to the offender's requisite intent and the required state of mind (if any) of the victim, it is usually sufficient that the offender, by means of repeated conduct (other than in Queensland, which refers to 'at least one occasion'), intends to induce in the target an apprehension or fear of violence or harm (which in most Australian jurisdictions includes the intention to cause the target either physical or mental harm). Accordingly this offence is well suited to cases of cyber bullying, where the purpose is normally to cause emotional, rather than physical, harm and distress.⁵⁹

56 Family Online Safety Institute, *Submission 38*, p. 6.

57 Communications Law Centre, *Submission 63*, p. 6.

58 Communications Law Centre, *Submission 63*, p. 6.

59 Mr Stewart Healley, *Submission 136*, p. 96.

11.70 The *Criminal Code Act 1995* (Cth) also includes offences relating to cyber-stalking, including:

- Using a telecommunications network intending to commit a serious offence. This is intended to be broad and cover the use of the Internet or other applications to commit such offences as fraud or stalking;
- Using a carriage service to make a threat. This is intended to cover threats made over the Internet to kill or cause serious harm; and
- Using a carriage service to menace, harass or cause offence. This is intended to cover online conduct that a reasonable person would find to be menacing, harassing or cause offence.⁶⁰

11.71 The Australian Institute of Criminology noted that there are difficulties in drafting anti-stalking legislation because not all behaviour is criminal.⁶¹ Mining information about a potential victim from publicly available information, such as profiles on social networking sites, is not illegal, nor is posting non-threatening messages. Ms Sonya Ryan believed that young people need to be encouraged to use links to certified sites to avoid people who, to seek to entrap them for criminal purposes, pose as celebrities online.⁶² When such activities are repeated over a period in an unwelcome way, these seemingly inoffensive acts acquire menacing overtones for the target.⁶³

11.72 Mr Healley commented:

All Australian jurisdictions now have stalking legislation proscribing behaviour calculated to harass, threaten or intimidate ...Common examples include following the target, sending articles to the target, waiting outside or driving past the target's home or place of work, and repeated contact by phone, email or text ... They are therefore of particular relevance to cyber bullying where, like all cases of bullying, there is a similar exploitation of power imbalance.⁶⁴

60 Attorney-General's Department, *Submission 58*, p. 4.

61 Australian Institute of Criminology, *Submission 56*, p. 10.

62 Ms Sonya Ryan, Director, Carly Ryan Foundation, *Transcript of Evidence*, 3 February 2011, p. CS64.

63 Australian Institute of Criminology, *Submission 56*, p. 10.

64 Mr Stewart Healley, *Submission 136*, p. 95, citing Butler D, Kift S and M Campbell, 'Cyber Bullying in School and the Law Is there an effective means of addressing the Power imbalance?' *eLaw Journal: Murdoch University Electronic Journal of Law*: 16(1) p. 84.

Sanctions against sexual grooming

11.73 Responsibility for combating sexual exploitation of children is shared between Australia's jurisdictions. The States and Territories are generally responsible for offences related to this abuse within their jurisdictions. The Commonwealth has traditionally enacted laws dealing with these offences occurring across or outside these jurisdictions, e.g. child sex tourism and offences involving the online environment.

11.74 In 1995, the Commonwealth first enacted legislation targeting the use of a carriage service, the Internet or mobile phone for sexual activity with children. This included grooming and procuring. The operation of this legislation was enhanced in 2010 by including increased penalties, and it now covers the following offences:

- Using a carriage service to transmit a communication with the intention of procuring a person who is, or who the sender believes to be, under 16 years of age to engage in sexual activity (procuring);
- Using a carriage service to transmit a communication with the intention of making it easier to procure a person who is, or who the sender believes to be, under 16 years of age to engage in sexual activity (grooming); and
- Using a carriage service to transmit an indecent communication to a person who is, or who the sender believes to be, under 16 years of age.⁶⁵

11.75 Over 400 predators are arrested by police each year and this number is increasing.⁶⁶ Ms Ryan commented:

Not all of these people are always prosecuted, because of legal loopholes or different things that happen. But that is a statement that the cybersafety police in WA made, that they are just scratching the surface and they do not have the manpower on the ground to be able to really penetrate this problem.⁶⁷

11.76 The ACT Council of P&C Associations called for the Australian Government to:

65 Attorney-General's Department, *Submission 58*, pp. 5-6.

66 Ms Sonya Ryan, Director, Carly Ryan Foundation, *Transcript of Evidence*, 3 February 2011, p. CS60.

67 Ms Sonya Ryan, Director, Carly Ryan Foundation, *Transcript of Evidence*, 3 February 2011, p. CS63.

follow a similar action as the USA in pressuring SNS to delete known sex offenders registered in Australia. In February 2009, MySpace deleted 90,000 profiles of sex offenders registered in the USA which was made possible as part of an agreement between the website and state attorneys general. It is recommended that the Australian Government introduce a similar agreement with popular social-networking sites to restrict access for known sex offenders in Australia.⁶⁸

Sanctions against sexting

11.77 Under Commonwealth legislation, there are only criminal implications for sender and receiver if an image constitutes child pornography. Distributing other images can be a form of cyber-bullying if a young person is coerced into posing, or if images are distributed without consent.⁶⁹

11.78 Images distributed in this way may also be picked up by pornographers and could be used to blackmail the subject. Originators could be charged with making child pornography, and the person receiving it with the e-crime of disseminating that material.⁷⁰

Under proposed changes to the Sex Discrimination Act to be introduced by the Australian government, young people who have experienced cyberbullying and online sexual harassment will be given legal protection, and victims under the age of 16 allowed to use sexual harassment laws to pursue their persecutors.⁷¹

11.79 The Victorian Office of the Child Safety Commissioner added that:

We support strong and effective sanctions against adults who produce and distribute child pornography or otherwise use technology to groom or abuse children. The more challenging issue for legislative and policy reform is how to respond to children who engage in such behaviours.⁷²

11.80 The Commissioner would like to see consideration given to:

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

69 NSW Government, *Submission 94*, p. 9.

70 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS24.

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

72 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 3.

whether criminal sanctions are the most appropriate response to such conduct, if so under what circumstances they should be used, and what other options might be most effective.⁷³

- 11.81 Family Voice Australia argued that laws should be applied to the possession of child pornography in the context of sexting, provided law enforcement authorities had discretion to dissuade one-time offenders from repeating the offence.⁷⁴
- 11.82 In Australia, 32 Victorian teenagers were charged with child pornography offences resulting from sexting.⁷⁵ Many young people are unaware that sexting may be considered a criminal offence.⁷⁶

Sanctions against illegal or inappropriate content

- 11.83 The Australian Library and Information Association also called for more funding to increase the effectiveness of policing of illegal material on the internet.⁷⁷

Promotion of suicide

- 11.84 It is an offence to use a carriage service to access, transmit, make available, publish or otherwise distribute material that:
- counsels or incites committing or attempting to commit suicide;
 - promotes a particular method of committing suicide, or
 - provides instruction on a particular method of committing suicide.
- 11.85 For the offence to be made out, the person must intend to use the material to counsel or incite suicide, or for it to be used by another person to counsel or incite committing or attempting to commit suicide.

73 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 3.

74 Mr Richard Egan, National Policy Officer, Family Voice Australia, *Transcript of Evidence*, 9 December 2010, p. CS55.

75 BoysTown, *Submission 29*, p.15.

76 BoysTown, *Submission 29*, p.14, citing Lenhart A, 2009, *Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging*, Pew Internet and American Life Project.

77 Australian Library and Information Association, *Submission 16*, p. 13.

- 11.86 A preparatory offence has been created if a person possesses, produces, supplies or obtains suicide-related material with the intention that it be used in committing an offence.⁷⁸

Breaches of privacy and identity theft

- 11.87 Recognition of the threats posed by identity crime has led to a number of measures directed at preventing online identity crime through systematic improvements to the national identity management system.⁷⁹
- 11.88 The centrepiece of this response is the National Identity Security Strategy, endorsed by the Council of Australian Governments in 2005. This Strategy is a cross-jurisdictional, whole-of-government approach which emphasises the following six elements:
- Development of a national document verification service to combat the misuse of false and stolen identities;
 - Improving standards and procedures for enrolment and registration for the issue of proof of identification documents;
 - Enhancing the security features on proof of identification documents to reduce the risk of incidence of forgery;
 - Improving the accuracy of personal identity information held on organisations' databases;
 - Enabling greater confidence in the authentication of individuals using online services; and
 - Enhancing the national interoperability of biometric identity security measures.⁸⁰
- 11.89 These measures are intended to make it more difficult for criminals to create new identities or incorporate fabricated or inaccurate information into false identification credentials.⁸¹
- 11.90 In March 2011, the *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011* (Cth) inserted three new identity crimes into the Criminal Code:

78 Attorney-General's Department, *Submission 58*, p. 6.

79 Attorney-General's Department, *Submission 58*, p. 6.

80 Attorney-General's Department, *Submission 58*, pp. 6-7.

81 Attorney-General's Department, *Submission 58*, p. 7.

- Dealing in identification information with the intention of committing, or facilitating the commission of a Commonwealth indictable offence;
 - Possession of identification information with the intention of committing, or facilitating the commission of, conduct that constitutes the dealing offence; and
 - Possession of equipment to create identification documentation with the intention of committing, or facilitating the commission of, conduct that constitutes the dealing offence.⁸²
- 11.91 That Act also contains measures to assist victims of identity crime, allowing a person who has been the victim of identity crime to approach a magistrate for a certificate to show they have had their identity information misused. The certificate may assist victims of identity crime in negotiating with financial institutions to remove fraudulent transactions, and other organisations such as Australia Post, to clear up residual problems with identity theft.⁸³
- 11.92 The Communications Law Centre commented that opportunities for criminal acts in the online environment will continue to increase, as it becomes further intertwined with the everyday lives of both adults and children/young people.⁸⁴

Information requests

- 11.93 One of the biggest frustrations identified by some school principals is the inability to trace cyber-bullying when bullying has an impact in a school. Compounding this is the inability, even with police support, to have harmful and inappropriate content removed from websites. This also has implications for cyber-bullying of teachers, and this is considered in Chapter 9.⁸⁵
- 11.94 Part 13 of the *Telecommunication Act 1997* (Cth) allows law enforcement agencies to make certified and uncertified requests for the disclosure of customer information. Mr Stewart Healley commented that:

For an uncertified request, the ISP must be satisfied that the disclosure of information is reasonably necessary for the enforcement of criminal law... Certified requests are those where a

82 Attorney-General's Department, *Submission 58*, p. 8.

83 Attorney-General's Department, *Submission 58*, p. 8.

84 Communications Law Centre, *Submission 63*, p. 6.

85 New South Wales Secondary Principals' Association, *Submission 32*, p. 3.

senior officer of a criminal law enforcement agency that the disclosure is reasonably necessary.⁸⁶

- 11.95 The South Australia Police raised the issue of information required for evidence:

Access to mobile Internet Profile (IP) data which can be used to identify an Internet user is now also impacting upon law enforcements ability to investigate matters. Companies such as Optus and Telstra have informed that IP data is not available after relatively short periods of time (up to one month only). In many cases, IP data is not requested until after the expiration of such a short period. Mandated requirements for retaining information pertaining to communication would be of direct benefit to law enforcement in investigations.⁸⁷

- 11.96 Western Australia Police also raised this issue:

One challenge currently being experienced by the WA Police is obtaining quicker and easier access to companies' information (Facebook, MySpace, Microsoft etc) either for a law enforcement purpose or when bullying needs to be reported. Advice is often provided to users on reporting abuse / bullying to the companies, however, it often takes many weeks before the companies resolve the issues reported.⁸⁸

- 11.97 Further, some service providers were critical of the adequacy of response by law enforcement agencies. Of note was the lack of knowledge in relation to seeking legal evidence.⁸⁹ For example, the Australian Council for Computers in Education commented that:

To date, police responses to risks associated with SNS use in all Jurisdictions studied for this report have tended to be fragmented and insufficiently coordinated.⁹⁰

Community education

- 11.98 Young people are not necessarily aware of the legal options:
-

86 Mr Stewart Healley, *Supplementary Submission 136.1*, p. 53

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

88 Office of Commissioner of Police, WA *Submission 78*, p. 3.

89 Mr John Lindsay, General Manager, Regulatory and Corporate Affairs, Internode, *Transcript of Evidence*, 8 July 2010, p. CS11.

90 Australian Council for Computers in Education, *Submission 128*, pp. 2-3.

that despite the comfort with which they use these technologies, teens are unaware of their legal options in the context of these technology rich areas, particularly those relating to privacy and their personal information. Additionally, many teens are still unaware of the practical and very realistic consequences of their actions.⁹¹

11.99 The Association of Independent Schools of South Australia called for:

A promotional campaign put in place to inform school communities what constitutes an e-crime. Many students may not be aware that what they are doing is not only bullying, but it may also be against the law.⁹²

11.100 The Office of Youth made the point that people do not know what is legal and what is not.⁹³ Professor Phillip Slee argued:

there does need to be exactly that kind of education for the community around what constitutes criminal activity. When we worked with the police we found that young people in particular did not know that uploading images or taking images et cetera could constitute stalking or blackmail. So again we come back to that notion of strongly advocating for an educational approach, albeit keeping in mind that there is a legal component to it.⁹⁴

11.101 The Australian Council for Computers in Education highlighted the need to consider the legal risks arising from using social networking sites as there is a concern about the level of understanding of the nature of the risks in areas of 'the law that give rise to possible legal liability for young people using [social networking sites]:

- Privacy disclosure and breach of confidence
- Intellectual property rights especially copyright infringement
- Defamation; and
- Criminal laws including harassment and offensive material.⁹⁵

11.102 The Australian Psychological Society added that:

91 Mr Nick Abrahams and Ms Ju Young Lee, *Submission 66*, p. 1.

92 Association of Independent Schools of SA, *Submission 19*, p. 12.

93 Mrs Tiffany Downing, Director, Office of Youth South Australia, *Transcript of Evidence*, 3 February 2011, p. CS21.

94 Professor Phillip Slee, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS15.

95 Australian Council for Computers in Education, *Submission 128*, p. 2.

while legal implications should not be the sole driver of cyber-safety measures targeted to children and young people, important components of cyber-safety include informing them about their 'digital footprint', including the likelihood that their activities are often very traceable, and facilitating them to take responsibility for the consequences of their actions, including that they may be held liable for inappropriate activity.⁹⁶

- 11.103 Increasingly the New South Wales Director of Public Prosecutions is prosecuting offences involving young people using the internet.⁹⁷ Offences may fall both with state and commonwealth jurisdictions because of the use of telecommunications.⁹⁸ Family Voice Australia made the point that 'prosecutions should only happen in the very worst cases'.⁹⁹

Legal risks

- 11.104 The National Children's and Youth Law Centre stated that in most cases bullying had occurred at schools as well as online and young people seek advice on the possibility of legal recourse.¹⁰⁰ The Centre also commented:

Some examples of these questions are whether schools can regulate young people's online access, whether you can be banned from using a website, the consequence of acrimonious online conversations, using unsecured wireless networks, what action can be taken about racist comments online, illegal downloads of music and movies, whether there is any law about protecting children online and use of file sharing programs.¹⁰¹

- 11.105 It believes that there should be support for schools including:

providing accurate information about rights, community education and support services, effective complaints procedures and accessible dispute resolution mechanisms. Legal remedies should be a measure of last resort in most cases (although the desirability of legal mechanisms when it comes to prosecuting child pornography offences is not in question). Children also need to be active participants in this process and must be consulted both

96 Australian Psychological Society, *Submission 90*, p. 17.

97 New South Wales Director of Public Prosecutions. *Submission 47*, p. 1.

98 New South Wales Director of Public Prosecutions. *Submission 47*, p. 1.

99 Mr Richard Egan, National Policy Officer, FamilyVoice Australia, *Transcript of Evidence*, 9 December 2010, p. CS55.

100 National Children's and Youth Law Centre, *Submission 138*, p. 6.

101 National Children's and Youth Law Centre, *Submission 138*, p. 8.

in the design of education programs and their evaluation. This lends young people a sense of ownership, and enhances the effectiveness and relevance of emerging policies and programs amongst their fellow peers.¹⁰²

National accredited training

- 11.106 Evidence to the Inquiry indicates that the police and the justice system in Australia are not sufficiently supporting or equipped to support some victims and parents/carers. For many people, complaining to local police about abuses in the online environment has not always been satisfactory. Only the worst cases of bullying and cyber-bullying seem to be investigated, let alone prosecuted. In practice, intervention orders against individuals are difficult to enforce. The increasing impact of the online environment means that without additional resources and education for police on the front line, this situation may worsen. The systematic education of frontline police in the range of cyber-safety issues will assist in increasing sensitivity of handling complaints about this difficult area.
- 11.107 To be effective, this education needs to begin during recruit training and to be reinforced through a range of courses throughout an officer's career. In keeping with the cooperative national approach required to deal with abuses in the online environment, the AFP is the appropriate body to devise suitable courses, in conjunction with the police forces of the other Australian jurisdictions.
- 11.108 One suggestion was the establishment of a National Accredited Bullying and Cyberbullying Training Program for the AFP and State Police:
- Provide the necessary resources to support Federal and State Police to minimise bullying and cyberbullying practices by providing Police Members with a National Accredited Bullying & Cyberbullying Training Program.¹⁰³

102 National Children's and Youth Law Centre, *Submission 138*, p. 10.

103 Mr Stewart Healley, *Submission 136*, p. 23.

Recommendation 21

That the Attorney-General work with State and Territory counterparts to invite all Australian Police Forces to develop a range of online courses to provide training in cyber-safety issues for all ranks, from basic training for recruits and in-service and refresher courses for more senior members.

11.109 The training should also be extended to Magistrates' Courts, to:

Provide the necessary resources to support Magistrate Court and DPP Staff to minimise bullying and cyberbullying practices by providing Judges and Prosecutors with a National Accredited Bullying & Cyberbullying Training Program.¹⁰⁴

11.110 The Committee was told of case where, to protect her child, a mother had to take out restraining orders against a number of girls:

At the initial hearing the magistrate who granted the interim orders stated something to the effect that he could not include Facebook and MySpace as he was not personally familiar with and did not understand those sites.¹⁰⁵

Recommendation 22

That the Attorney-General work with State and Territory counterparts to initiate a mandatory training program for judicial officers and all relevant court staff addressing cyber-safety issues, to ensure they are aware of these issues, and of emerging technologies.

Law enforcement

11.111 Professor Marilyn Campbell commented that while legislation can set a benchmark for societal norms, it does not follow that young people must be imprisoned if they offend and that:

104 Mr Stewart Healley, *Submission 136*, p. 23.

105 Name withheld, *Submission 130*.

the police only uphold the law, and there is no law against being nasty and there is no law against bullying.¹⁰⁶

- 11.112 Professor Elizabeth Handsley referred to the similarity with domestic violence law and the possibility of applying existing legislation:

there is plenty of law that could be applied to that behaviour; it is just a matter of getting the enforcement mechanisms in place that pick it up and properly apply it to that behaviour. But there is always room for context-specific laws that make it very clear to law enforcers, 'No, you really need to take this into account and to take it seriously.'¹⁰⁷

- 11.113 Bullying is usually seen as a behavioural matter and not a criminal offence and police are rarely involved.

- 11.114 However, the Community Law Centre suggests that 'the offence of cyber-assault be specifically incorporated into legislation and strengthened to adequately protect consumers including children throughout Australia.' It also point out noted that:

New South Wales is the only jurisdiction that explicitly criminalises cyber-bullying by school children into its Crimes Acts. Section 60E of the *Crimes Act 1900* (NSW) makes it an offence where a person 'assaults, stalks, harasses or intimidates' any school staff or student while attending school. This wording, however, leaves bullying outside of school premises without the ambit of this section.¹⁰⁸

- 11.115 It should be noted that:

cyberbullying can constitute criminal conduct, especially when the behaviour is seriously threatening, harassing or intimidating. While there may be a natural tendency to seek to avoid the criminalisation of young people in this context, criminal sanctions are appropriate to more cases than are generally appreciated, while very few young people seem to appreciate their potential for attracting criminal liability. Media reports and other accounts, however, have recently highlighted that schools themselves, if not teachers and parents also, are increasingly inclined to resort to the criminal law; often out of fear, frustration or in the interests of

106 Associate Professor Marilyn Campbell, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, pp. CS13, 16.

107 Professor Elizabeth Handsley, President, Board Member and Chair of Executive Committee, Australian Council on Children and the Media, *Transcript of Evidence*, 3 February 2011, p. CS45.

108 Communications Law Centre, *Submission 63*, p. 6.

community safety. It is imperative to consider the issue of either criminalising or providing formative discipline for these behaviours.¹⁰⁹

11.116 Mr Stewart Healley made the point that:

Nevertheless, cyber bullying may easily be conceived in terms of well know criminal offences such as assault, threats, extortion, stalking, harassment, and indecent conduct. In addition, an increasing array of new offences, such as torture, voyeurism, cyber stalking, and telecommunications offences may be relevant. The New South Wales provisions and some of these other offences as they apply to cyber bullying are worth closer examination.¹¹⁰

11.117 Under common law, the responsibility of schools for cyber-bullying is not well understood.¹¹¹ The Australian University Cyberbullying Research Alliance submitted that:

In the case of the perpetrator, depending on circumstances, such an action might be framed as action for the tort of 'assault', an intentional infliction of psychiatric harm, defamation or the embryonic tort protecting privacy. Unlike criminal law, age is no barrier to a civil liability to pay compensation for cyberbullying.¹¹²

11.118 The Alliance also emphasised practical considerations:

The decision whether to bring an action against a child perpetrator is therefore more likely to involve more practical considerations such as whether he or she has sufficient financial resources to make him or her worth suing. Whatever the position in other countries, under Australian law parents are generally not legally liable for the acts of their children and thus it is usually schools which are involved in civil litigation.¹¹³

11.119 The following comments were made by respondents to various questions throughout the Committee's *Are you safe?* survey:

109 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 28.

110 Mr Stewart Healley, *Submission 136*, p. 91.

111 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 27.

112 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 28.

113 Australian University Cyberbullying Research Alliance, *Submission 62*, pp. 28-29.

Add a law that says every website needs to act on cyberbullying, whatever site they run (Male aged 15).

Stronger laws regarding bullying practice online (Female aged 17).

Providing the police would be good but it will not help to solve the problem. It could make the bullies more aggressive? (Female aged 16).

With poloking and enforcing using teachers and parents to enforce these are not a good idea, most of the time I have noticed that my generation does not care or respect most teachers and parent, they need to know there will be servere consquences but also you need to find a way to make then understand respect amoung others, at a young age and contunie to drill it in, also mabye teaching the discipline may help (Female aged 16).

- 11.120 The AFP made the point that although there are numerous crime prevention, education and awareness programs actively endeavouring to raise awareness of parents, carers, teachers and children, these are mostly targeted at mainstream audiences.¹¹⁴ The AFP added that very few of these programs have been evaluated for their impact.¹¹⁵

Role of industry

- 11.121 The Australian Institute of Criminology refer to the greater potential of an effective partnership between the public and private sectors rather than attempting to use law enforcement on its own in dealing with online risks.¹¹⁶

- 11.122 The AFP advised that,

Legal mechanisms for compelling [content service providers (CSP's)] 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.¹¹⁷

114 Australian Federal Police, *Submission 64*, p. 2.

115 Australian Federal Police, *Submission 64*, p. 4.

116 Australian Institute of Criminology, *Submission 56*, p. 11, citing Choo K-KR 2009a, *Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences*, Research and public policy no. 103. Canberra: Australian Institute of Criminology.

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

11.123 The Australian Institute of Criminology added that:

The private sector must also play a role in crime prevention as most online environments are commercially owned and operated (e.g. social networking sites). Although there is an imperative for private sector organisations to respond to corporate and shareholder interests, these interests should not neglect the need to provide a safe and secure environment for users, particularly children and young people. Business interests, therefore, need to devote resources both to maximising profit as well as minimising opportunities for systems to be used for illegal activities.¹¹⁸

Concluding comments

11.124 Cyber-values stressed the need to deal with the underlying values instead of adopting defensive stances and excessive regulations:

For most ethical problems, participants resorted to legal sanctions and technical precautions for solutions.¹¹⁹

11.125 All Australian jurisdictions have laws that can be used against crimes committed in the online environment. Inevitably, the enactment of laws follows criminal acts, and it is not clear that current statutes include a range of effective cyber-safety protection. A review of what has been enacted in the various jurisdictions would be a means of assessing what is effective, and where additional legislation is required. The AFP reflected,

The Commonwealth legal and regulatory framework is under constant review. Law reform in this area presents a number of challenges due to the rapidly changing digital environment and the transnational and highly adaptable nature of online criminality.¹²⁰

11.126 The Communications Law Centre commented that opportunities for criminal acts in the online environment will continue to increase, as it becomes further intertwined with the everyday lives of both adults and children/young people.¹²¹

118 Australian Institute of Criminology, *Submission 56*, p. 11.

119 Cyber-values, *Submission 8*, p. 2.

120 Australian Federal Police, *Submission 64*, p. 13.

121 Communications Law Centre, *Submission 63*, p. 6.

- 11.127 That review could also address the provision of more adequate recourse for victims of cyber-safety crimes, particularly but not only cyber-bullying and identity theft. It could also be extended to include effective legal remedies and adequate compensation for the harm done to victims, especially young people.¹²²

Recommendation 23

That the Attorney-General in conjunction with the National Working Group on Cybercrime undertake a review of legislation in Australian jurisdictions relating to cyber-safety crimes.

- 11.128 The Alannah and Madeline Foundation added that there should also be a nationally coordinated cyber-policy plan involving all jurisdictions to ensure that:

People who have been the victims of cyber abuse [have] a dedicated body to which they can address concerns and complaints, and which has the expertise to remove offending material and prosecute offenders rapidly.¹²³

- 11.129 The process of seeking information from international police forces and other agencies through mutual assistance treaties was designed at the beginning of the digital age, in 1987. It now rarely produces timely results for Australian investigators of online crime. The Australian Institute of Criminology commented:

the mutual legal assistance treaties that are in existence present problems not only for child exploitation matters but for all transnational police investigations. There probably is a need to improve the speed of undertaking those inquiries, but conducting prosecutions and gathering evidence across jurisdictions is bound to be difficult.¹²⁴

- 11.130 A review of the current operations of these treaties is under way:

In January [2011], the government released a second exposure draft of some proposed legislative reforms to Australia's mutual assistance laws which will be designed to promote more

¹²² Communications Law Centre, *Submission 63*, p. 6.

¹²³ Alannah and Madeline Foundation, *Submission 22*, p. 13.

¹²⁴ Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS9.

responsive and flexible measures to a degree; that is obviously at the Australian end. Mutual assistance is always a two-way street where there is another country involved as well. Another step that we are taking is that the Attorney-General, in the quintet of attorneys-general, with the US, Canada, New Zealand and the United Kingdom – there is a meeting in the middle of the year and, at that meeting, the attorneys propose to discuss cyber threats and how we might more effectively cooperate in dealing with them as well.¹²⁵

11.131 The Australian Government has announced its intention to accede to the Council of Europe *Convention on Cybercrime 2001*.

11.132 In relation to an appropriate legal framework, the Alannah and Madeline Foundation highlighted:

- The need to legally define the rights and responsibilities of schools in responding to bullying and cyberbullying situations, and cyber-defamation;
- Legal remedies in themselves are not a solution to bullying, but are a necessary part of the solution; and
- The need to clarify the role of the criminal and civil law in relation to cyberbullying and bullying.¹²⁶

11.133 The Foundation is of the view that a legal framework should be established to manage cyber-abuse that crosses state and political boundaries, and that:

Federal, State, and Territory government convene a working group involving other stakeholders to consider an appropriate legislative response to cyberbullying and bullying in general in our schools.

Because of the lack of boundaries for the abuse that occur online and with mobile phones, all Australians need to be confident that consistent rules and consequences will apply in all states and territories.¹²⁷

11.134 The Department of Broadband, Communications and the Digital Economy questioned this approach:

125 Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch, Attorney-General's Department, *Transcript of Evidence*, 24 March 2011, p. CS9.

126 Alannah and Madeline Foundation, *Submission 22*, p. 5.

127 Alannah and Madeline Foundation, *Submission 22*, p. 13.

The real question that I think confronts us is whether a legislative framework would be any faster than a voluntary framework. We have found no evidence that the relevant websites, these large multinational websites, are reluctant to take this sort of material down. Their user policies are actually very broad in terms of the kinds of materials they can take down compared to, for example, what is covered in the Broadcasting Services Act. They cover a much wider range of material that they describe as inappropriate than is described in legislation. So the breadth of the policies is broader, and we have not seen any evidence of a reluctance on their part to take it down. The key is how you work through a large multinational organisation to move quickly, and it is not clear that legislation would make them move any more quickly than a voluntary arrangement.¹²⁸

11.135 Further, ACMA commented that:

ACMA and the Attorney-General's portfolio, especially through the Federal Police, have moved to work very closely together. So if a complaint comes in we do triage so it goes to the right place in government. Secondly, we are also focusing on the same issue that other countries have focused on, which is about having points of influence in American companies and educating them to understand that we have local sensitivities which may not at first blush be immediately apparent to them, because community standards do vary from country to country. I think Australia has a particularly good framework for setting out what is important to Australians. So they are the challenges in dealing with the types of problems we have been talking about that we have been working hard to meet.¹²⁹

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

129 Ms Andree Wright, Acting General Manager, Consumer, Content and Citizen Division, Australian Communications and Media Authority, *Transcript of Evidence*, 3 March 2011, p. CS15.

Policing

Policing and justice

- 12.1 It is clear that the Australian Federal Police (AFP) and State and Territory police forces are committed to improving safety in the online environment. It is equally clear, however, that some people who report bullying or harassment to local police stations often do not receive much support. It was noted that, because of resource constraints, stations are 'far too overstretched' to engage with anything but high-level cyber-crime and in some cases an understanding of the issues.¹

Criminalisation of online behaviour

- 12.2 The Attorney-General's Department noted that the *Criminal Code Act 1995* (Cth) contains comprehensive offences dealing with the misuse of telecommunications, and cyber-crime.² The Commonwealth Director of Public Prosecutions submitted:

There are a number of Commonwealth offences which relate to the potential abuse of children online, such as offences involving grooming and procuring children using a carriage service (sections 474.26 and 474.27 of the Code) and offences of using a carriage service for child pornography material and child abuse material (sections 474.19, 474.20, 474.22 and 474.23 of the Code). These

1 Name withheld, *Submission 140*, p. 2.

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

offences are prosecuted by the [Commonwealth Director of Public Prosecutions] (CPP). The CDPP is prosecuting an increasing number of offences involving the on-line exploitation of children ... The Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010 (Cth) inserted new offences into the Code which specifically relate to the potential abuse of children online.³

Table 12.1 Proven Offences to 22 June 2010 of offences under the Code

Act/Section	Outcome	<i>FY05/06</i>	<i>FY06/07</i>	<i>FY07/08</i>	<i>FY08/09</i>	<i>FY09/10</i>	Total
Criminal Code 474.19	Proven	2	22	38	110	129	301
Criminal Code 474.20	Proven		4	2	6	3	15
Criminal Code 474.22	Proven		4	7	9	4	24
Criminal Code 474.23	Proven		1	1	1		3
Criminal Code 474.26	Proven		4	6	12	14	36
Criminal Code 474.27	Proven	1	1	3	11	14	30
Totals	Proven	3	36	57	149	164	409

Source *Commonwealth Director of Public Prosecutions, Submission 49, p. 5. Table relates to a total of 356 defendants.*

12.3 It was suggested that, while there is enough legislation that can be applied to abusive behaviour, enforcement mechanisms are required. The Stride Foundation made the point that students see cyber-bullying as it relates to student to student:

One of the key components of the definition of Cyber Bullying is that it relates to students on student behaviour. It does not include adult on student or adult on adult behaviour as there are clear laws and definitions that cover these areas.⁴

12.4 Further, the Association of Independent Schools of South Australia make the point that:

Many teachers and parents may not be aware that as well as being morally wrong, cyber-bullying and other inappropriate behaviours may also be against the law. An e-crime is where technology, for example a mobile phone, is used to commit an offence such as harassment. E-crimes can be reported to police and offenders can be prosecuted. This is not widely known throughout the community.⁵

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

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

5 Association of Independent Schools of SA, *Submission 19*, p. 12.

- 12.5 The possibility of enforcement of criminal laws for behaviour online is not always appreciated.⁶ The Stride Foundation believe that,

Assumed anonymity and the perceived lack of penalties have created the image that the internet is a lawless world which provides great freedom to the user. What is often lacking is an awareness by students of the potentially serious legal ramifications of their behaviour. Teachers and students need to be made aware of current penalties that exist. For example in NSW the Crimes Act, Section 545AB covers the offence of intimidation. Teasing or spreading rumours about someone online is considered intimidation and under the Act carries a maximum penalty of five years detention and/or \$5500 fine. Harassing someone online or making threats electronically can carry penalties of up to 10 years detention.⁷

- 12.6 Students need to be made aware that the misuse of telecommunication devices is considered a very serious situation in Australia and a Commonwealth offence. Interviews with cyber-bullies have often revealed they considered their online harassing behaviour as 'pranking' or joking around. Both students and adults involved with online behaviour need to understand the sending of offensive or harassing messages is considered by the law as assault.⁸

- 12.7 The criminalisation of young people has attracted the following sentiments:

It may seem to some that a criminal prosecution would be an extreme response to bullying behaviour. In the first place, the Director of Public Prosecutions may be dubious in a given instance that a case can be established beyond reasonable doubt, particularly with respect to the necessary intention to commit the relevant crime. Nevertheless, even where there is such reticence on the part of the prosecuting authority, targets of cyber bullying may find that the very involvement of a police investigation helps them to regain a sense of control and power otherwise lost to the bully.

6 Professor Elizabeth Handsley, President, Board Member and Chair of Executive Committee, Australian Council on Children and the Media, *Transcript of Evidence*, 3 February 2011, p. CS46.

7 Stride Foundation, *Submission 6*, p. 9, citing Signy H, 2007, 'Bullies who leave no bruises', *The Age*, Melbourne.

8 Stride Foundation, *Submission 6*, p. 9, citing Carr-Greg M, 2007, *Real Wired Child*, Penguin Books, Maryborough, Victoria.

Examination of the range of criminal offences that may be relevant is therefore warranted.⁹

12.8 Yet Commander Grant Edwards of the AFP commented:

suffice to say that it is positive in the sense that we are getting very good conviction rates out of the prosecutions that we are putting before court.¹⁰

12.9 While a range of sanctions against abuses of cyber-safety already exists in Australian jurisdictions, several participants in the Inquiry expressed concerns about criminalising some adolescent behaviour in the online environment. For example:

we should be wary about criminalizing behaviour that is more effectively and more appropriately addressed through non-criminal measures, such as education and counselling ... The harms associated with the criminalization (as child pornography) of naïve experimentation or rule-breaking on the part of minors are likely to outweigh the benefits to the community at large or to those minors.¹¹

12.10 It was agreed that cyber-bullying should not necessarily be regarded as entirely different to bullying at school. In particularly serious cases, criminal investigation and prosecution 'may well be warranted'.¹²

12.11 It was also suggested that there is enough legislation on cyber-stalking, misuse of telecommunications and harassment, for example, to criminalise behaviour. But children under ten are not held criminally responsible for their actions and, between 11 and 14 years, courts decide whether young people intended to commit a criminal act.¹³

12.12 There had been a proposal to amend the Criminal Code to ensure that it can deal with serious cyber-bullying. The Alannah and Madeline Foundation believed that 'no-one wanted to criminalise children's behaviour' because this abuse had to be seen in the context of the ways

9 Mr Stewart Healley, *Submission 136*, p. 91, citing Butler D, Kift S and M Campbell, 2009, 'Cyber Bullying in School and the Law Is there an effective means of addressing the Power imbalance?' *eLaw Journal: Murdoch University Electronic Journal of Law*: 16(1): 84

10 Commander Grant Edwards, Acting National Manager, High Tech Crime Operations, Australian Federal Police, *Transcript of Evidence*, 24 March 2011, p. CS5

11 Mr Bruce Arnold, *Submission 60*, pp. 3-4.

12 Commander Grant Edwards, Acting National Manager, High Tech Crime Operations, Australian Federal Police *Transcript of Evidence*, 24 March 2011, p. CS23.

13 Associate Professor Marilyn Campbell, School of Learning and Professional Development, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS26.

they behave. To make ‘an enormous number’ of them of criminals would be an inappropriate legislative response to a behavioural problem that is the responsibility of schools and, particularly, parents.¹⁴

- 12.13 Professor Philip Slee thought that there was pressure to go down the legal path of criminalising the behaviour of young people, and that caution should be exercised.¹⁵ Dr Julian Dooley and Ms Robyn Treyvaud supported this view: that behaviour is the problem, not the technology.¹⁶ The Australian University Cyberbullying Research Alliance stated that regulating technology, or taking legal action, would not change behaviour.¹⁷
- 12.14 Mr Bruce Arnold agrees that a cautious stance should be adopted when considering arguments for criminalising behaviour that he believed would be more effectively and appropriately addressed through education and counselling.¹⁸ He also believed that the harms associated with criminalising what he saw as ‘naive experimentation’ or rule-breaking were likely to outweigh the benefits to the community, or the individual(s). Education campaigns were more likely to be effective than trials of 15 year olds, or seizing mobile phones.¹⁹
- 12.15 Ms Robyn Treyvaud noted that mobile phones are probably the area where parents/carers can have influence. It seems to have been assumed that pre-paid services might moderate inappropriate use because of the limited credit available. It appears, however, that behaviour is modified if parents/carers might find out, via account statements, that such images have been sent. Further, it is in schools where students know that there is a log of where they have been that inappropriate images are not sent.²⁰
- 12.16 Professor Sheryl Hemphill suggested that there should be less legal interventions, with more emphasis on the right way to behave, because of the risk of putting young people on the path to criminal behaviour.²¹ The

14 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. CS26.

15 Professor Philip Slee, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS14.

16 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS5; Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, December 2010, p. CS35.

17 Australian University Cyberbullying Research Alliance: *Submission 62*, p. 27.

18 Mr Bruce Arnold, *Submission 60*, p. 3.

19 Mr Bruce Arnold, *Submission 60*, p. 4.

20 Ms Robyn Treyvaud, Founder, Cyber Safe Kids, *Transcript of Evidence*, 9 December 2011, pp. CS39-40.

21 Associate Professor Sheryl Hemphill, Senior Research Fellow, Murdoch Children’s Research Institute, *Transcript of Evidence*, 9 December 2010, p. CS24.

Queensland Catholic Education Commission agreed that an emphasis on education, rather than on punitive action, seemed to be a more enduring way to proceed in a complex area.²²

12.17 The Family Online Safety Institute stressed the importance of differentiating between teasing or ‘mean comments’ and actual criminal harassment. It recommends that instead of criminalising behaviour, solutions should include education, empowerment and the use of website tools to reduce the likelihood that young people will fall prey to cyber-bullying.²³

12.18 While the Australian University Cyberbullying Research Alliance accepted the ‘natural tendency’ to avoid criminalising young people’s actions and added the following points:

- Criminal sanctions were appropriate to more cases than was generally appreciated;
- Very few young people seemed to appreciate their potential for attracting criminal liability;
- Recent reports had highlighted that schools, if not teachers and parents/carers, were increasingly inclined to resort to criminal law as a result of fear, frustration, or in the interests of community safety;
- It was imperative to consider either criminalising behaviour or providing ‘formative discipline’;
- Civil law may be invoked when targets decide to turn to the courts to gain some reparation from those responsible for abusive behaviour;
- Under Australian law, parents/carers are not generally legally liable for their children’s acts, so that schools are usually involved in civil litigation;
- While our society is increasingly litigious, consideration needs to be given to the view that the ability of schools to respond appropriately to abuse is hampered by ‘the often unrealistic fear’ of being sued; and
- Finally, there is the issue of extending schools’ duty of care to off-site behaviour, at any time of day or night.²⁴

22 Queensland Catholic Education Commission, *Submission 67*, p. 4.

23 Family Online Safety Institute, *Submission 38*, p. 6.

24 Australian University Cyberbullying Research Alliance, *Submission 62*, pp. 28-29.

- 12.19 Reference was made to a case in Western Australia where an explicit video had been made, sent by mobile phone and downloaded via a memory stick to a computer at home. The young recipient was charged with possessing child pornography. This was seen as an example of laws being used against those they were designed to protect. If found guilty in some Australian jurisdictions, the young person could be placed on a sex offenders' register. Such cases raise the issue of whether laws need to be changed because of the ways technology is changing, and the ages of the users.

Restorative justice programs

- 12.20 Restorative justice programs are based on shared ownership, or a peer approach, to resolve problems that arise at schools. They take the form of conferences involving a range of people, including community representatives, perpetrators, victims, parents/carers, law enforcement, teachers and school staff. Incidents are discussed, as are ways of resolving them, and perpetrators are present when victims explain the impact incidents had on them. Community and law enforcement representatives can discuss ways of restoring harm that has been done.²⁵
- 12.21 As this process seeks to be educative rather than punitive, it can be effective in resolving issues. Though these programs are becoming more widely used in schools, their effectiveness is not clear.²⁶
- 12.22 Most schools have effective policies and programs to address bullying and its effects, but the prevalence of cyber-bullying seems to be growing. The damage that this abuse can do to some students as either victim or perpetrator indicates that, in terms of schools' duty of care, prompt and effective action should be taken.
- 12.23 While it was pointed out that such programs take a great deal of staff time, involving perpetrators in a restorative process should enlighten them about the hurt that they have caused. Such programs would be a structured way to reduce that hurt for victims, to assist in their recovery

25 Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS23.

26 Associate Professor Sheryl Hemphill, Principal Research Fellow, Murdoch Children's Research Institute, *Transcript of Evidence*, 9 December 2010, p. CS27; Australian Secondary Principals Association, *Submission 33*, p. 3.

from the abuse and lead to greater involvement of parents/carers, police and local communities in schools.²⁷

- 12.24 The Association of Independent Schools of South Australia commented on the firm, supportive and considered manner in which schools deal with cyber-bullying and referred to:

The Restorative Justice approach is used by some AISSA member schools when dealing with incidents of cyber bullying. It focuses on developing an understanding in students of the social and emotional impact of their behaviour, for oneself and others, rather than an emphasis on tangible consequences. The focus is on restoring an appropriate relationship.²⁸

- 12.25 The Australian Institute of Criminology supported the restorative justice approach in which:

You have conferences of the victim, the offender, community representatives and law enforcement all meeting together to discuss the nature of the incident and how it can best be resolved. You have an offender present when a victim explains the impact of the activity on them. The parents can also be present. The representatives from the community and law enforcement can talk together about restoration for the harm that has been done. I think that could be a good alternative approach.²⁹

- 12.26 The NSW Government also supported the restorative justice approach, as it:

concentrates on promoting values likely to lead to responsible citizenship, such as pride in one's school and an obligation to help others. Addressing the problems of bullying is seen as requiring confrontations with the person bullying, the deliberate inducement in them of appropriate shame, and action undertaken by them to restore positive relations with the person being bullied... There is Australian data that indicates that there is a decrease in suspension rates through the application of restorative conferencing in schools, along with high rates of participant satisfaction (e.g. person harmed, parents and

27 Association of Independent Schools of SA, *Submission 19*, p. 13.

28 Association of Independent Schools of SA, *Submission 19*, p. 13.

29 Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS23.

wrongdoer) and high rates of compliance with agreement (above 90%).³⁰

12.27 Mr Stewart Healley advised:

Police are often reluctant to charge young people with criminal offences where other, less punitive, measures can be used. This may involve the use of restorative justice, where the person who has been cyber bullied and the people doing the cyber bullying (as well as their support network) are brought together to talk through the issues and come up with an agreed solution. Other options include cautions or disciplinary action taken by schools or parents.³¹

12.28 He also made the point that restorative justice program do not work in all cases:

Unfortunately, for the remaining 10% of teenagers that do not “choose to be” or “accept” any form of Social Responsibility; and are usually supported “blindly” and sometimes “aggressively” by their Parents / Guardians no matter what evidence is produced, will not be suitable for the Restorative Justice Pathway and will be assessed as an “Ineligible Offender”.³²

12.29 Mr Healley added that:

However, my previous 11 years as an operational Police Officer have given me the knowledge and experience to know however few in number, whatever conflict resolution methods you employ there are some children and adults that do not wish to alter their behaviour choices and see that they have a right to do whatever, wherever, whenever they chose and that includes inflicting pain and suffering on others with an attitude of “who’s going to stop me, then!”³³

Intervention orders

12.30 Dr Helen McGrath referred to the number of intervention orders being taken out by students against students:

30 NSW Government, *Submission 94*, p. 25.

31 Mr Stewart Healley, *Submission 136*, p. 46.

32 Mr Stewart Healley, *Submission 136*, p. 135.

33 Mr Stewart Healley, *Submission 136*, p. 44.

My experience has been that parents tell me that when they have tried to make a complaint to their local state police branch, even though the local state police branch may be aware of the federal e-crime offences, they are usually discouraged from going further and it is not made easy for them. One of the areas of concern that I have is how effectively the Australian Federal Police are working with state police to facilitate that process if that is the way in which parents want to go.³⁴

12.31 While victims can take out intervention orders against perpetrators, these are 'almost impossible in practice to enforce'. Where a school is reluctant to take action, desperate parents/carers sometimes complain to local police because they cannot see any other way to stop the abuse. Going to the police or taking court action is not usually an effective first step, as complainants seem generally to be discouraged from proceeding further.³⁵

12.32 The Independent Education Union of Australia made the point that:

If one of the things that arises from that approach and then taking it to the next logical step by seeking apprehended violence orders against students at the same school where proximity becomes the determinant, it is actually an unworkable solution that they cannot be within 50 metres of each other. That might be the entire length of the school buildings in that particular school. It becomes an unworkable solution even though it is an approach that the law provides for. I think it is really critical that the point she makes is upmost in our minds in that whatever solutions we are proposing, they have to be absolutely workable.³⁶

12.33 Dr Helen McGrath explained that sometimes parents are desperate and while this may not be a good solution:

the reason why so many intervention orders are taken out against children and young people is that the parents could not get the school to make it stop, therefore they thought they had absolutely no other action. The action per se, even though it might have been hard to implement, which I would agree with you about, was enough to project the school into action. She suggested that, if there were mandatory reporting of ongoing psychological harm to

34 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS25.

35 Dr Helen McGrath: School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, pp. CS25-26, 28-29.

36 Mr Chris Watt, Federal Secretary, Independent Education Union of Australia, *Transcript of Evidence*, 30 June 2010, p. CS28.

young people, it might at least trigger a response such as there is now going to be a mandatory restorative justice conference with that family, with those children, with the school leadership, et cetera.³⁷

- 12.34 Details were provided to the Committee of what could be regarded as a case study in the lack of effectiveness of schools, law enforcement and the justice system. A 15 year old was recently forced to change schools because of bullying, harassment intimidation, and defamation on social networking sites, lack of action by senior school staff and an assault. Restraining orders were successful on the protagonists.³⁸ The writer explained the impact of the event:

The other members of the group continued to post on Facebook about the event and as a result of the physical attack I determined to take out restraining orders on behalf of my child.

Two girls (the one who admitted to the physical attack and another who was facing charges for another incident) accepted the restraining orders. However the other four continue to be seen as a collective (I lodged six individual orders) and continue to contest the orders.

At the initial hearing the magistrate who granted the interim orders stated something to the effect that he could not include Facebook and MySpace as he was not personally familiar with and did not understand those sites.

I will clarify that when the orders were put into effect, my subsequent complaints for breach of an order as a result of Facebook activity by some of the Respondents were taken seriously and acted upon by Police.³⁹

- 12.35 The Stride Foundation cautioned about the potential to compound the harm by trivialising cyber-bullying incidents and not taking them seriously:

To tell the target to 'ignore it', 'get over it', 'don't worry, or it happens to everyone' does not in anyway help the target to

37 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, pp. CS28-29.

38 Name withheld, *Submission 130*, pp. 2-3.

39 Name withheld, *Submission 130*, p. 3.

deal with the lack of confidence, self-esteem or social comfortability.⁴⁰

- 12.36 Baily commented that promoting a safe online environment or bully-free zone is nowhere near as effective as enforcing and policing, and making young people aware that it happens.⁴¹ Similarly, Lisa commented:

Police enforcement is really needed. I had an issue, which turned really bad and when I contacted police, I was told to grow up and that they can't do anything about it. How is that going to help the youth that are receiving death threats, and police will do nothing to help and put it done to "teenage drama"? I suggest getting a better police force who actually do their job, instead of ignoring laws.⁴²

- 12.37 Therefore, there needs to be greater awareness of the options available to parents and young people in situations where the school have not been able to resolve the situation adequately.⁴³

Coordination

- 12.38 South Australian Police and Western Australian Police drew attention the need for greater coordination of available resources between agencies to deal with cyber-safety issues. The WA Force argued that there was a need for a national body to investigate, advocate and act on cyber-safety issues.
- 12.39 Google commented on its 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

40 Stride Foundation, *Submission 6*, p. 8.

41 Baily, *Submission 147*, p. 1.

42 Lisa, *Submission 145*, p. 1.

43 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS34.

Crimes Against Children National Conference and the Virtual Global Taskforce.⁴⁴

12.40 The Australian Council for Computers in Education stated that:

To date, police responses to Risks associated with SNS use in all Jurisdictions studied for this report have tended to be fragmented and insufficiently coordinated.⁴⁵

12.41 The AFP detailed where cooperation would be particularly beneficial:

For example, from a law enforcement perspective, it is vital that information about trends, offenders' modus operandi derived post each operation is linked into current prevention strategies. This ensures prevention and awareness raising campaigns are targeting the vulnerabilities in which online child sex offenders have identified and pursued.⁴⁶

Legal risks

12.42 The Australian Council for Computers in Education highlighted the need to consider the legal risks arising from using social networking sites as there is a concern about the level of understanding of the nature of the risks. The areas of law where there are potential liabilities for young people using social networking sites include:

- Privacy disclosure and breach of confidence;
- Intellectual property rights especially copyright infringement;
- Defamation; and
- Criminal laws including harassment and offensive material.⁴⁷

12.43 The National Children's and Youth Law Centre stated that in most cases bullying had occurred at schools as well as online and the centre has had requests for advice in relation to possible legal recourse.⁴⁸

44 Google Australia & New Zealand, *Submission 13*, p. 3.

45 Australian Council for Computers in Education, *Submission 128*, pp. 2-3.

46 Australian Federal Police, *Submission 64*, p. 4.

47 Australian Council for Computers in Education, *Submission 128*, p. 2.

48 National Children's and Youth Law Centre, *Submission 138*, p. 6.

Feedback from young people

- 12.44 The Committee's *Are you safe?* survey revealed that overall, young people are generally positive in their engagement with police. Demonstrating the breadth of police involvement in this area, the following comments were made by survey participants responding to various questions throughout the survey.

Government should create a cyber-safety police force and have a website where kids can report cyber-bullying. Police can chase this up and parents of the other kids will be held liable. This would reduce and deter people from bullying (Male 18).

I have been cyber-bullied, but it was a few years ago. It was 27 pages of teasing and swearing, then my dad told the bullies that they will see him in the school office the next morning. I was too scared to go to school, but I did. The next morning, the principal said they couldn't do anything, because it was out of school, so they got no punishment. He said to not bother with the police because we were only 12. I still got cyber-bullied, and I got very upset. I hope in the future, they will get punished (Female 14).

I think that if you want bullying to be controlled, more laws should be enforced, police men and women should come to the schools and talk to youth about it and make children scared and instead of teachers handling it police should get involved. The bullies at my schools are mostly the rich ones that get whatever they want and have more than everyone else, or the girls that are really beautiful and use their looks to bully people in ways (Female 15).

I think the main problem or reason that cyber bullying seems to be increasing is that most young people are unaware that cyber bullying can be as serious/harmful as face-to-face bullying. It seems that many people are willing to post a nasty comment online, often people who would never dream of saying the same to a person's face. Young people need to be made aware that cyber bullying is just the same and can have the same disastrous consequences as other bullying forms. There is also the issue of anonymity, where bullies believe they cannot be traced and are therefore able to say whatever they wish. Ensuring young people are aware that police or other authorities have full access to internet history and the ability to track internet use I think would reduce the number of people willing to bully on the internet (Female 17).

kids are all wrapped in cotton wool now and arnt allowed out side due to media making parents believe pedophiles are everywere. if kids had something to do (and police chilled out and wernt so enfocive over things such as riding/skating on the road) kids wouldnt even go on a computer (Male 17).

Kids need to be taught not to be idiots and make others lives a living misery. If you become a victim of cyber bullying, immediately block the person that is doing it, if it is taking place on Facebook or the like. Then report the person to your teacher or the police if it is serious enough... (Male 16).

Most people don't quite understand that there are people who can help and some people don't think the police can do anything to stop stalking or cyber bullying. Also people don't understand that it is the World Wide Web and its huge and terrifying because you just don't know (Female 16).

police should come and talk to students and should be putting fear into the bullies not the victim (Male 14).

The police came in to tell us about how 3 clicks on a girls facebook page could tell us what her house looked like and where she lived and what school she went to. enough to stalk her! I think that scared most people a bit to check their privacy settings (Female 14).

“after seeing a email about how a police person who went undercover who found out enough information about a person that they could locate there house just by saying what sport team they play for. Is is worring how easy it is to get information about people (Female aged 13).

the police should do more to protect us and teach us about all the bad things (Female 15).

the protection could be increased, by having a random conversation check, this could be done by police or any form of authorities. you could teach people to report this (Male aged 15).

There is a huge fuss over cyber-bullying. I have been an online gamer since I was 6, and cop crap every day from anonymous gamers, and I have no trouble with it, I just treat it as banter and ignore it. Although, inter school cyber-bullying is a totally different thing, and on a more serious level (especially as the bully and the victim know each other), it is quite overated. Calling names etc, is so easily blockable, and ignorable. however, when it gets to matters such as, embarrassing pictures of the victim being posted by the bully, that's when the police

should be involved straight away. I really think people my age just need to grow up (Male aged 15).

There should be a lot more police/government visits to us students at school, to help reduce the bullies and make the charges even more heavier (Female aged 15).

we need cyber police!!! (Male aged 13).

we should have the police/teachers supervise kids on the computer (Female aged 13).

Well being exposed to the internet is a bad thing because the police can get involved and shit will hit the fans i reasently got kiked out for what i did. All i can say is teach them better things make the internet safer. Protect the young people (Male aged 15).

what made me really think about and realise what some of the things i did was cyberbullying and wrong, was when we had a police officer come to our school to tell us what cyberbullying really was. this was when i realised some of the things i did were wrong and illegal (Female 17).

Concluding comments

- 12.45 Policing is an area where a great deal is happening and there is a lot of work still to be done. While legislative change is being mooted in a number of jurisdictions, the expansion of educative and restorative justice approaches provide alternative approaches.
- 12.46 Australian police forces are actively involved in a number of international law enforcement initiatives which are covered in Chapters 1 and 15.

An online ombudsman?

- 13.1 There were divergent views on the merit of establishing an office of online ombudsman to investigate, advocate and act on cyber-safety issues.
- 13.2 Those in favour saw the ombudsman as providing investigative and advocacy functions as well as presenting an opportunity for a more visible and centralised reporting place. Those opposing the proposal raised concerns about duplication of existing facilities, the actual functions of the office, jurisdictional considerations and timeliness of procedures. Some participants remained undecided, perhaps because of uncertainty about the role of the ombudsman.

Role of an ombudsman

- 13.3 The Australian and New Zealand Ombudsman Association describes the term 'ombudsman' as being 'understood by the public as signifying an independent office, which primarily has a complaint handling and investigation function'.¹
- 13.4 The Australian University Cyberbullying Research Alliance defined an ombudsman as:
- a government official responsible for impartially investigating citizens' complaints against a public authority or institution and trying to bring about a fair settlement.²
- 13.5 The Australian and New Zealand Ombudsman Association stressed that:

1 Australian and New Zealand Ombudsman Association, Media Release, 18 May 2010, *Peak body seeks to halt the misuse of the term Ombudsman*, p. 1.

2 The Australian University Cyberbullying Research Alliance, *Submission 62*, p. 47.

It is important that members of the public are not confused about what to expect when they approach an Ombudsman. Public trust in, and respect for, the Ombudsman institution generally – and its independent dispute resolution function specifically – must not be undermined. Neither should the term Ombudsman be used in a way which distorts the appropriate character of an Ombudsman office.³

13.6 It added that:

Where problems arise in an industry or an area of government services, the call for an ombudsman commonly follows. In itself, this is not a problem – indeed it is a testament to the high level of public respect for the independence, integrity and impartiality of Ombudsman offices.⁴

[However] using the term ombudsman to describe an office with regulatory, disciplinary and/or prosecutorial functions confuses the role of Ombudsman with that of a regulatory body.⁵

13.7 The Association outlined six essential criteria expected of ombudsman offices: independence, jurisdiction, powers, accessibility, procedural fairness and accountability.⁶ The Telecommunications Industry Ombudsman summarised these attributes as:

- *independence* - the office of the Ombudsman must be established by legislation or as an incorporated or accredited body so that it is independent of the organisations it investigates;
- *jurisdiction* - the jurisdiction should be clearly defined in legislation or in the document establishing the office and should generally extend to the administrative actions or services of organisations falling within the Ombudsman's jurisdiction;
- *powers* - the Ombudsman must be able to investigate whether an organisation within jurisdiction has acted fairly and reasonably in taking or failing to take administrative action or in providing or failing to provide a service;

3 Australian and New Zealand Ombudsman Association, *Submission 53*, p. 1.

4 Australian and New Zealand Ombudsman Association, Media Release, 18 May 2010, *Peak body seeks to halt the misuse of the term Ombudsman*, p. 1.

5 Australian and New Zealand Ombudsman Association, Media Release, 18 May 2010, *Peak body seeks to halt the misuse of the term Ombudsman*, p. 1.

6 Australian and New Zealand Ombudsman Association, Media Release, 18 May 2010, *Peak body seeks to halt the misuse of the term Ombudsman*, p. 1.

- *accessibility* - there must be no charge to a complainant for the Ombudsman's investigation of a complaint;
- *procedural fairness* - the actions of the Ombudsman and staff must not give rise to a reasonable apprehension of partiality, bias or prejudice; and
- *accountability* - the Ombudsman must be accountable to the Parliament if it is a Parliamentary Ombudsman and to an independent board of industry and consumer representatives if an Industry-based Ombudsman.⁷

13.8 The Association called for stronger controls on the use of the term 'ombudsman'.⁸ The Telecommunications Industry Ombudsman added that, if the Committee recommends the establishment of an ombudsman's office, this should meet with the criteria set out by the Australian and New Zealand Ombudsman Association.⁹ Alternatively:

if the body proposed is to have other functions - including for example advocacy or regulatory functions - which would generally not be compatible with the functions of an 'Ombudsman', the TIO would strongly encourage that another and more appropriate title be used.¹⁰

13.9 The Australian and New Zealand Ombudsman Association stressed that in situations where the office of an ombudsman is under the direction or control of an industry or a government minister, they are not independent.¹¹

For example, an Ombudsman office must be established as a standalone body by way of its own Act or Constitution. Its primary responsibility must be to resolve consumer/citizen disputes, independently, fairly and reasonably and without direction.¹²

7 Telecommunications Industry Ombudsman, *Submission 46*, p. 6. The Australian and New Zealand Ombudsman Association Policy Statement provided additional explanation - Australian and New Zealand Ombudsman Association, *Submission 53*, p. 5.

8 Australian and New Zealand Ombudsman Association, Media Release, 18 May 2010, *Peak body seeks to halt the misuse of the term Ombudsman*, p. 1.

9 Telecommunications Industry Ombudsman, *Submission 46*, p. 6.

10 Telecommunications Industry Ombudsman, *Submission 46*, p. 6.

11 Australian and New Zealand Ombudsman Association, Media Release, 18 May 2010, *Peak body seeks to halt the misuse of the term Ombudsman*, p. 1.

12 Australian and New Zealand Ombudsman Association, *Submission 53*, p. 1.

The office must be truly independent from the bodies or individuals about whom complaints are made. The Ombudsman must not be – nor be able to be perceived as – an advocate for a special interest group, agency or company.¹³

13.10 The Association commended the Benchmarks for Industry-Based Customer Dispute Resolution Schemes as principles to be observed by offices which provide an external dispute resolution service for consumer complaints.¹⁴

13.11 The Attorney-General's Department made the point that:

The power of an Ombudsman generally lies in his or her ability to investigate complaints and then notify the relevant government agency or the public of the findings. The Department notes that many of the websites an Online Ombudsman would receive complaints about would have no, or only a minimal, presence in Australia. Consideration will need to be given to how an Australian Ombudsman could perform an effective oversight and investigation role in this context.¹⁵

The Department also notes that there are a range of agencies that deal with complaints about the online environment including ACMA, the AFP, ACCC and the Privacy Commissioner. In assessing the merits of establishing an Online Ombudsman, it will be important to examine how the role of this new body can be clearly delineated from the roles of existing agencies to ensure there is no confusion about where to direct complaints or delays causing by adding another layer to the current system.¹⁶

Support for an online ombudsman

13.12 The Queensland Council of Parents and Citizens' Associations supported the establishment of an online ombudsman 'to investigate, advocate and act on cyber-safety issues'.¹⁷ Australian University Cyberbullying Research Alliance also saw merit in this approach:

13 Australian and New Zealand Ombudsman Association, *Submission 53*, p. 2.

14 Australian and New Zealand Ombudsman Association, *Submission 53*, p. 2.

15 Attorney-General's Department, *Submission 58*, p. 9.

16 Attorney-General's Department, *Submission 58*, p. 9.

17 Queensland Council of Parents and Citizens' Associations Inc, *Submission 99*, p. 2.

... to advocate and act on cyber-safety issues, and would suggest that it could be structured in such a way that enables and promotes engagement with education/academia/research, in addition to police and industry. It would be important that it not be a figurehead solely for the police, for example.¹⁸

- 13.13 When appearing before the Senate Legal and Constitutional Affairs Legislation Committee in March 2010, Ms Susan McLean was asked of the benefits of having an online ombudsman who can advocate in respect of the social networking sites to get results and to deal with offensive material. Ms McLean commented that:

I think that would be fabulous provided that he or she had sufficient powers. If it were just someone saying, 'Look, we've got a range of issues here and we need the stuff taken down because it is clearly offensive,' and they say, 'Well, it's within our operating guidelines and we self-report,' you are not going to achieve anything. I think it is imperative that they be equipped with the correct tools ... In the last 10 days I have had four calls from people extremely distressed by the fact that they have repeatedly – in excess of 10 times each – contacted Facebook to get content removed, being threatening content against a principal, content against a schoolteacher ... – and two high-profile AFL identities who have had impostor profiles set up. They were all at their wit's end given the fact that they had reported it and reported it and nothing had been done, the content was still there. They were concerned for the safety and welfare of the people that were attaching themselves to friends on the impostors' profiles. In the case of the principal and the schoolteacher, there were serious welfare considerations as well. I deal with this on a weekly basis. When I was a police officer I could do something ... Whilst the line on Facebook is 'we take your privacy seriously and we will actively look at your complaints and act promptly', they do not. ... I think that a government appointed official with some teeth and some power would be an excellent idea.¹⁹

- 13.14 The Young People Big Voice group comprises 14 to 20 year olds and was formed to provide advice to the Centre for Children and Young People by

18 The Australian University Cyberbullying Research Alliance, *Submission 62*, p. 47.

19 Ms Susan McLean, *Transcript of Evidence*, 9 March 2010, Senate Legal and Constitutional Affairs Legislation Committee, Reference: *Criminal Code Amendment (Misrepresentation of Age to a Minor) Bill 2010*, p. 9.

advising and collaborating on research activities and advocating to Government on important issues:

YPBV members are generally supportive of the idea of an Online Ombudsman to investigate, advocate and act on cyber-safety issues. YPBV recommend that one of the functions of an Online Ombudsman be to facilitate Australian children to share their views on developing effective responses in relation to issues of cyber-safety.²⁰

13.15 Mr Johann Trevaskis also supported the establishment of an ombudsman position:

If nothing else, it will offer a central collection point for real data about cyber-safety issues, so that future government policy can be based on good information about what cyber-safety issues arise and with what frequency.²¹

Parents and/or children may be more comfortable reporting an incident to an Ombudsman rather than to the police, which may be more intimidating or may be perceived as an overreaction.²²

13.16 He also provided some qualifications in relation to:

- the necessity to implement procedures for the exchange of information between the ombudsman and the police;
- the Ombudsman can advocate with online service providers but any attempt at enforcement is likely to be unhelpful (any breach of actual law should be left to law enforcement and the justice system); and
- statistical information about number and type of issues notified to the Ombudsman (via whatever mechanism) should be reported annually to the public, and to the parliament.²³

13.17 The System Administrators' Guild of Australia supported the establishment of an independent online ombudsman:

As in the telecommunications industry, the ombudsman's primary responsibility should be in advocating for users and other stakeholders and in resolving user concerns. Further, SAGE---AU believes that the ombudsman's responsibility should be to advocate to government and law enforcement, and within Internet

20 Centre for Children and Young People, *Submission 31*, p. 3.

21 Mr Johann Trevaskis, *Submission 40*, p. 2.

22 Mr Johann Trevaskis, *Submission 40*, p. 2.

23 Mr Johann Trevaskis, *Submission 40*, p. 2.

centric industries, on matters pertaining to Internet usage education and policing.²⁴

- 13.18 The Office of Youth South Australia saw the establishment of an ombudsman office as a step towards addressing the lack of a:

clear agency responding to cyber-safety issues and quite a bit of public confusion about who to go to for help. Additionally, there is public concern that police responses are not always adequate and often when people do seek help, there is little that can be done and the individual is left feeling frustrated that there is no one to follow up and resolve their concerns.²⁵

- 13.19 Brilliant Digital Entertainment referred to the absence of an:

independent position that rises above the opposing position and competing vendors that would enable on-line safety to become a fundamental right rather than wishful thinking.²⁶

The proposed role of Online Ombudsman has the potential to have a far reaching effect not only on the safety of on-line activity but also make a positive contribution to Australia's digital economy.²⁷

- 13.20 It called for the role to be sufficiently empowered to influence the online environment and the powers of the ombudsman 'to reach across a wide variety of organisations and take innovative or creative actions'.²⁸ It further commented that:

In order to achieve the full potential of this role the Ombudsman should have the capacity to influence or act jointly with a range of stakeholder organisations such a law enforcement agencies, a variety of other ombudsmen, certain government agencies and have enforceable investigative and dispute resolution powers. The role should have the authority and obligation to submit amicus curiae briefs in Court matters likely to have an impact or otherwise influence the course of internet activity including e-commerce, law enforcement and content distribution.²⁹

24 System Administrators' Guild of Australia, *Submission 71*, p. 8.

25 Office of Youth South Australia, *Submission 98*, p. 5.

26 Brilliant Digital Entertainment, *Submission 102*, p. 9.

27 Brilliant Digital Entertainment, *Submission 102*, p. 9.

28 Brilliant Digital Entertainment, *Submission 102*, p. 10.

29 Brilliant Digital Entertainment, *Submission 102*, p. 10.

- 13.21 It was submitted to the Committee that an ombudsman could provide ‘another legal avenue to bring content providers like Google to heel when it comes to upholding their Terms of Service’ and to deal with persistent spammers through the appropriate channels.³⁰ Further:

the legislation covering this would be very important to get right, and give the Ombudsman certain powers of jurisdiction when it comes to content. I believe that the Gutnick case could well be useful in this regard. Expanding this decision into a workable visible law applying to the Internet in Australia could have the world sitting up and taking notice. If we get it right, we could set the standard for genuine and workable cyber safety.³¹

- 13.22 Ms Catherine Davis from the Australian Education Union saw the online ombudsman as part of potential measures to mitigate some of the anti-social behaviour.³²

Those opposing the establishment of an ombudsman

- 13.23 The ACT Council of P & C Associations called for ‘a firm strategic stance to pressure websites that are popular with children to introduce sufficient privacy and safety protocols’ and stated that:

Council recognises that the government has limited power in patrolling the internet and therefore it should take a moral stance against offending websites rather than fund an online ombudsman.³³

- 13.24 The Council was not convinced that the position would have meaningful power, and added that:

Unless a site is Australian registered, an online ombudsman will have no power to enforce control over online material or proceed with any further action. Illegal content on Australian sites can already be raised with the ACMA. But, in terms of offensive material, it is difficult to see how an ombudsman

30 Name withheld, *Submission 106*, p. 4.

31 Name withheld, *Submission 106*, p. 4.

32 Ms Catherine Davis, Federal Women’s Officer, Australian Education Union, *Transcript of Evidence*, 30 June 2010, p. 4.

33 ACT Council of P&C Associations Inc, *Submission 41*, pp. 3-4.

could have any power to control what is posted on websites, particularly if hosted overseas.³⁴

- 13.25 The ACT Council of P & C's Associations suggested a more productive approach would be :

for the government to urge the owners of websites 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.³⁵

- 13.26 Yahoo!7 commented that:

We remain committed to making the Internet a safer place for all users, especially those who are more vulnerable such as children, and working with government and community stakeholders to take positive steps forward in this respect. Whilst we would be very happy to consider ways in which government, industry and relevant communities could work in a more coordinated manner towards this goal, we are not convinced that the appointment of an Online Ombudsman would be an effective step in the right direction.

- 13.27 Yahoo!7 also referenced the work of industry in promoting safe online environments for users:

At present, most of industry work both individually and collectively with various government departments who have an interest in cyber-safety and have informal processes in place to deal with issues as they arise. All websites should have mechanisms in place which allow users to report illegal or offensive content directly to them in order that the content can be taken down expeditiously. We appreciate that awareness of these mechanisms may not be top of mind for some people and the Internet Industry Association is currently preparing a reference guide which identifies how to escalate these sorts of issues for each of the more popular social networking websites. We fear that the scope of work which would logically be tasked to an Online

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

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

Ombudsman may be duplicative and ignorant of relationships and processes that are already in place. We are also mindful of the fact that many of the more popular social networking services (where safety concerns are of greater concern) are operated out of the United States and an Online Ombudsman may not have jurisdiction to actually compel these companies to take action where there has not been a breach of the website terms of use. Lastly, whilst we think that coordination between government, industry and community stakeholders could be better coordinated and harnessed, we would rather see the investment that would be required to establish an Online Ombudsman's office used to supplement funding to existing organizations that are doing very important work in this area such as law enforcement agencies and the ACMA.³⁶

13.28 Telstra Corporation also made the point that:

the appointment of a separate Online Ombudsman is not required but such a function could be co-ordinated by the Australian Communications and Media Authority (ACMA) within the existing Australian legislative framework. ... Telstra understands concerns about the need for a cohesive, integrated contact point to investigate, advocate and act on Cyber-Safety issues. In Telstra's view this function could be co-ordinated by the Australian Communications and Media Authority (ACMA) within the existing Australian legislative framework, without the need to appoint a separate Online Ombudsman. Challenges would arise in executing such a function and in ensuring effective remedies given jurisdictional limitations in relation to content hosted offshore. In this respect, the ACMA is well-positioned to coordinate with its counterparts overseas. Cooperative and more informal processes established between industry, the ACMA and Government will ensure that these challenges can be managed quickly as they arise.³⁷

13.29 The Australian Library and Information Association believes that:

the Australian Communications and Media Authority is already fulfilling the functions of an ombudsman such as investigating, advocating and acting on cybersafety issues. Therefore, we do not support the establishment of an Online

36 Yahoo!7, *Submission 2.1*, p. 1.

37 Telstra, *Submission 14*, pp. 2-4.

Ombudsman which may cause confusion for concerned parents and users in the community.³⁸

- 13.30 The Australian Federal Police (AFP) did not see a need for an additional 'reporting point or investigative structure dedicated solely to cyber safety':

Rather the need is to consider an enhanced coordination, longer term evaluation and policy synergies of existing or proposed cyber safety programs.³⁹

- 13.31 In response to a question on the usefulness of an online ombudsman, Commander Taylor of the AFP told the Senate Legal and Constitutional Affairs Legislation Committee that:

My concern would be that there is a possibility that crimes would not be reported as quickly as they should be or could be. If parents are concerned that an offence is occurring, we would want that to be reported as quickly as possible so that any action that has to be taken can be taken. I am not sure if an ombudsman could add anything further than the current regime we have already got in place.⁴⁰

- 13.32 The Communications Council was of the opinion that:

rather than establishing a new body such as the Ombudsman, which may make matters increasingly complex, options in which cyber safety issues are tackled through existing structures should be explored... The Council would support an option which would see relationships between existing enforcement agencies and publishers be strengthened.⁴¹

- 13.33 The Association of Independent Schools of South Australia commented that:

Whilst the safety of students in Independent schools is paramount, member schools expressed concern that establishing an Online Ombudsman may not be the most effective way to ensure students remain safe from cyber-harm... The application of an

38 Australian Library and Information Association, *Submission 16*, p. 13.

39 Australian Federal Police, *Submission 64*, p. 25.

40 Commander Stephanie Taylor, Australian Federal Police, Hansard 9 March 2010, Senate Legal and Constitutional Affairs Legislation Committee, Reference: *Criminal Code Amendment (Misrepresentation of Age to a Minor) Bill 2010*, p. 13

41 The Communications Council Inc, *Submission 65*, pp. 6-7.

administrative/regulatory approach to cyber-safety is not considered the most appropriate risk management strategy.⁴²

13.34 This Association added that:

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. This is an alternative to the establishment of an Online Ombudsman that the AISSA may support.⁴³

13.35 The Internet Industry Association made the point that informed users already have the ability to respond to misuse of social networking sites as most popular social websites already have such services within their networks.⁴⁴ The Association also advised that:

At present, understanding and appreciation of such resources is uneven. In conjunction with the Government, schools and the community, the IIA proposes improved education on such facilities... The IIA understands the case for an Online Ombudsman is inspired in part on the effectiveness of our local telecommunications, banking, insurance and other utility ombudsman-like offices.⁴⁵

In principle, they often operate as a 'last resort' grievance service. This means that if a user complains to an ombudsman before taking their complaint to the service that caused the issue in the first place, they may only waste time getting their complaint processed. In other words, an Ombudsman may add another layer of regulation which may slow the response time for legitimate complaints to be dealt with by relevant providers.⁴⁶

We note that law enforcement agencies have generally praised the responsiveness under existing informal protocols with the main social media sites. We would not like to see anything undermine or add complexity to those arrangements. There is no evidence of systemic failure such as to warrant the establishment of such an office... In addition where a jurisdiction crosses borders there is a risk that an Online Ombudsman may offer only symbolic

42 Association of Independent Schools of South Australia, *Submission 19*, p. 3.

43 Association of Independent Schools of South Australia, *Submission 19*, p. 15.

44 Internet Industry Association, *Submission 88*, p. 10.

45 Internet Industry Association, *Submission 88*, p. 10.

46 Internet Industry Association, *Submission 88*, pp. 10-11.

assurance as they may not have any powers beyond that of publicity where a complaint is well-founded.⁴⁷

13.36 This Association did not support the 'establishment of an online ombudsman until it can be established that such a role will add value to online safety and avoid adding delay to current processes'.⁴⁸

13.37 ninemsn stated that:

Our preliminary view is that an ombudsman would duplicate the reporting mechanism already in place by ACMA in relation to inappropriate content. In terms of the more pernicious online offences, ninemsn believes that the Australian Federal Police remains the most appropriate forum for investigation and prosecution.⁴⁹

13.38 Web Management InterActive Technologies commented that:

Until there is a framework which encourages a Protective environment, any such position would run the risk of holding a great deal of responsibility and yet have little in the way of mechanisms in which to achieve any real goals. It would be a little like putting a policeman in the middle of the highway with no uniform, no tools of the trade and no respect from the passing traffic. There is much more to do before we reach the point of establishing that position.⁵⁰

13.39 The jurisdiction of an ombudsman was also questioned because of international online developments.⁵¹ The question was raised as to what an online ombudsman regulates:

In circumstances where globally acceptable benchmarks for bad conduct are breached, such as murder, theft, drug offences or other crime, extradition treaties are entered into for the purposes of mutually dealing with offenders. This spirit of cooperation between independent sovereign jurisdictions who have the same or similar values about human behaviour, is not repeatable when it comes to the Internet because of how different our approach is... In circumstances where law has genuinely been broken, the police are able to cooperate internationally with their counterparts

47 Internet Industry Association, *Submission 88*, p. 10.

48 Internet Industry Association, *Submission 88*, p. 11.

49 ninemsn, *Submission 91*, p. 6.

50 Web Management interactive technologies, *Submission 96*, p. 9.

51 Mr Geordie Guy, *Submission 105*, p. 16.

overseas (our AFP are well regarded internationally on these issues). What would an online ombudsman bring to the situation?... An online ombudsman would be wholly ineffectual, or be nothing more than a figurehead.⁵²

13.40 The Consultative Working Group on Cybersafety commented that:

Many websites operate on a global basis and often only have a minimal presence in Australia. The CWG considers there would be significant limitations as to what an Australian Ombudsman can legally oversight and report on. In addition, without jurisdiction over sites hosted outside Australia, the scheme would rely on voluntary compliance without any guarantees that this would occur which would in turn undermine the effectiveness of an Online Ombudsman.⁵³

13.41 The Working Group added that:

In Australia there are already several mechanisms for dealing with online complaints established by the ACMA, the AFP, ACCC, and the Privacy Commissioner. Establishing yet another mechanism may exacerbate existing confusion in the minds of the public as to where to direct complaints and potentially add time and complexity to complaint resolution without necessarily improving outcomes for consumers. It would be necessary to clarify the existing roles and look at ways of removing duplication if an Online Ombudsman were introduced.⁵⁴

13.42 It concluded that:

there are other ways to safeguard the interests of consumers, as has occurred overseas. For example, the European Union's Safer Social Networking Principles, which most major social networking sites have signed up to, provide an alternative and means of regulating the sector. Approaches such as this need to be explored further as they are more likely to include a larger proportion of the internet community.⁵⁵

13.43 The Association of Independent Schools South Australia outlined a number of existing mechanisms which facilitate the investigation and reporting on cyber-safety issues:

52 Mr Geordie Guy, *Submission 105*, p. 16.

53 Australian Government's Consultative Working Group on Cybersafety, *Submission 113*, p. 38.

54 Australian Government's Consultative Working Group on Cybersafety, *Submission 113*, p. 38.

55 Australian Government's Consultative Working Group on Cybersafety, *Submission 113*, p. 39.

The requirements of school registration set out by the [Non-Government Schools Registration Board] ensure that child protection and anti-bullying and harassment policies are in place in all schools to protect students from harm, including cyber-harm.⁵⁶

The Association does not support duplication of policies and processes. Enhanced red tape will not enhance the effectiveness of strategies to ensure cyber-safety.⁵⁷

When serious incidents that compromise student safety occur, the Police are contacted and take carriage of incidents. There is also legislation in place to support victims of cyber harm, such as harassment and defamation laws.⁵⁸

At a local level, schools have developed policies to follow when managing incidents of cyber-bullying and abuse. In incidents involving students, there is usually a broader context that needs to be considered with schools often being in the best position to consider this. Schools can implement a supportive set of strategies, with the support of Police or others if required, without the heavyhanded approach an Ombudsman may introduce.⁵⁹

- 13.44 Further, the Association of Independent Schools of South Australia did not support the establishment of an 'Online Ombudsman as the overarching advocacy body for this area without further evidence to support that it would have a positive impact on eliminating cyber-safety issues', and added:

In issues between students, it is sometimes the case that the aggrieved student and parents remain dissatisfied with the outcome, regardless of the process taken. If an external body such as an Online Ombudsman is readily available to handle complaints, parties may be less willing to resolve the matter at a local school level. Schools are concerned that parents and students may not use their best endeavours to resolve the issues at a school level and escalate matters unnecessarily.⁶⁰

The AISSA also expresses concern that an Online Ombudsman may not be the most efficient administrative process by which to

56 Association of Independent Schools South Australia, *Submission 19*, pp. 14-15.

57 Association of Independent Schools South Australia, *Submission 19*, p. 15.

58 Association of Independent Schools South Australia, *Submission 19*, p. 15.

59 Association of Independent Schools South Australia, *Submission 19*, p. 15.

60 Association of Independent Schools South Australia, *Submission 19*, p. 15.

report incidents of cyber harm. It may in fact slow down the process of reporting, investigating and acting upon issues, when cyber-safety is an area that moves rapidly and needs to be constantly monitored and managed. In addition, schools may be reluctant to involve an Ombudsman because of the perceived additional administrative duties associated with this process. Teachers may also be confused about their role in the investigation and management of incidents because of a perception that an Ombudsman will solve the problem. Consequently, incidents may go undetected, unreported and unresolved.⁶¹

The Association is also concerned about the negative impact on young people resulting from being involved in a legalistic process and the associated administrative burden that would be generated.⁶²

- 13.45 The Department of Broadband, Communications and the Digital Economy commented that:

looking at the incidents that have led to the call for an ombudsman. I am not aware of one incident where the material that was of concern was not hosted on an offshore website, such as Facebook, which makes the question of extraterritoriality very difficult. That is the first issue that would have to be dealt with. The second side of it, as you have rightly pointed out, is that there are already a number of Commonwealth agencies that have a role in taking and dealing with complaints in this space, including the ACMA, the AFP and the ACCC. We are not aware of a type of complaint in this space that would not fall within the jurisdiction of one of those three agencies – if it were not an extraterritoriality issue.⁶³

Other options

- 13.46 The Association of Independent Schools of South Australia would prefer to see an:

61 Association of Independent Schools South Australia, *Submission 19*, p. 15.

62 Association of Independent Schools South Australia, *Submission 19*, p. 15.

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

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... Currently in South Australia, mandatory reporting requirements exist for teachers and others in relation to suspected physical, emotional and sexual abuse and neglect. This could be extended to include online maltreatment or abuse, though this would require extensive consultation and negotiation with states. Any variation to the mandatory reporting laws would need to be supported by adequate funded training of teachers to recognise and report incidents of cyber-harm. This could be an alternative to introducing an Online Ombudsman.⁶⁴

- 13.47 The Alannah and Madeline Foundation advocates a broad community change approach to cyber-safety through the empowerment of young people and adults to keep themselves safe and to deal with online risks. This includes the ability to report and seek support when risks and potential harm are identified.⁶⁵ The Foundation added that:

When in immediate danger, the advice always given is to call 000. Children and young people are always encouraged to seek help from a trusted adult. Help Line and Kids Helpline receive calls regarding cyberbullying and cybersafety issues. Social networking sites also have mechanisms on their sites for reporting cybersafety issues... There are currently a number of other, more specialised, mechanisms for reporting cybersafety issues, including reporting to the Australian Communications and Media Authority (ACMA) issues around cybersafety and inappropriate content, reporting to the Privacy Commission concerns around breaches of privacy, reporting to the Australian Human Rights Commission complaints of discrimination and human rights breaches, and reporting potential criminal activity and illegal content to the Australian Federal Police.⁶⁶

- 13.48 The Foundation advocated that any new mechanism being considered for investigating, advocating and acting on cybersafety issues should consider the significant resources, support and expertise already available and 'should include how these current mechanisms can be better harnessed, coordinated and communicated'.⁶⁷ Rather, the existing avenues of

64 Association of Independent Schools South Australia, *Submission 19*, pp. 15-16.

65 Alannah and Madeline Foundation, *Submission 22*, p. 42.

66 Alannah and Madeline Foundation, *Submission 22*, p. 42.

67 Alannah and Madeline Foundation, *Submission 22*, p. 42.

complaint, reporting and redress could be strengthened by an appropriate legal framework for bullying, cyberbullying and other cyber-risks – a change that ‘is fundamental for an effective response to cybersafety issues’.⁶⁸

Those undecided

13.49 Netbox Blue did not have a firm view on establishing an online ombudsman, but saw that a similar office to the Banking, Insurance or Telecommunications Industry Ombudsman may be helpful.⁶⁹ It qualified this by adding that:

the fact that legal jurisdiction is uncertain especially for the most popular networking sites, could lead to merely another layer of mediation without any real power.⁷⁰

13.50 Netbox Blue also cautioned that:

It is something that would require legal coordination across several international borders. It would be useful to clarify where the gap exists and how an online ombudsman can fulfil such roles as against other mediation options available.⁷¹

13.51 The Australian Communications Consumer Action Network commented that:

There are many different agencies involved in promoting e-security and cyber-crime awareness – the ACCC, BDCDE, the Australian High Tech Crime Centre – and we expect these agencies will have undertaken assessments of the effectiveness of their campaigns and messages.⁷²

13.52 The Australian Education Union suggested ‘a feasibility study into the role, powers and objectives of an online ombudsman in preference to a mandatory ISP-level filtering policy’.⁷³

13.53 Though undecided about an online ombudsman, Professor Bjorn Landfeldt commented that:

68 Alannah and Madeline Foundation, *Submission 22*, p. 42.

69 Netbox Blue Pty Ltd, *Submission 17*, p. 6.

70 Netbox Blue Pty Ltd, *Submission 17*, p. 6.

71 Netbox Blue Pty Ltd, *Submission 17*, p. 6.

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

73 Australian Education Union, *Submission 11*, p. 5.

I believe that cyberbullying – and bullying as a wider matter than just cyberbullying – is something that needs attention and more concerted effort than putting out little fires here and there. The Children’s Ombudsman in Sweden is a fantastic institution. It provides many more services. It provides a safety net and a voice for children in society that I have not experienced in Australia ... because children are well aware that the ombudsman is a point of contact; everyone is aware of that. It is not hard to get to the ombudsman as a child and go there with any concern. The ombudsman deals with children.⁷⁴

Conclusion

- 13.54 While there was considerable support throughout the Inquiry for a centralised reporting authority, the evidence supporting the formation of an online ombudsman position was mixed. Those strongly supporting the ombudsman approach appeared to recommend such an office assume reporting, investigative and advocacy roles, rather than those of an ombudsman *per se*.
- 13.55 It was not evident to the Committee that, in attempting to increase cyber-safety for the community, evaluations of the effectiveness of existing campaigns and the resultant proposals for improvement had been adequately brought together for the benefit of stakeholders. Therefore there is a need for better coordination. The question remains as to how a central organisation should be managed and the designation of a formal figurehead. The role of an ombudsman may be too restrictive to achieve this goal.

74 Associate Professor Bjorn Landfeldt, University of Sydney, *Transcript of Evidence*, 24 March 2011, pp. CS25-26.

PART 5

Australian and International Responses

Australian responses to cyber-safety issues

- 14.1 Australia's response to cyber-safety issues has been largely educational. International responses to cyber-safety issues will be set out in Chapter 15.

Australian Government responses

- 14.2 Responses to the range of cyber-safety issues are fragmented across agencies and jurisdictions.

Australian Communications and Media Authority

- 14.3 The Australian Communications and Media Authority (ACMA) is located within the Department of Broadband, Communications and the Digital Economy. It is responsible for the regulation of broadcasting, radio-communications, telecommunications and online content. This includes the Internet, radio and TV, phones and licences for consumers and industry.
- 14.4 ACMA has a range of important, free resources in place to improve cyber-safety: a Cyber Safety Help Button was launched at the end of 2010, while a collection of programs has been in operation for some time.
- 14.5 Since 2000, it has undertaken a sequence of research projects exploring children's use of online technologies, with a focus on the home environment.¹
- 14.6 It has also conducted a three-year program of research examining developments in safety initiatives around the world aimed at protecting both minors and adults.²

1 Australian Communications and Media Authority, *Submission 80*, pp. 3-5.

- 14.7 In addition to its research and promotional activities, ACMA has other resources :
- The *Cybersmart* website and the suite of education resources for young people and teachers contained on that site;
 - Professional Development for Educators;
 - Internet Safety Awareness Presentations for students, parents and teachers;
 - Pre-service teacher training program; and
 - The public libraries suite of resources.³
- 14.8 As already noted, at the National Day of Action Against Bullying and Violence on 18 March 2011, it staged a national *Cybersmart Hero* event created to tackle cyber-bullying. This is a one-hour, in-school, on-line activity for students in Years 5 and 6 that addresses the responsibilities of the people in the best position to influence bullying and cyber-bullying: the bystanders.
- 14.9 On 18 March, ACMA also provided a suite of lesson plans for teachers on how to prevent and manage cyber-bullying. These plans bring the discussion into the open, and encourage students to tell their parents/carers or teachers when they are aware of cyber-bullying.⁴
- 14.10 Under the *Broadcasting Services Act 1992* (Cth), ACMA has the regulatory responsibility for a hotline where complaints can be made about offensive and inappropriate content. It has observed a 'steady increase' in the number of complaints, particularly relating to online child abuse and child sexual abuse material hosted overseas.⁵ It is the primary agency for removing online content and works with the Australian Federal Police (AFP), which assess information to decide whether there should be an investigation. If a website is hosted offshore, these authorities are limited in what they can do.⁶
- 14.11 Roar Educate commented that ACMA's predominant resources were derived from the United Kingdom's Child Exploitation and Online Protection Centre, and have been available for 'five or six years'.⁷

2 Australian Communications and Media Authority, *Submission 80*, p. 2.

3 Australian Communications and Media Authority, *Submission 80*, p. 5.

4 *acma(sphere)*, Issue 62, April 2011, p. 6.

5 Australian Communications and Media Authority, *Submission 80*, p. 8.

6 Australian Communications and Media Authority, *Submission 80*, p. 8; Australian Federal Police, *Submission 64*, p. 7.

7 Mr Craig Dow Sainter, Managing Director, Roar Educate, *Transcript of Evidence*, 20 April 2011, pp. CS28-29.

Cybersmart programs

14.12 ACMA pointed out that its research programs had been progressively redesigned to incorporate the views of children and young people, with findings indicating that issues such as cyber-bullying have been of increasing concern. *Click and Connect: Young Australians' use of online social media* sought to understand the extent to which young people use social networking and their experiences in dealing with risks online.⁸

14.13 The Cybersmart website is the cornerstone of ACMA's *Cybersmart* program. It acts as a 'one-stop' shop for general cyber-safety information, with information targeted to six specific audiences:

- 'young children' (not defined);
- children;
- teenagers;
- parents;
- teachers; and
- librarians.⁹

14.14 Under the *Cybersmart* brand, ACMA delivers a 'diverse, comprehensive and effective range' of programs and resources tailored to meet the needs of teachers, parents/carers, librarians and young people.¹⁰ These programs have proven to be 'extremely popular' and continue to be in high demand.¹¹

14.15 It noted that online safety messaging had generally assumed that any degree of risk was negative, while emerging research suggested that a certain level of risk taking was necessary for the development of resilience in young people.¹² Its research programs had therefore been progressively redesigned to incorporate the views and experiences of young people.

14.16 Since 2009:

- There have been 2,335 separate Internet Safety Awareness presentations and professional development workshops, with participants from over 3,300 schools;

8 Ms Andree Wright, Acting General Manager, Digital Economy Division, *Transcript of Evidence*, 3 March 2011, p. CS3.

9 Australian Communications and Media Authority, *Submission 80*, p. 21.

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

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

12 Australian Communications and Media Authority, *Submission 80*, p. 6.

- 263,000-plus teachers, students and parents have attended one hour general Internet safety awareness presentations;
- Over 7,500 teachers have participated in free full-day professional development workshops;
- There have been 6.6 million page views of the *Cybersmart* website; and
- More than 2.6 million hard copy *Cybersmart* resources have been distributed to schools, community groups and families across Australia.¹³

14.17 ACMA noted that its resources continued to be in 'high demand', and were 'widely acknowledged' as based on evidence and world-class. Tributes were paid to the quality and range of its material.¹⁴

Cybersafety Help Button

14.18 The Cybersafety Help Button launched on 10 December 2010 was developed in response to advice from the Youth Advisory Group. This body said that it would like a 'one-stop-shop' for cyber-safety advice and assistance.¹⁵ The Button provides users, particularly children and young people but also parents/carers and teachers, with easy online access to a wide range of cyber-safety and security resources to help with cyber-bullying, unwanted contacts, scams, frauds and inappropriate material.¹⁶

14.19 The Department of Broadband, Communications and the Digital Economy commented that:

We have taken very seriously the advice that the children have given us. Indeed, the button was as a result of their advice. They said, 'Look, it's all bewildering. We don't know where to go. You can't expect us to remember all these government websites. They're changing all the time. We're confused. We want a one-stop shop. Make it easier for us so that we can press the one button

13 Ms Andree Wright, Acting General Manager, Digital Economy Division, *Transcript of Evidence*, 3 March 2011, p. CS3.

14 Ms Andree Wright, Acting General Manager, Digital Economy Division, *Transcript of Evidence*, 3 March 2011, p. CS4.

15 Australian Government's Consultative Working Group on CyberSafety, *Submission 113*, p. 7.

16 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS2.

and go to all the sites that are relevant. That would make life a lot easier.’ So we proceeded to develop the button.¹⁷

14.20 This Help Button is based around three actions that a user can take if there are concerns about material online:

- talking to a professional, either over the phone or online;
- reporting matters that may be of concern to a range of agencies; and
- learning about cyber-safety.

14.21 There are also proposals to extend the features of the Help Button. For example, social networking site and games that are popular with children have conditions of use which are long, detailed and legalistic:

It is very difficult for a 12-year-old to try to understand all of that legalistic language. More often than not, they will just scroll to the bottom of the page and click ‘I Agree’ and then proceed, and they will not read it. But they are saying, ‘Sometimes I am clicking yes to something and I have no idea what I’m doing but, because my mate did it ... they were looking for was some easy way in which they could understand the key features of each of the different social networking sites and popular games: some really simple, attractive format. So we are looking to add as a feature of the button an ability for children – and, indeed, parents and teachers, if they wish – to find out about the latest game or the latest social networking site and what the key features of it are and what they need to understand about it. That will, I think, assist both children and parents when they make the decision about it. It is an often difficult decision when the child says, ‘I want to play this’ or ‘I want to go on that. Am I allowed?’ and the parent says, ‘I am not sure. I don’t know what you’re talking about.’ This may help parents by providing them with some sort of guide in that regard.¹⁸

14.22 While user downloads continue to increase, numbers do not accurately reflect actual usage, as the Help Button can be downloaded once and applied to multiple sites or computers.

17 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS22.

18 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS22-23.

- 14.23 The Department is seeking to expand progressively what is behind the three actions already on the Help Button. Work has also begun on a second stage that will include an application compatible with mobile platforms and browser-level applications. This work is expected to be completed in the second half of 2011. It is also intended to add advice on the range of options that are available about localised filtering systems.¹⁹
- 14.24 Promoted by members of the Consultative Working Group on Cybersafety, the Help Button has been downloaded by the Queensland Department of Education and Training across its network and is available on over 177,000 computers in that State. There are, therefore, 'at least 200,000' of these Buttons on a range of computers around Australia. Other State/Territory school systems have been encouraged to adopt the Help Button, as have libraries.²⁰
- 14.25 BraveHearts believes that online reporting systems are important tools in responding to child exploitation. The use of hotlines provided an alternative to reporting to law enforcement agencies to which people may be reluctant to report illegal content.²¹
- 14.26 The South Australian Office for Youth was critical of the Help Button because it believed that, although there is a button to report matters online, it goes to a page that is not 'very user friendly'. While it might be downloaded by parents/carers, doubts were expressed that young people would download or use it.²²

Consultative Working Group on Cybersafety

- 14.27 The Consultative Working Group on Cybersafety is an initiative of the Government's Cybersafety Plan. It includes representatives of industry and community organisations, and Australian government agencies. Chaired by a senior officer of the Department of Broadband, Communications and the Digital Economy, its roles are to:
- Consider all aspects of cyber-safety faced by Australian children;

19 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS2-3, 21, 23.

20 Ms Patrea Walton, Acting Deputy Director-General, Department of Education and Training, Queensland, *Transcript of Evidence*, 17 March 2011, p. CS80; Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS17.

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

22 Mrs Tiffany Downing, Director, Office for Youth SA, *Transcript of Evidence*, 3 February 2011, p. CS24.

- Provide information to Government on measures required to operate and maintain world best practice safeguards for Australian children in the digital economy; and
- Advise the Government on priorities for action by government and industry.²³

14.28 The Working Group's Terms of Reference specify six areas of focus:

- The online environment in which Australian children currently engage;
- The nature, prevalence and implications of cyber-safety risks;
- Australian and international responses to current cyber-safety risks;
- Opportunities for cooperation across Australian and international stakeholders;
- Information required to realise the potential for achieving and continuing world's best practice of safeguards; and
- Ensuring that the Group's deliberations take account of new technologies.²⁴

Department of Education, Employment and Workplace Relations

14.29 The Department of Education, Employment and Workplace Relations (DEEWR) pursues activities based on the knowledge that the well-being and safety of children and young people at school is essential for their academic development, and for that nation's ongoing economic prosperity and social cohesion.²⁵

14.30 The National Safe Schools Framework was originally endorsed by all Australian Ministers for Education in 2003. It included an agreed 'set of national principles to promote safe and supportive school environments, and appropriate responses to address bullying, harassment, violence, child abuse and neglect'.²⁶

14.31 Consultations have indicated that the National Safe Schools Framework has been an effective vehicle for raising community awareness of safe school environments. It has 'promulgated a greater understanding and

23 Australian Government's Consultative Working Group on CyberSafety, *Submission 113*, p. 1.

24 Australian Government's Consultative Working Group on CyberSafety, *Submission 113*, p. 1.

25 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 4.

26 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 7.

appreciation of the relationship between such environments, student well-being and improved learning'.²⁷

- 14.32 Following a review in 2009, a revised Framework was endorsed in 2010 and launched on 18 March 2011, to coincide with the National Day of Action Against Bullying and Violence. The revised National Safe Schools Framework will be distributed to all primary and secondary schools.²⁸
- 14.33 The Australian Government and State/Territory education authorities are represented on the Safe and Supportive Schools Communities project management group. This is a cross-jurisdictional forum enabling identification of emerging 'national priorities, sharing of knowledge and exchange of effective, evidence-based practice'.²⁹
- 14.34 This project collaborated in developing a nationally agreed definition of bullying which has been included in the revised National Safe Schools Framework. It is intended to use this definition in relevant policies and guidelines.
- 14.35 DEEWR provides funding and other support for a range of programs and initiatives, including the seven general capabilities to be addressed in the Australian curriculum:
- Literacy;
 - Numeracy;
 - ICT competence;
 - Critical and creative thinking;
 - Ethical behaviour;
 - Personal and social competence; and
 - Inter-cultural understanding.³⁰
- 14.36 The safety of young people in the online environment is paramount, and \$125.8 million has been allocated for a comprehensive Cybersafety Plan that includes:
- \$49 million over four years to the AFP Child Protection Operations Team for detection and investigation of online child sex exploitation;

27 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 7.

28 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 8.

29 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 14.

30 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 9.

- \$42.4 million over four years to develop and implement Internet service provider-level filtering;
- \$11.9 million to ACMA to implement a comprehensive range of education and outreach activities; and
- \$4.3 million to ACMA over four years to develop a new cyber-safety website with up-to-date and age-appropriate educational material, and to improve the online helpline to provide a quick and easy way for children to report online incidents that cause them concern.³¹

14.37 This Plan also recognises the value of young Australians providing advice to Government on cyber-safety issues by providing \$3.7 million over four years to the Youth Advisory Group and its online forum.³²

Attorney-General's Department

14.38 The Attorney-General's Department has released the *Protecting Yourself online – What everyone needs to know* pamphlet and has distributed 270,000 copies.³³ The *ID Theft – Protecting your Identity* booklet has had 60,000 copies distributed.³⁴

14.39 The Australian Education Union encouraged greater interagency collaboration and made the point that:

It is clear therefore that there is no shortage of effort going into policy responses to issues of cyber-safety but perhaps there is evidence of a need for greater inter-agency cooperation (given programs and policies are being released under the auspices of the Department of Broadband, Communications and the Digital Economy, the Attorney General, and to education departments) and for better engagement between schools and working within the broader community.³⁵

State and Territory Government responsibilities

14.40 Authorities in the Australian States and Territories have a range of responsibilities and programs designed to make young people safe in the

31 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 11.

32 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 11.

33 Attorney-General's Department, *Submission 58.1*, p. 1.

34 Attorney-General's Department, *Submission 58.1*, p. 1.

35 Australian Education Union, *Submission 11*, pp. 7, 9.

online environment. The submission from the Consultative Working Group on Cybersafety gave details of State/Territory programs to develop cyber-safety educational programs.³⁶

New South Wales

Education

- 14.41 Internet and online communication services are provided in NSW schools by the Department of Education and Training for research and learning and communication between students and staff. Access to the online environment assists students to develop the skills necessary for effective and appropriate use of the Internet. It also provides a context for learning about roles and responsibilities in communication, respectful relationships and personal safety.³⁷
- 14.42 The *KidsMatter* and *MindMatters* initiatives have both been informed by, and have informed, the development of the National Safe Schools Framework, with bullying and harassment as one of its target areas.³⁸ Since 2007, cyber-safety has been the focus of the bullying and harassment arm of the project. It has trained 130,000 people across the country and reached 1,500 secondary schools since 2000.³⁹
- 14.43 The Department's *Online Communication Services: Acceptable Usage for School Students* policy includes access and security, privacy and confidentiality, intellectual property and copyright, as well as misuse and breaches of acceptable use of technology.⁴⁰ As part of the curriculum, students also receive instruction in these issues.
- 14.44 Under an 'Acceptable Use' policy, students are aware that:
- they are responsible for their actions while using the Internet and online communication services, and

36 Australian Government's Consultative Working Group on CyberSafety, *Submission 113*, pp. 3-4.

37 NSW Government, *Submission 94*, pp. 2-3

38 NSW Government, *Submission 94*, pp. 23-24.

39 Mr Jeremy Hurley, Manager, National Education Agenda, Principals Australia, *Transcript of Evidence*, 11 June 2010, p. CS8.

40 NSW Government, *Submission 94*, p. 3.

- the misuse of Internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.⁴¹
- 14.45 Students are asked to report any Internet sites accessed that are considered to be inappropriate, as well as any suspected security breach from other schools, TAFE or from outside the Department.⁴²
- 14.46 Senior students in NSW schools have access to the *Digital Education Revolution-NSW* wireless network in schools. Their laptops can connect anywhere students collaborate, study and learn. This wireless network provides a secure online environment. Laptops are subject to a strict Internet filtering policy and any site not recognised is blocked, including so-called proxy sites that enable users to by-pass filters.⁴³
- 14.47 A Digital Citizenship education program has been developed that is proposed for implementation in 2011. This is a strategy to teach students the skills to be good digital citizens.
- 14.48 The Department is also represented on the *Safe and Supportive School Communities* project: a collaborative initiative of Australian governments overseeing the *Bullying, No Way!* website. In support of this initiative, schools are provided with a range of anti-bullying material.⁴⁴
- 14.49 In partnership with the Department and schools, NSW Community Justice Centres developed a Peer Mediation Program. As one of a broad range of conflict mediation strategies for schools, it was initiated in 1994 as an early intervention strategy offering an effective method of dealing with and resolving some student disputes. The issues and principles raised by cyber-bullying are similar to those encountered in bullying.⁴⁵
- 14.50 Each NSW school is required to have an anti-bullying policy and, when required, these matters are initially dealt with internally. Police liaison officers address cyber-bullying issues in schools, but an incident only becomes a police responsibility if it involved a criminal offence.⁴⁶
- 14.51 The Digital Citizenship program includes cyber-bullying as a theme in all years K-10. It promotes the expectation that all students should be active in preventing it, and understand that even single hostile cyber actions can

41 NSW Government, *Submission 94*, p. 3.

42 NSW Government, *Submission 94*, p. 17.

43 NSW Government, *Submission 94*, p. 3.

44 NSW Government, *Submission 94*, p. 17.

45 NSW Government, *Submission 94*, pp. 18-19.

46 NSW Government, *Submission 94*, p. 29.

have a widespread negative impact because of rapid dissemination and the relative permanency of sent messages.⁴⁷

- 14.52 The Department places advertisements in daily newspapers describing 'cyber bullying', explaining briefly how it occurs, pointing out measures that can be taken to reduce it and listing contacts for assistance.

Victoria

Education

- 14.53 To maximise the opportunities presented by new technologies for teaching and learning, the Victorian Department of Education and Early Childhood Development is developing the *KnowledgeBank: Next generation* portal. This will provide a range of quality assured and targeted digital resources for teaching and learning. It will also evaluate and research innovative ways to use new technologies that suited the way students learn, collaborate and network.⁴⁸
- 14.54 As part of the Government's Respect Agenda, the Department is also developing and would implement a *Respect in Schools* strategy that includes advice on dealing with bullying and Cyber-bullying. This strategy also includes reviewing the *Safe Schools are Effective Schools* policy, with a view to replacing it with: *Building Respectful and Safe Schools*.⁴⁹
- 14.55 The Learning On Line website presented advice for schools on cyber-safety and the responsible use of digital technologies. It had been developed to help schools make the most of the opportunities presented by developments in, and increased accessibility of these technologies. It also sought to support students using the online environment by minimising risks that may arise.⁵⁰
- 14.56 The Learning on Line Cybersafety pilot program focused on developing children's ability to act safely and responsibly in the online world, and to prepare them effectively to protect themselves online so they can resolve issues that may arise.⁵¹
- 14.57 The pilot program is aimed at three levels:

47 NSW Government, *Submission 94*, p. 9.

48 Victorian Government, *Submission 112*, p. 1.

49 Victorian Government, *Submission 112*, p. 2.

50 Victorian Government, *Submission 112*, p. 2.

51 Victorian Government, *Submission 112*, pp. 2-3.

- Years 3 and 4 - Cybersmart: What does it mean to be cybersmart?
 - Years 5 and 6 - Shout Out, Make a Difference.
 - Years 7 to 10 - Bystanders: What action can I take?⁵²
- 14.58 The Youth Central website is an initiative for young people aged from 12 to 25 which devoted a section to 'Cyber Smarts'. It included guidelines on how to protect young people from cyber-bullying, tips for keeping the 'person/private' balance, and how to be cyber-safe.⁵³
- 14.59 In its 2010/2011 Budget, the Victorian Government committed \$3.6 million to enable six community-based organisations to extend their cyber-safety education programs to more school age children, particularly those from diverse or marginalised backgrounds who are often at risk of bullying behaviour. It will fund those organisations to develop young leaders to work with their peers to help reduce this behaviour, and minimise its impact, by giving vulnerable young people the skills to keep themselves safe online.⁵⁴
- 14.60 In October 2009, the Department convened the Leading Responsibility in a Digital World student summit, attended by 230 Year 10 students. It facilitated discussions between adults and the young people about the issues associated with the online environment. Students summarised the day's thoughts and declared each school's commitment to take action and lead in this environment.⁵⁵
- 14.61 The Youth Affairs Council Victoria is a not-for-profit organisation funded by the Victorian Government. It has hosted events that bring together young people, teachers, service providers and researchers to examine the prevalence and impact of bullying in the State. It looked for ideas for interventions and solutions, via such forums as *The Sticks and Stones and Mobile Phones - Bullying in the New Millennium*, hosted in August 2009.⁵⁶
- 14.62 The Department is an active member of, and contributes financially to, the national *Safe and Supportive School communities: Finding Workable solutions for countering bullying, harassment and violence in schools* project for the Australian Education, Early Childhood Development and Youth Affairs Senior Official's Committee.⁵⁷

52 Victorian Government, *Submission 112*, p. 3.

53 Victorian Government, *Submission 112*, p. 3.

54 Victorian Government, *Submission 112*, pp. 3-4.

55 Victorian Government, *Submission 112*, p. 4.

56 Victorian Government, *Submission 112*, p. 4.

57 Victorian Government, *Submission 112*, p. 5.

- 14.63 This is the only national project bringing representatives together from all Australian educational jurisdictions to create safer schools free from bullying, harassment and violence. The 'well-known, respected and comprehensive' website *Bullying, No Way!* is an important result of this project.⁵⁸
- 14.64 In 2010/2011, the project will focus on strategic support for implementation of the National Safe Schools Framework and related national priorities with a range of activities.
- 14.65 Victoria actively supports the Alannah and Madeline Foundation and, in 2009, contributed \$250,000 to its *Cyber Safety and Wellbeing* pilot program, now known as the *eSmart* program. This will contribute to ensuring children benefit from the learning opportunities provided by the online environment in a safe way.⁵⁹

Queensland

Education

- 14.66 The Queensland Department of Education and Training has built a safe and secure online learning environment that all students can access from their homes. They are able to use blogs and a range of resources, as well as engage with other students through online forums. A great deal of work has been done to ensure that staff, students and parents/carers are more aware of cyber-safety and the responsible use of technology. The Department will ensure that important messages about cyber-safety continue to be shared and reinforced in school communities.⁶⁰
- 14.67 In 2010, it established the Queensland Schools Alliance Against Violence. This is a group of key stakeholders, including representatives from the State, Catholic and Independent school sectors, parents/carers, Principals' associations, unions and the Commission for Children and Young People and Child Guardian. Its purpose was to provide advice on best practice to deal with bullying, cyber-bullying and violence.⁶¹
- 14.68 The Alliance's report has been used to develop resources for use in all schools in the State. These included:
-

58 Victorian Government, *Submission 112*, p. 4.

59 Victorian Government, *Submission 112*, p. 5.

60 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, pp. CS79-80.

61 Ms Anita Smith, Senior Education Officer, Student Wellbeing, Learning and Teaching, Services, Brisbane Catholic Education, *Transcript of Evidence*, 17 March 2011, p. CS25.

- a *Declaration against Bullying and Violence*;
 - toolkits for schools and for parents, and
 - a starter kit for developing local community alliances against bullying and violence.⁶²
- 14.69 Work that has been based on the report's recommendations will be reviewed in about September 2012.
- 14.70 Students were consulted about bullying, and recommendations made by Professor Ken Rigby of were used to advise schools about tackling bullying and cyber-bullying. In 2010, Dr Michael Carr-Gregg undertook 'a large number' of valuable workshops in ten locations across the State to support and provide advice to parents/carers, teachers and school leavers about bullying and cyber-bullying. He has continued to give these workshops in 2011.⁶³
- 14.71 The Department will be in partnership with the Alannah and Madeline Foundation to provide *eSmart* to all State schools. This is a framework that guides schools to make sure that they are doing everything they can to combat cyber-bullying and promote cyber-safety.⁶⁴
- 14.72 As already noted, ACMA's Help Button has been placed on over 177,000 school-based computers in the State. All schools are required to develop responsible behaviour plans for students, and these had to be reviewed to ensure that they included strategies to deal with bullying and cyber-bullying. The enrolment process includes 'Acceptable Use' agreements with parents/carers about the use of technology by students.⁶⁵
- 14.73 The Department has a repository of resources around bullying and cyber-bullying, the '*Bullying.No Way!*' website, provided by the Australian Government under the Safe and Supportive Schools Communities project.⁶⁶

62 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, pp. CS79-80.

63 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, p. CS80.

64 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, p. CS80.

65 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, p. CS80.

66 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, pp. CS80-81.

South Australia

Education

- 14.74 The South Australian Department of Education and Children's Services recognised the issue of bullying in 1996 and detailed it in the school discipline policy. School communities are encouraged to work together to create an environment free from harassment and bullying. Since 2005, all Departmental schools have been required to have an anti-bullying policy and they are now also encouraged to have a cyber-bullying emphasis. The non-government education sector has the same requirements.⁶⁷
- 14.75 It has developed the pre-school to Year 12 package *Keeping Safe: Child Protection Curriculum*, and trained 17,000 of its 20,000 teachers in its use. The Catholic sector in South Australia is implementing it, as are schools in the Northern Territory. It is unique because it connects cyber-safety with child protection, emphasising the importance of implementing the document and teaching respect for relationships. It provides advice on Internet security, including examples of cyber-safety user agreements, and actions principals can take following a cyber-safety event. It also addresses the issue of teachers' digital footprints.⁶⁸
- 14.76 In May 2009, it advised principals on actions that they can take on cyber-bullying or electronic crime. This clarified their use of disciplinary powers, including suspension and exclusion, for events occurring beyond the school gates and outside school hours where the well being of a student, teacher or member of the school community is affected.⁶⁹
- 14.77 In 2010, the Department:
- provided \$100,000 in grants to schools to implement innovative practices. These are being written up for placement on the Department of Education and Children's Services website; and
 - collaborated with the South Australian Police to have cyber-safety as part of the two-yearly primary schools' music extravaganza.⁷⁰

67 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, pp. CS66-67.

68 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS68.

69 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS68.

70 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS69.

- 14.78 In 2005, the South Australian Government formed the Coalition to Decrease Bullying, Harassment and Violence in South Australian schools. Its initiatives have included:
- The 2006 Safer South Australian Schools Conference;
 - The pamphlet *Cyber bullying, e-crime and the protection of children and young people*, 150,000 copies of which were distributed to all schools in the State;
 - Co-ordination of National Safe Schools Weeks in 2006 and 2007;
 - Providing advice on the National Safe Schools Framework; and
 - Support for Dr Barbara Spears of the University of South Australia to gain a grant from the Commonwealth to capture stories from young people, their parents and school staff on cyber-behaviour issues. A web site was developed based on this research. Advice was provided to the school sector, including the Department's policy *Cyber-safety: Keeping Children Safe in a Connected World*.⁷¹
- 14.79 Collaboration between the three sectors, public, Catholic and independent, 'is not uncommon' in South Australia, so that a number of child protection documents are policy in all schools in the State.⁷² The Department referred to the low rate of bullying in South Australia, noting the suggestion that this was the result of initiatives already undertaken, such as the Coalition mentioned above, and collaboration between the three schooling sectors.
- 14.80 As part of registration in South Australia, teachers are required to complete *Responding to Abuse and Neglect Education and Care* training, and update this every three years. There are elements of cyber-safety in this training, as it acknowledges that teachers are required to maintain a professional; presence on the Internet. It also addresses the issue of teachers' digital footprints, including those of pre-service teachers who are likely to use social networks more often than older teachers.⁷³

South Australian Office for Youth

- 14.81 In response to a growing concern about the risks to young people associated with using social networking sites, the South Australian Office
-

71 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, pp. CS67-68

72 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS68.

73 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS69.

for Youth ran a Social Networking Education and Awareness Campaign in June 2010.⁷⁴

14.82 The temporary Safer Social Networking info-line was open from 4 to 11pm on two days, seeking:

- to provide young people and their parents/carers with the necessary information to enable a better understanding of, and to set, privacy settings on individuals' social networking sites; and
- to identify key social networking issues for young people.⁷⁵

14.83 An online survey was placed on the Office's website.

14.84 The one-stop-shop Cyber Safety Information Portal provided young people and their parents/carers with a range of information on cyber-safety.

14.85 The info-line received 27 calls, and 103 people responded to the survey. The campaign showed public concern for many of the issues raised in this Inquiry, including some that were not often publicised, such as underage users, hacking, how easy it was to lie about identity online and trusting others without knowing who they were.⁷⁶

14.86 In addition to recording concerns about general privacy and identity theft issues it also revealed two other matters. The first was the need for more education about other issues not often raised, such as:

- Knowing what to do if something happens online;
- Understanding users' rights;
- Understanding that the same rules apply online as in the 'real' world; and
- What parents/carers or grandparents can do if they are concerned about young people's online safety.⁷⁷

14.87 The second matter was enforcement. During the Campaign, the Office referred 13 callers to police or ACMA to investigate cyber-safety threats. Many of these callers had already spoken to the police and felt that their concerns had not been adequately addressed. Others had concerns, e.g. about cyber-bullying or hate pages on Facebook, but did not know who to

74 South Australian Office for Youth, *Submission 98*, p. 1.

75 South Australian Office for Youth, *Submission 98*, p. 1.

76 South Australian Office for Youth, *Submission 98*, p. 6.

77 South Australian Office for Youth, *Submission 98*, p. 4.

contact for assistance. For example, at that time, the Office believed that there was no agency clearly responsible for responding to cyber-safety threats, particularly for young people.⁷⁸

- 14.88 The Australian Education Union referred to the Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools, commenting that it:

comprises the 3 main education authorities, (DECS, Catholic Ed and Independent Schools) together with the University of SA. This coalition has produced brochures for families etc on Cyber bullying, e-crime and the protection of children and young people.⁷⁹

Western Australia

Education

- 14.89 The West Australian Education Department has implemented a tiered approach to filtering Internet access to minimise the risk of student and staff exposure to inappropriate content. It has a central filtering service blocking access to approximately 750,000 sites identified as containing content unsuitable for educational needs. This centrally-managed blacklist is linked to similar services around the world and is updated daily to reflect changes occurring on the Internet.⁸⁰
- 14.90 Each school has an Internet filter, enabling a further level of Internet access to meet local needs best.
- 14.91 Computers used on school networks are supplied with pre-configured Internet browser software default settings to block certain actions that might inadvertently lead to sexual content.⁸¹
- 14.92 A *Students Online* policy has been introduced for public schools to establish school-based procedures that both protect and inform students, and their parents/carers, about use of Departmental online services. All schools have a local policy all students are required to sign encouraging good practice and appropriate online behaviour. The Department works closely with ACMA, and has promoted its *Cybersmart* initiatives.⁸²

78 South Australian Office for Youth, *Submission 98*, p. 4.

79 Australian Education Union, *Submission 11*, p. 10

80 Western Australian Department of Education, *Submission 115*, p. 2.

81 Western Australian Department of Education, *Submission 115*, p. 2.

82 Western Australian Department of Education, *Submission 115*, pp. 2-3.

- 14.93 The Department accepted that the scale and nature of the Internet was such that no filtering mechanism could offer protection from all inappropriate content in a school. When used with user awareness, agreed operating procedures and adequate supervisory techniques in classrooms, this combination of technologies and practices provides a high level of protection.⁸³
- 14.94 The WA Government supported the Child Health Promotion Research Centre at Edith Cowan University to develop *The Cyber Bullying Formative Study (2007-2008)* to address the rise in Cyber-bullying. This study revealed that few children who had been victims of bullying online would not discuss the issue with parents/carers or teachers for fear of having mobile phones or computers removed, or because they believed that adults were unaware of the problem and did not know how to prevent it.⁸⁴
- 14.95 It provided \$400,000 for the first Youth Summit conducted by the Child Health Promotion Research Centre as part of its 2007/2008 Study. Two summits were held to identify effective and appropriate prevention and management strategies for young people, involving responses coordinated between school and families.⁸⁵
- 14.96 The first Summit enabled 200 Year 10 students to engage in problem-solving about cyber-bullying. The second was for staff and parents/carers, and the result was a Declaration presented to the Minister. The ideas outlined in this document demonstrated the willingness of young people to own a problem and develop their solutions. It also confirmed 'that student-focussed solving of problems is the most powerful strategy to combat cyber-bullying'.⁸⁶
- 14.97 A cross-sectoral and inter-agency body, the Cyber Safety for Children Working Party, has been set up, the first in Australia to establish links between stakeholders supporting schools to address online safety issues.⁸⁷ It provides a forum for the discussion and application of findings about the nature, prevalence, implications of and level of risk associated with cyber-safety threats, as well as the effectiveness of both Australian and international responses to safety threats.

83 Western Australian Department of Education, *Submission 115*, p. 4.

84 Western Australian Government, *Submission 118*, pp. 3-4.

85 Western Australian Government, *Submission 118*, p. 4.

86 Western Australian Government, *Submission 118*, p. 4.

87 Western Australian Government, *Submission 118*, p. 4.

- 14.98 The WA Government believes that this Working Party would be an effective tool to support the cultural change required in schools to reduce the effects of cyber-bullying.⁸⁸
- 14.99 The WA Education Department, the WA Catholic Education Office and the Australian Independent Schools (WA) have a close relationship with ACMA, ensuring that all their schools have access to material that it has developed.
- 14.100 The K-10 Syllabus embedded the national *Statement of Learning for Information and Communication Technologies* which included building an understanding of the legal, ethical and health and safety implications of using the online environment, and responsibilities as users and developers.⁸⁹
- 14.101 A range of evidence-based intervention plans has been developed by the Child Health Promotion Research Centre to deal with bullying, compatible with Australian curriculums, programs and practice. As these represent best practice, the WA Government believes that they should be considered for wider implementation in Australian schools.⁹⁰
- 14.102 Commissioned by the Department of Broadband, Communications and the Digital Economy, in 2009 the Child Health Promotion Research Centre conducted a review of cyber-safety literature. This provided the most recent and comprehensive review of cyber-safety issues conducted to date in Australia, including best practice safeguards.

Tasmania

Education

- 14.103 The Tasmanian Department of Education uses information and communications technology as a core skill across all areas of the curriculum. Each school develops a plan for their requirements, with a view to engaging the local community so that it is clear that responsible use of technology happens across a day, not simply during school hours. Within a safe and secure framework, schools have considerable freedom

88 Western Australian Government, *Submission 118*, pp. 4-5.

89 Western Australian Government, *Submission 118*, p. 5.

90 Western Australian Government, *Submission 118*, p. 6.

about their technology arrangements, as well as how they handle difficult issues.⁹¹

- 14.104 Parents/carers, students and teachers must all sign 'conditions of use' forms, and information sessions are organised to educate them about cyber-safety, these are not mandatory for parents/carers. However, it appears that '95-plus percent' of parents/carers sign and return these agreements, and use is made of any opportunities that arise for teachers/principals to complete the process.⁹²
- 14.105 The Department uses a filtering service provided by Telstra Corporation that allows sites to be blocked routinely, as well as individual URLs. While Web 2.0 technologies such as YouTube and Facebook are allowed into schools by default, primary students are not allowed to access Facebook because of age restrictions. A high school can decide to block Facebook but, as the aim is to educate students in the responsible use of technology, a teacher may construct a lesson using Facebook.⁹³
- 14.106 Detailed reports are kept on a range of incidents at schools, and information is therefore available on students' use of technology. Strategies are also in place within schools to support students after events that occur on social networking sites.
- 14.107 A Memorandum of Understanding has been reached with the Tasmanian Police because of concerns about the number of violent incidents being filmed on mobile phones. In operation in part of the State for two years, it is likely to be extended to the rest of Tasmania later in 2011.⁹⁴
- 14.108 When there has been a violent incident at a school, the police are notified, their processes are followed and they decide whether to take action on behalf of the Department. The police can also be involved in approaching, for example, YouTube through the AFP to remove unsavoury material.⁹⁵

91 Mr Trevor Hill, Director, Information Technology Services, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS4.

92 Mr Trevor Hill, Director, Information Technology Services, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS4.

93 Mr Trevor Hill, Director, Information Technology Services, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, pp. CS5-6.

94 Ms Liz Banks, Acting Deputy Secretary, Early Years and Schools, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, pp. CS7-8.

95 Ms Liz Banks, Acting Deputy Secretary, Early Years and Schools, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. 8.

- 14.109 While teachers have to apply periodically for re-registration, unless they have been outside the profession for some time, there is no requirement for 'refresher' professional courses.⁹⁶
- 14.110 While Departmental schools are able to use ACMA's Help Button but, because they can decide how they use it, the rate of introduction has not been high.⁹⁷

Northern Territory

Education

- 14.111 The Northern Territory Government considered that governments had an important role in developing policies and programs to prevent and deal with all forms of bullying, including cyber-bullying. They also ensured that schools are appropriately supported and resourced to provide parents/carers and teachers with access to training about cyber-bullying and other online safety issues.
- 14.112 Schools in the Northern Territory therefore, have policies, aligned to the *Safe Schools Northern Territory Code of Behaviour*. Parents/carers and students are required to sign an 'Acceptable Use' agreement covering in general terms the inappropriate use of the online environment, including bullying and harassment.⁹⁸
- 14.113 Positive Behaviour Advisors in schools also taught Student Representative Councils and School Captains, of public, Catholic and independent schools, about dealing with cyber-bullying with the expectation that they will share this approach with their schools.
- 14.114 The Territory's Education Department is developing a professional Learning on Demand Module in cyber-safety for its educators to undertake in 2011. It includes information on cyber-bullying, online reputations and cyber-stalking.⁹⁹
- 14.115 While the sample size of cyber-bullying incidents in the Territory is insufficient to provide objective analysis, incidents have increased as young people gain greater online access.

96 Ms Liz Banks, Acting Deputy Secretary, Early Years and Schools, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS12.

97 Mr Trevor Hill, Director, Information Technology Services, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS13.

98 Northern Territory Government, *Submission 84*, p. 7.

99 Northern Territory Government, *Submission 84*, p. 7.

- 14.116 School based police officers in the Territory have a significant role in the investigation of cyber-bullying complaints, and the delivery of safety instruction to young adults. They have been delivering education awareness presentations since 2008.¹⁰⁰
- 14.117 These have been complemented by the immediate and thorough investigation of all complaints about cyber-bullying within the school environment, including requirements for parental/carer support and information on the consequences of misuse of carriage services. Education and encouragement is also provided to parents/carers and families to become more conversant with the online environment, and to monitor actively what young people are accessing on the Internet.

The Australian Capital Territory

- 14.118 The ACT Government acknowledged the need to take advantage of opportunities presented by developments in the online environment, while recognising the need to educate and protect young people against associated risks. This environment provided a means for citizens to have access to information that was consistent with the *Human Rights Act 2004* (ACT). It contained provisions about protecting families and children, freedom of expression and taking part in public life.¹⁰¹
- 14.119 The ACT is actively involved in combating cyber-crime and cyber-safety, both within the Territory and through cooperation with other jurisdictions. Agencies have introduced programs to educate young people on the safe use of the online environment, and to equip those in responsible positions with the skills to address issues that may arise.
- 14.120 The *Children and Young People Act 2008* (ACT) provides for the promotion, wellbeing, care and protection of young people in ways that recognises their right to grow in a safe and stable environment.¹⁰² Under the *National Framework for Protecting Australia's Children*, initiatives are under way, including:
- The *ACT Young People's Plan 2009-2014* took account of issues of importance to young people, including measures to be taken to address cyber-bullying, and
 - The ACT Children and Young People's Commissioner is obtaining the views of children and young people on issues including the use

100 Northern Territory Government, *Submission 84*, p. 6.

101 ACT Government, *Submission 82*, p. 1.

102 ACT Government, *Submission 82*, p. 2.

of online media tools. The Commissioner will then advise the Government on how to improve services for this group.¹⁰³

- 14.121 Commenting on programs in the ACT, the Australian Education Union noted that:

there is a Safe Schools Taskforce which is a cross-sectoral group with representation from each school sector, the Youth Advisory Council, parent groups, principals, education unions and ACT Policing. The taskforce examines policies and procedures and makes recommendations to maintain and improve the safety of children and young people in ACT schools. These recommendations have resulted in new or updated policies (including Providing Safe Schools P-12, Countering Bullying, Harassment and Violence in ACT Public Schools, the Keeping Children Safe in Cyberspace guide and the Code of Conduct for public schools, outlining what is expected of all people when on ACT public school grounds), plus associated pamphlets and posters for schools and families. The taskforce is currently planning a forum for students on cyber-safety in 2011.¹⁰⁴

Education

- 14.122 The Government believed that the ACT is at the forefront of information and communications technology. It has used the *myclasses* Virtual Learning Entertainment Environment since 2003. At the beginning of a school year, or on enrolment, all students must sign an 'Acceptable Use' form before they can go online. They are monitored while online, and inappropriate websites are blocked on the school system.¹⁰⁵
- 14.123 In 2009, a blogging feature for teachers was introduced into the *myclasses* environment. When it was apparent that some students were using it inappropriately, and without teachers' knowledge, it was removed.
- 14.124 A new Virtual Learning Entertainment Environment, Connected Learning Communities, has been deployed to all ACT public schools to replace *myclasses*. It enables schools to access digital content to enrich programs via the Internet. During its selection and development, consideration was given to the level of risk and cyber-safety concerns that it could bring.¹⁰⁶

103 ACT Government, *Submission 82*, p. 2.

104 Australian Education Union, *Submission 11*, p. 10.

105 ACT Government, *Submission 82*, pp. 3-4.

106 ACT Government, *Submission 82*, p. 4.

14.125 The Connected Learning Communities provides teachers with the opportunity actively to develop essential skills and capabilities in students to participate safely in the online environment. Its features include:

- An ACT Safe-Report Abuse button located at the top of every page. This would automatically open a new mail message in which students can type in the issue. The recipient of these messages would be a selected staff member;
- The individual user name and password given to each student, which must be authenticated before access is given to the network, and prevents students from making anonymous contributions within this environment;
- Students and teachers will be able to use a range of social networking tools that were once unavailable in classrooms because of privacy issues, and the risks of students engaging online with unknown people. Schools will be able to select the people with whom their students connect: their year, the whole school or across schools; and
- If students are using the networks inappropriately, monitoring and tracking systems will allow schools to lock accounts within seconds and examine the students' digital footprint.¹⁰⁷

14.126 The ACT works with other organisations, including the AFP, ACMA and the *Budd:e* Program, to educate teachers, parents/carers and students about Cyber-safety. This included the distribution of posters brochures and teaching materials to schools. Many schools had hosted information nights about safety online and cyber-bullying, and those which had taken part had indicated that these were well-received and 'extremely beneficial'.¹⁰⁸

14.127 While reports of specific incidents are low in the ACT, where cyber use escalated into bullying behaviour in a school, it is important that schools respond appropriately. These incidents are dealt with under a range of policy documents developed in accordance with the National Safe Schools Framework. ACT policies will be updated to reflect changes that are required in the recent review of the Framework.¹⁰⁹

14.128 A Safe Schools Taskforce has been created to ensure that the ACT remains a national leader in tackling bullying at school, and that all ACT schools

107 ACT Government, *Submission 82*, p. 5.

108 ACT Government, *Submission 82*, pp. 5-6.

109 ACT Government, *Submission 82*, p. 6.

deal with it in the same manner. Including systemic Catholic and independent schools ensures that the best ideas from the three sectors are shared and used for the benefit of all students.

- 14.129 In 2010, a sub-group of this Taskforce was formed specifically to consider cyber-safety and cyber-bullying issues.¹¹⁰ A forum, involving Year 9 students from all ACT schools, teachers, parents/carers and organisations such as the AFP, was held in Canberra on 18 March 2011.

Non-government and industry responses

- 14.130 Australian organisations and service providers have taken a range of measures to encourage cyber-safety, and to combat cyber-bullying in particular. The following individuals and organisations that participated in the Inquiry have devised a range of programs dedicated to dealing with the abuse, and to improve cyber-safety for young people generally.

Australian organisations

- 14.131 The Safer Internet Group includes organisations such as the Australian Council of State School Organisations, the Australian Library and Information Association, Google, iiNet, the Inspire Foundation, the Internet Industry Association, the Internet Society of Australia, Internode, the System Administrators Guild of Australia and Yahoo!.¹¹¹ The Group aims to develop 'the Internet as a platform for education, communication and economic activity and acknowledges that for the vast majority of users, the internet is a safe place' and:

advocates for effective action to be taken to ensure that Internet users, and particularly children, have a safe experience online, while preserving the benefits of open Internet access for all Australians. The SIG believe that the most effective way to protect Australia's children on the Internet is achieved by a combination of safety enhancing measures which include a primary focus on effective education and comprehensive policing of the Internet.¹¹²

- 14.132 The Stride Foundation is a not-for-profit organisation dedicated to helping improve the physical, mental and social well-being of young people and

110 ACT Government, *Submission 82*, p. 7.

111 Safer Internet Group, *Submission 12*, p. 1.

112 Inspire Foundation, *Submission 3*, p. 11.

their communities. Its purpose is to empower young people to realise their full potential, and to have the opportunity for brighter futures. It started as a peer-support foundation, and now takes on the cultural change of schools. It is not the same as other organisations with similar aims because it works with young people before any issues encountered, such as bullying, conflict, stress, depression suicide or low self-esteem, begin to have negative effects on lives.¹¹³

14.133 The keys to Stride's *CyberS@vvy* program are:

- Understanding the lack of empathy involved;
- Looking at how digital footprints work, and how students and perpetrators can be traced;
- Legal penalties; and
- How to refer serious issues to a trusted adult.¹¹⁴

14.134 Berry Street is the largest independent, not-for-profit child and family welfare organisation in Victoria, providing an extensive range of services for young people and families across the State.¹¹⁵

14.135 It approached cyber-safety through vulnerable young people living out-of-home and engaged in alternative education. One of its aims is to increase online access for those young people. As has been pointed out, those in out-of-home care can have less access to technology than their peers. This organisation sees technology as a valuable tool for connecting socially isolated young people with their community, and with their families.¹¹⁶

14.136 With funding from Telstra Corporation, the Victorian Office of the Child Safety Commissioner and the State's Department of Human Services, Berry Street developed *BeNetWise* in 2009. Its key aims related to raising awareness about technology, the value of technology for this group and the importance of online safety for such vulnerable young people.¹¹⁷

113 Stride Foundation: *Submission 6*, p. 1; Ms Kelly Vennus, Programs and Training Manager, *Transcript of Evidence*, 9 December 2010, p. CS2.

114 Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS3.

115 Berry Street, *Submission 95*, p. 2.

116 Ms Sherree Limbrick, Director, Statewide Programs, Berry Street, *Transcript of Evidence*, 9 December 2010, pp. CS3-4.

117 Berry Street: *Submission 95*, p. 5; Ms Sherree Limbrick, Director, Statewide Programs, *Transcript of Evidence*, 9 December 2010, p. CS3.

- 14.137 The Alannah and Madeline Foundation included cyber-bullying within its *eSmart Schools Framework* which provided a ‘consistent and practical’ whole-school approach for the implementation of evidence-based cyber-safety programs and practices. Because it needed to be addressed head-on, *eSmart* was not another program for cyber-safety, but a system for driving its implementation in schools. It was a road map or model for cultural and behaviour change targeting the whole school community, not a one-off lesson, unit of work, program or policy isolated from the day-to-day business of schools.¹¹⁸
- 14.138 The National Association for the Prevention of Child Abuse and Neglect has a range of programs and campaigns that educate children and young people in their online environments. They can be used, or adapted for use, in other jurisdictions, and include:
- *SOSO*, a digital collaboration with the digital marketing group Zuni; and
 - *Cyber Bullying Affects Real Lives*, of which *Web Warriors* is a key element that asks young people to take a stand against cyber-bullying.¹¹⁹
- 14.139 The Inspire Foundation was established in 1996 as a direct response to Australia’s then escalating rates of youth suicide, seeking to have a ‘global impact’ on the mental health and well-being of young people. It serves those aged between 14 and 25 through three national programs.
- 14.140 They are at the centre of all the Foundation does: as partners in the development and delivery of all its initiatives. It uses technology innovatively to reach young people and to build trusted social brands that are a part of their landscape. Its work is evidence-based and underpinned by research and evaluation conducted in partnership with academic institutions and research centres.¹²⁰
- 14.141 To deal with threats to cyber-safety, and cyber-bullying in particular, it recommended a multi-faceted, cross sectoral and educative approach. This view was based on evidence and experience that restrictive approaches to technology are ineffective.¹²¹

118 Alannah and Madeline Foundation: *Submission 22*, p. 35; Dr Judith Slocombe, Chief Executive Officer, *Transcript of Evidence*, 11 June 2010, p. CS7.

119 National Association for the Prevention of Child Abuse and Neglect, *Submission 97*, p. 3.

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

121 Inspire Foundation, *Submission 3*, p. 6.

14.142 The Alannah and Madeline Foundation believes that *eSmart* is not just another cyber-safety program, but a system for driving its implementation in schools as part of a planned and systematic approach. It provides a consistent and practical whole-school approach for the implementation of evidence-informed cyber-safety programs and practices. It is a culture and behaviour change model targeted at the whole school community and, as such, is not a one-off lesson, unit of work, program or policy that sits in isolation from the day-to-day business of schools.¹²²

14.143 More specifically, *eSmart* aims to:

- Integrate cyber-safety with schools' current knowledge and practices about well-being, including policies such as the NSSF;
- Assist schools to develop more effective curriculum around cyber-safety and wellbeing and the smart use of technologies;
- Help give teachers skills in smart, safe and responsible use of technologies;
- Assist school communities in developing safe and supportive schools where bullying and violence are minimised and the values of responsibility, resourcefulness, relationships and respect are fostered in cyber-space; and
- Assist schools in becoming cyber-safe.

14.144 *eSmart* supports exploration of:

- Protective behaviours;
- Supportive and relationship building behaviours, and
- Reporting incidents.

14.145 It embraces:

- Whole-of-school well-being issues including values/relationships/self-esteem;
- E-security;
- Ethics including downloading and plagiarism, and
- Criminal activity, including sexual harassment and predation.

122 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. CS7.

14.146 *eSmart* is underpinned by the positive embrace of information and communications technology and the promotion of smart use of technology. It is designed to:

- Help schools develop policies and practices (developed with input from students and parents) encouraging students to use technology responsibly and respectfully;
- Point schools to high quality teaching resources on cyber-safety and those which help create a safe, respectful and caring environment;
- Encourage schools to embrace the positives of Internet and communications technology within their teaching practice to enhance learning;
- Establish a system for schools to provide evidence that they are actively implementing these policies and practices, and
- Help reduce the digital divide between adults and young people, so adults can become a credible source of advice on avoiding the risks of cyber-space.

14.147 The major mechanism for delivery of *eSmart* into schools is an interactive website. Schools are further supported by other resources such as a welcome kit, newsletters and a Help Desk, as well as training in using the system.¹²³

14.148 Roar Educate applauded the *eSmart* initiative, as a key to both awareness and cultural change within schools. It did not believe however that, in isolation, it can bring about the holistic approach needed by schools to manage cyber-safe risk management. *eSmart* needs to be complemented by other systems.¹²⁴

Aboriginal initiatives

14.149 Dr Julian Dooley, commented that

In 2006 we began a project to reduce cyberbullying behaviour experienced by Aboriginal children in the mid-west of Murchison region of Western Australia. Aboriginal community members, including elders, children, young people, parents, carers and Aboriginal school staff, talked with us about what they called 'bullying', why they think it happens and how it feels to be

123 Alannah and Madeline Foundation, *Submission 22*, pp. 35-36.

124 Mr Craig Dow Sainter, Managing Director, Roar Educate, *Transcript of Evidence*, 20 April 2011, p. CS17.

Aboriginal and be bullied. This project led to the development of a number of important outcomes, including a website www.solidkids.net.au which provides evidence based and culturally appropriate information on strategies for young Aboriginal people, schools and families.¹²⁵

14.150 Although these are very important resources, much more work is needed to protect Aboriginal youth.¹²⁶

Australian ICT industry bodies

14.151 Since 2002, Australian Internet service providers compliant with Internet Industry Association Codes have been eligible to apply for 'IIA Family Friendly ISP' status. These Codes exist as part of Australia's co-regulatory regime, and they are legally enforceable by ACMA. Such Internet service providers are authorised to display a logo which signifies adherence to best practice standards. The Association noted that ISPs representing about 85 percent of the market are family friendly.

14.152 Under the registered Code, Internet service providers providing access to users within Australia are required to:

- Take reasonable steps to ensure that Internet access accounts are not provided to persons under the age of 18 years without the consent of a parent, teacher or other responsible adult. A number of suggested options for achieving this are included in the Code;
- Take reasonable steps to encourage commercial content providers to use appropriate labelling systems, and to inform them of their legal responsibilities in regard to the content they publish. The Internet Industry Association has compiled a resource for this purpose, and Internet service providers are advised to direct users to the Association's URL;
- Provide an optional filter or filtered service to users on a cost recovery basis, and
- Take reasonable steps to provide users with information about:
 - ⇒ supervising and controlling children's access to Internet content;
 - ⇒ procedures which parents can implement to control children's access to Internet content;
 - ⇒ their right to make complaints to ACMA about online content; and

125 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS5.

126 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS5.

⇒ procedures by which such complaints can be made.¹²⁷

14.153 The Association referred to the ‘very specific parameters’ around the sites that are subject to ACMA’s take-down provisions. These fall into the ‘prohibited content’ classification under the Codes underpinned by legislation. Such sites are required to be removed by 6pm on the business day following the day on which they are notified. When sites are subject to take-down, they are subject to limits of Australian jurisdiction. The ‘vast majority’ of such sites are not hosted here.¹²⁸

14.154 Google Australia works closely with a network of experts who advise it on promotion of child safety and how to combat abuse in its products. It drew attention to the range of measures that it takes to do these things, including the advice that it provides to its users.¹²⁹

14.155 Microsoft Australia believed that the following responses would assist parents/carers to deal with cyber-bullying:

- Communicate by discussing the issue with children, and encourage them to report it to a trusted adult;
- Block communications through filters, and children not to respond to the abuse;
- Investigate so that they know what children are talking about, and what they do online;
- Use Family Safety Software which can supply an activity report on computer usage. This in turn can be a starting point for a discussion about online activities; and
- Report by knowing who to contact if a young people is being cyber-bullied, such as her/his school, the site service provider, and the police.¹³⁰

14.156 Microsoft Australia also commented on its recently established Digital Crimes Unit, which includes:

A worldwide team of lawyers, investigators, technical analysts and other specialists whose mission is to make the Internet safer

127 Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association, *Transcript of Evidence*, 11 June 2010, p. CS10; Internet Industry Association, *Submission 88*, p. 13.

128 Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association, *Transcript of Evidence*, 11 June 2010, pp. CS16-17.

129 Google Australia & New Zealand, *Submission 13*, p. 2,

130 Microsoft Australia, *Submission 87*, p. 3.

through strong enforcement, global partnerships, public policy and technology solutions.¹³¹

14.157 Yahoo!7 referred to the 'distinct lack' of evidence into how Australian young people engage with the online environment, and how their parents/carers see the risks of using the Internet.

14.158 It also believed that further research into the prevalence and scale of online safety risks would inform and shape the debate about which safety measures would be most effective in managing those risks.¹³²

14.159 Yahoo!7 provides training to the law enforcement community and has created the Australian Law Enforcement Process Guide.

14.160 It has also:

- a dedicated online safety education site called Yahoo!7 Safely with information for parents of younger children and teenagers about how to be safe online;
- been an active member of the Consultative Working Group on Cybersafety and the Safer Internet Group;
- been an active supporter of Safer Internet Day for two consecutive years;
- been working closely with the Australian Competition and Consumer Commission on their Scamwatch and consumer fraud efforts; and
- through the Internet Industry Association, developed a family friendly filtering accreditation which can be used by Internet service providers and filtering software vendors, and is developing a voluntary code whereby providers would actively filter websites containing child abuse images out of their services.¹³³

14.161 It gave examples of its initiatives, in education, policing, safer social networking, research and technology, to improve safety online. It noted that Yahoo! has enabled a SafeSearch feature within Yahoo!7 to prevent the display of adult content in queries. Parents/carers can lock this function on, and young people registered as under 17 years old cannot turn it off.¹³⁴

131 Microsoft Australia, *Submission 87*, p. 2.

132 Yahoo!7, *Submission 2*, pp. 2-4.

133 Yahoo!7 *Submission 2.2*, pp. 1-2.

134 Yahoo!7, *Submission 2*, pp. 3-4.

- 14.162 Yahoo!7 works closely with Australian law enforcement agencies to provide assistance when its services are abused. This included establishment of a 24 hour/seven days per week compliance function which can respond immediately if Yahoo!7 is contacted about a situation indicating that a young person may be in danger.¹³⁵
- 14.163 Telstra Corporation is an industry partner with the Australian Government to link young people, parents and teachers with expert cyber-safety advice and targeted information via ACMA's Cybersmart website. It has agreed to cross-promote the Authority's website as part of its focus on helping to protect Australians from cyber-bullying and invasions of privacy.¹³⁶
- 14.164 Other activities by Telstra include:
- participation on the Consultative Working Group on Cybersafety ;
 - providing tools, tips and educational information to customers;
 - supporting Safer Internet Day, the Australasian Consumer Fraud Taskforce's Fraud Week, Privacy Week and National Cyber- Security Awareness Week;
 - its Computer Emergency Response Team;
 - being an original partner of the Virtual Global Taskforce;
 - being a dedicated Trading Post Trust and Safety team; and
 - tasking a company Chief Privacy Officer and Privacy Managers to ensure that business units adhere to its privacy policies and procedures.¹³⁷
- 14.165 Singtel Optus noted that the Australian Mobile Telecommunication Association has developed a range of fact sheets and other material for parents and young people on topics such as bullying and mobile phones. There is also a website that provides information on bullying and online safety generally.¹³⁸
- 14.166 Netbox Blue is a privately owned Internet management company, providing schools, businesses and government organisations with tools to

135 Yahoo!7, *Submission 2*, p. 3.

136 Telstra Corporation, *Submission 14*, p. 7.

137 Telstra, *Submission 14*, p. 5.

138 Singtel Optus, *Submission 42*, p. 2.

protect their networks from internal/external threats, control data threats and ensure staff/students use the Internet safely and productively.¹³⁹

- 14.167 It has devoted more than three years to develop 'patent-pending and unique' technology to address issues in the Inquiry's Terms of Reference, including cyber-bullying. It believed that this software would prevent inappropriate communications on social networking sites such as Facebook and Twitter. It could be used at schools, on laptops provided for use outside those networks and soon, at homes. It noted that this technology was already being used at schools across Australia.¹⁴⁰
- 14.168 Device Connections is the exclusive distributor of My Mobile Watchdog, 'a sophisticated safety technology' that allows parents to see:
- the full content of text messages received and sent;
 - photos received and sent;
 - the full contents of emails received and sent, and
 - a log of the mobile phone calls received and made, their time and duration.
- 14.169 This technology is aimed at children aged from six to 14, and was established to help parents educate and manage their children's safety. It was driven by concerns about cyber-bullying and sexting. Parents can set up an alert notification function within the system so that, when a suspicious or unauthorised person tries to call, text or email a young person, the communication is routed through the My Mobile Watchdog data centre. Notifications or alerts by SMS message or email are sent 'instantly' to all the people nominated in the parents' web account.¹⁴¹
- 14.170 My Mobile Watchdog can be used on all phones operating on Windows Mobile 5 and 6, it was recently launched for all android operating systems and the capability is being developed for more handsets. Device Connections sees this system as 'only one piece' in a very complex puzzle of managing cyber-safety education and training for parents/carers, the community and young people themselves. This service costs about \$150 per year, providing licences for up to five children.¹⁴²

139 Netbox Blue, *Submission 17*, p. 1.

140 Netbox Blue, *Submission 17*, pp. 2-3.

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

142 Mr Geoffrey Sondergeld, Director, Device Connections, *Transcript of Evidence*, 17 March 2011, pp. CS49-51.

- 14.171 It included in its submission a report from the United States about the effectiveness of My Mobile Watchdog in helping 'parents monitor and keep their children safer' while using their mobile phones.¹⁴³
- 14.172 The Communication Alliance Industry Code deals with the *Handling of Life Threatening and Unwelcome Communications*, and is an example of co-regulation.¹⁴⁴

Marketing

- 14.173 The Australian Direct Marketing Association is the peak industry body for the Australian direct marketing industry and operates a Direct Marketing Code of Practice which includes specific provisions to address marketing to minors.¹⁴⁵ The Code specifies that members limit the sale of restricted goods and services to minors and indicate when parental consent is required. The Australian Direct Marketing Association has a number of platforms designed to provide guidance to its members about appropriate conduct when interacting with young people.¹⁴⁶

143 Device Connections, *Submission 51*, p. 22.

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

145 Australian Direct Marketing Association, *Submission 36*, pp. 3-4.

146 Australian Direct Marketing Association, *Submission 36*, p. 4.

International Responses to Cyber-Threats

- 15.1 This chapter presents some of the international initiatives of which the Committee is aware. They are examples of the continuing efforts by governments, corporations and organisations around the world to safeguard children and young people more effectively.

United Kingdom

- 15.2 Governments and civil society in the United Kingdom have developed numerous initiatives to address cyber-threats and online bullying.

Task Force on Child Protection on the Internet

- 15.3 The Task Force on Child Protection on the Internet was established in March 2001 in response to a number of serious cases where British children had been 'groomed' via the internet. Childnet International commented on the Task Force, as:

a unique collaboration bringing together, in a positive partnership, representatives from the internet industry, children's charities, the main opposition parties, government departments, the police and others who shared the aim of making the United Kingdom the best and safest place in the world for children to use the internet.¹

- 15.4 In 2008, the Task Force released its *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services*. This document produced practical recommendations for the providers of social

¹ Childnet International, *Submission 18*, p. 4.

networking sites so they can enhance the safety of those using their services. The *Good Practice Guidance* also sought to provide:

- industry and others with safety advice;
- tips for children and young people; and
- guidance for parents/carers to ensure the safety of their young people.

15.5 Childnet International also referred to commitments by the then British Prime Minister, Gordon Brown, in December 2009 to review periodically the success of each set of the guidance, arguing that:

These necessary reviews will ensure that parents and young people are confident that the guidance is being applied and understand how. This level of accountability is vital in understanding how the best practice guides are being conformed to and what more needs to be done.²

15.6 The Australian Communications and Media Authority (ACMA) contributed to the Foreword and highly commended the *Good Practice Guidance* document.

15.7 Similar documents have also been promoted by industry groups, such as the British 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.³

Child Exploitation and Online Protection Centre and *ThinkUKnow*

15.8 The Child Exploitation and Online Protection (CEOP) Centre is the United Kingdom's national law enforcement agency, focussing on criminal activities where children are sexually abused. CEOP also operates the *ThinkUKnow* website in Britain. It is designed for parents and contains a number of resources such as tests, information, webcasts and videos. It also explains the meaning of commonly-used terms in relation to the Internet and provides a series of measures that can protect children online.

15.9 CEOP and the Australian Federal Police (AFP) are partners in the Virtual Global Taskforce (VGT) and it is through this relationship *ThinkUKnow* was brought to Australia.

2 Childnet International, *Submission 18*, p. 5.

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

United Kingdom Council for Child Internet Safety

- 15.10 Formed in 2008 by then Prime Minister, the United Kingdom Council for Child Internet Safety brings together over 140 organisations and individuals to help 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.
- 15.11 The Council is formed of four working groups: an Education Group, an Industry Group, a Public Awareness Group and a Video Games group, as well as an Experts Research Panel.
- 15.12 In 2009, the Council launched the public awareness campaign 'Click Clever Click Safe' initiative to promote Internet safety amongst children and parents. In March 2010, a review of the strategy concluded that since the establishment of the Council, the concept of online safety has become embedded within the public consciousness. Childnet International commented that:

the importance of education is emphasised again as well as continuing programs to raise awareness of the issues surrounding Internet use. The positive review of [the Council] serves to emphasize the importance of effective Government involvement in the debate.⁴

Education programs

- 15.13 Research by the Office for Standards in Education, Children's Services and Skills reveals that the most effective schools in keeping students safe online and helping them to take responsibility for their own safety have a multi-layered managed approach, involving students, parents and teachers, where there are fewer inaccessible sites.
- 15.14 The Alannah and Madeline Foundation commented:

If we look towards the United Kingdom, which has perhaps the most robust cybersafety and cyberbullying education campaign, we can see the British Home Office have achieved good results in tackling the issue. They have raised awareness of the issue through multifaceted media campaigns that harness the power of industry. They have also mandated school policies and procedures through the Federal Department of Education, embedded targeted resources in the school curriculum, and run professional

4 Family Online Safety Institute, *Submission 38*, pp. 10-11.

development through local education networks. The UK is also currently looking to reform legislation in relation to cyberbullying.⁵

Childnet International

- 15.15 Childnet International is a British-based charity working domestically and internationally to help make the Internet a great and safe place for young people, alongside enabling them to use interactive technologies safely and responsibly.
- 15.16 Childnet focuses on education, awareness and policy. It has worked to develop the *Know IT All* range of resources, providing advice on cyberbullying. These resources were designed to help young people and parents manage the risks that they may encounter online. Childnet's initiatives are discussed more thoroughly in Part 2 of this report.

United States

Online Safety and Technology Working Group

- 15.17 The American government initiated the Online Safety and Technology Working Group (OSTWG) under the auspices of the National Telecommunications and Information Administration (NTIA). This Group was established in 2008 and comprises representatives from the Internet industry, child safety advocacy organizations, educational and civil liberties communities, the government, and law enforcement communities. It presented its report, *Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group*, to the NTIA in June 2010. This report recommended various strategies to promote online safety for children through education, labelling and parental control of technology. Broadly, the report recognised that there is no single solution to keeping children safe online and that all stakeholders (parents, industry, schools and governments) must work to improve the safety of children on the Internet.
- 15.18 Notably, the OSTWG report recommends the creation of a web-based 'clearing house' to make online safety research available to the public and

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

emphasised the vital role of education in reducing young people's exposure to risks online.

15.19 The Working Group Subcommittee on Parental Controls and Child Protection Technology

surveyed the available products; trends in consumer demand and product use; and strategies for improving the utility of current and future technologies.

- The marketplace for parental control products is quite deep and constantly evolving. It functions effectively for users who understand basic computer security, but the diversity of options can exacerbate user confusion.
- Awareness-building efforts and greater transparency about product features are required. A common set of terms, agreed upon by the industry, should be developed to this end. Community reporting and policing on sites that host user-generated content should also be promoted.⁶

15.20 There is a wealth of learning and best practice to draw on from countries around the world where industry, government, children's charities and the law enforcement community have worked together to develop a comprehensive suite of safety measures.⁷

NetCetera: Chatting with Kids About Being Online

15.21 In December 2009, the American Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and the Department of Education released a booklet assisting parents and teachers: *NetCetera: Chatting with Kids About Being Online*. The Family Online Safety Institute commended this initiative:

This booklet was a great step to education parents and teachers about online safety and is a good example of what the Australian government could be doing to empower parents in this changing media landscape.⁸

15.22 *NetCetera* identifies online risks, including those associated with texting and mobile phones, and gives parents the tools to begin discussions with their children about the risks these technologies can bring.

6 The United States Online Safety and Technology Working Group, *Youth Safety on a Living Internet*, 4 June 2010.

7 Yahoo!7, *Submission 2*, p. 2.

8 Family Online Safety Institute, *Submission 38*, pp. 9-10.

Children's Agenda for Digital Opportunity

- 15.23 In March 2010, the American FCC also released the *Children's Agenda for Digital Opportunity*, an initiative focussing on 'four pillars': digital access for all children, digital literacy, digital citizenship and digital safety. A core focus of this initiative is the empowerment of parents and teachers, as well as greater utilisation of technological solutions to the problems children face online.

OnGuard Online

- 15.24 Operated by the FTC, *OnGuard Online* is a web-based Internet resource providing a collaboration of resources from various agencies in American Federal Government as well as leading operators in the technology industry. The site assists users to guard against internet fraud, secure their computers and protect personal information.
- 15.25 *OnGuard Online* also provides tips for parents on how a balance might be found between granting privacy to their children and monitoring their activities online to ensure safety.

Centre for Safe and Responsible Internet Use

- 15.26 The Centre for Safe and Responsible Internet Use, a non-government organisation, provides research and outreach services to address issues regarding the safe and responsible use of the Internet.
- 15.27 Resources provided by the Centre include:
- Online resources for parents including guides to creating cyber-savvy teens, articles and hardcopy books;
 - Links to useful websites;
 - Guides for parents and educators to avoid cyber-threats and cyber-bullying; and
 - Reports, articles on various topics such as philosophy and approach of cyber-safety, the filtering software issue.

Wired Safety resources

- 15.28 *Wired Safety* asserts it is the world's largest Internet safety, help and education resource. It collates a wide range of resources and information for parents, children and teachers on cybercrime, cyber-law and cyber-safety, including:

- *Wired Kids Inc*: a charity dedicated to protecting all Internet users, especially children, from cybercrime and abuse;
- *Wiredkids.org*: a website to help children help each other through virtual volunteering;
- *Cyber Law Enforcement Organization Network* of law enforcement officers specialising in cybercrime investigation, training other law enforcement officers and assisting cybercrime victims online;
- *Stop Cyber Bullying*: Explains how to prevent cyber bullying according to the age of the child;
- *Net bullies*: Provides advice for parents, children and teachers on cyber bullying; and
- *Teenangels*: Groups of 13 to 18 year old volunteers trained in all aspects of online safety, privacy and security. They run unique programs in schools to teach responsible and safe internet surfing to other teens and younger children, parents, and teachers.

National Center for Missing and Exploited Children

15.29 The National Center for Missing and Exploited Children is a private, non-profit organisation which aims to prevent the abduction, endangerment and sexual exploitation of children. Its resources include:

- *CyberTipline*: used to report internet-related child sexual exploitation;
- *Netsmartz* website: offers online resources, workshops and offline learning activities available to parents to facilitate discussion with their children and teens about internet safety; and
- *NSTeens*: a series of online clips advocating online ethics and proper attitudes to have when gaming, chatting, etc.

Cyber-safety.com

15.30 The *cyber-safety.com* website aims to assist parents and educators about keeping children safe online. The developers of the site also play an advocacy role, seeking to raise awareness of online threats in the community.

Cybercitizen Awareness Program

15.31 The Cybercitizen Awareness Program seeks to educate young people on the danger and consequences of cyber-crime. The program is designed broadly to establish a general sense of responsibility and community in an effort to develop smart, ethical and socially conscious online behaviour in young people.

Cybersmart!

- 15.32 The *Cybersmart!* website draws together a range of initiatives, including:
- *CyberSmart! Online Workshops* facilitate professional development of teachers and parents and offers participants a hands-on experience to develop their online skills;
 - *CyberSmart! Student Curriculum* is a web-based learning tool for young people to learn how to use the Internet safely; and
 - *CyberSmart! Educator Toolbar* offers users 24 hour/seven day access to annotated essential resources to support student learning.

Canada

Definetheline.ca

- 15.33 *Definetheline.ca* is an initiative of Professor Shaheen Shariff and McGill University seeking to provide a portal for greater engagement between policy-makers, teachers, parents, and youth in user-friendly ways. The project hopes that engagement of this kind will allow all stakeholders to learn from each other and share resources.
- 15.34 Generally, *definetheline.ca* seeks to define digital citizenship and socially responsible online communications as well as distinguishing digital citizenships from cyber-bullying.

Internet 101

- 15.35 Internet 101 is a collaborative project between the police forces in the National Capital region of Canada. The project works with local police officers to host school-education campaigns and seminars. It also provides online Internet safety resources.

New Zealand

Netsafe

- 15.36 Netsafe is a non-profit organisation comprising of the Ministry of Education, the New Zealand police, the Police Youth Education Service, educators from primary to university levels, the Department of Internal Affairs, New Zealand Customs Service, community organisations, businesses, parents and students, as well as members of the industry including InternetNZ, Microsoft, IBM and Vodaphone.
- 15.37 Netsafe produces a variety of resources including:
- Netbasics: a collection of animated movies for children available online;
 - *Netsafe Helpline* to assist all members of the public with cyber-safety issues;
 - *Hector's world* website: a website targeted for children and includes discussion points, questions and answers for parents to use with their children;
 - Online resources specifically for adults and parents: detailed tips on how to use a public computer, how to behave when posting information on the Internet and tips for buying or playing online;
 - Lectures, seminars and workshops on cyber-safety topics are held at schools, parents' groups and community organisations;
 - Fighting text bullying: Netsafe has partnered with Vodafone NZ, Telecom NZ and New Zealand Police to combat text bullying; and
 - Online resources explain how to make a complaint to a mobile phone company.

Leading international collaborations

- 15.38 The Australian New Zealand Policing Advisory Agency (ANZPAA) commented that 'the borderless environment the internet creates extends beyond the response capacity of a single jurisdiction. Establishing and maintaining stakeholder networks are therefore paramount'.⁹ ANZPAA

9 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 4.

also commented on the urgent need for international law to ‘effectively facilitate global co-operation for the investigation of cyber crime offences’.¹⁰

- 15.39 Various international arrangements exist that are leading to such frameworks. Some of these are included below.

Virtual Global Taskforce

- 15.40 The Virtual Global Taskforce (VGT) was launched in 2003 as an international alliance of law enforcement agencies, bringing together partners from Australia, America, Britain, Italy, Canada, Interpol, United Arab Emirates and New Zealand. In December 2009, the AFP officially assumed the position of Chair of the VGT.

- 15.41 The AFP commented that

this is a significant appointment for the AFP which will serve to further strengthen Australia’s law enforcement efforts in globally combating child exploitation online.¹¹

- 15.42 The VGT is made up of police forces from around the world working together to fight online child abuse. Its aim is to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse. The objectives of the VGT are to make the internet a safer place, to identify, locate and help children at risk, and to hold perpetrators appropriately to account.¹²

Council of Europe Convention on Cyber-Crime

- 15.43 The *Council of Europe Convention on Cyber-Crime* is the first international treaty on crimes committed via computer networks. Its primary objective is to pursue a common criminal policy aimed at the protection of society against cyber crime, by adopting appropriate legislation and fostering international co-operation.¹³

- 15.44 The Convention requires its signatories to criminalise certain conduct and appropriate powers to be available to law enforcement agencies. It also makes available a range of procedures to facilitate information sharing and greater multilateral access to information.

10 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 4.

11 Australian Federal Police, *Submission 64*, p. 17.

12 Australian Federal Police, *Submission 64*, p. 17.

13 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 4.

15.45 The Cybercrime Convention is not limited to European nations and the Attorney-General's Department proposed that Australia accede to the Convention. ANZPAA advised that:

acceding to the Convention would ensure Australia's laws and arrangements are consistent with international best practice and improve Australia's ability to engage internationally in the fight against cyber-crime. It would also complement the broader policy agenda in the development of a national approach to combat cyber-crime.¹⁴

15.46 In April 2011, the Joint Standing Committee on Treaties recommended that Australia accede to this Convention. It did, however, express some concerns regarding the privacy, human rights protections and the judicial review provisions in the Convention.¹⁵

United Nations Crime Prevention and Criminal Justice Commission

15.47 In April 2011, the Twentieth Session of the United Nations Crime Prevention and Criminal Justice Commission was held in Vienna. The prominent theme for this session was 'Protecting children in a digital age: the misuse of technology in the abuse and exploitation of children.'

15.48 The Commission focussed on two primary sub-themes:

- the nature and scope of the problem of misuse of new technologies in the abuse and exploitation of children; and
- responses to the problem of misuse of new technologies in the abuse and exploitation of children.¹⁶

15.49 A report from the Commission is yet to be released.

The Australian/European Research Training School

15.50 The Australian/European Research Training School on cyberbullying is evidence of the:

quest for world's best practice in developing the next cohort of internationally collaborative researchers. All current promotion,

14 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 4.

15 Joint Standing Committee on Treaties, *Report 116: Treaties tabled on 24 and 25 November 2010, 9 February and 1 March 2011, Treaties referred on 16 November 2010 (Part 3)*, April 2011, p. 92.

16 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 5.

prevention and intervention work on cyberbullying is benchmarked to international findings.¹⁷

- 15.51 *An Australian Training School: From Research to policy and practice - Innovation and sustainability in cyberbullying prevention* was successfully held in Melbourne, Australia, from 11 to 16 April 2010. It was the first venture to be held jointly between European Collaboration in Science and Technology, and the Australian Department of Innovation, Industry, and Science Research. It brought together 30 European and 18 Australian early career researchers and PhD candidates working in cyberbullying research and related fields.¹⁸

Australia New Zealand Policing Advisory Agency

- 15.52 The Australia New Zealand Policing Advisory Agency (ANZPAA) is a joint initiative of the Australian and New Zealand Police Ministers and Commissioners and provides strategic policy advice on cross-jurisdictional policing initiatives that enhance community safety and security. The cross jurisdictional nature of cyber-crime requires a coordinated response by all agencies. ANZPAA facilitates collaboration within policing and the development of effective relationships with other stakeholders.¹⁹
- 15.53 ANZPAA runs various forums such as the ANZPAA Child Protection Committee and the nationally-focussed e-Crime Committee.²⁰

ANZPAA Child Protection Committee

- 15.54 The ANZPAA Child Protection Committee (ACPC) is comprised of the Heads of Child Protection from all policing agencies in Australia and New Zealand. A primary focus of the ACPC is the protection of children from extreme cyber-threats. The online environment has seen the proliferation of child exploitation material, while the popularity and accessibility of social networking sites has become a rich environment for sexual predators to locate and groom children.²¹
- 15.55 The ACPC develops partnerships with key stakeholders, including telecommunication companies, internet service providers and pioneers in

17 The Australian University Cyberbullying Research Alliance, *Submission 62*, p. 46.

18 The Australian University Cyberbullying Research Alliance, *Submission 62*, p. 31.

19 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 1.

20 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 2.

21 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 3.

the technological field. The ACPC is engaged in the following initiatives designed to mitigate cyber-safety threats:

- The use of hash set values as a means of identifying previously seized child exploitation material and to block the further transmission of these images through technological solutions such as the Global File Registry;
- The standardisation of child exploitation material categorisations and the sharing of hash sets internationally;
- Implementation of the Child Exploitation Tracking System and the Australian National Victim Image Library across all jurisdictions;
- The establishment of information sharing practices and national training packages across the jurisdictions;
- The development of national guidelines for evidence presentation of child exploitation material;
- The development of a framework for content service provider liaison in emergent situations that is agreed and understood by all Australian law enforcement agencies; and
- The development of cooperative relationships with relevant stakeholders including internet service providers.²²

15.56 In addition to these initiatives, ANZPAA seeks to contribute a ‘holistic response to cyber-safety through various cross-jurisdictional and multi-agency forums’.²³

Australia’s contributions

15.57 Although the fast-paced and evolving nature of the Internet will mean that the three sectors (government, industry and not-for-profits) will have to continue working to develop safeguards for newly emerging risks, the Committee is heartened by the numerous ways in which Australians are working collectively to ensure the safety of our young people. Further, Australia is working collaboratively within, and in many cases leading, multi-national bodies to address these pressing issues.

22 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 3.

23 Australia New Zealand Policing Advisory Agency, *Submission 151*, p. 4.

15.58 However, the NSW Secondary Principals' Council called for greater collaboration to resolve issues of jurisdiction:

Government needs to develop international-Australian agreements so that international & Australian sites that cause issues for young people can be forced to remove inappropriate material that constitutes cyber-bullying, illegal content, content which encourages inappropriate social or health behaviours or content that can lead to identity theft.²⁴

New technologies

- 16.1 It is important that Australia maximises opportunities presented by new and emerging technologies allowing for the evolution of digital economy and interactive educational opportunities. These technologies are usually accompanied by protective mechanisms to deal with risks online. Although this Report has examined behavioural aspects of promoting cyber-safety and reducing cyber-bullying, new technologies can form part of a multi-faceted solution.
- 16.2 Inspire Foundation emphasised the opportunities provided by technological advances to impact positively on the lives of young people:
- in order to utilise and not diminish this potential, the approach to addressing issues of cyber safety must be cross-sectoral, multi-faceted and dynamic, reflecting the complexity of the online environment itself.¹
- 16.3 BoysTown points out that this provides the opportunity for Australia to enhance online services, and suggested that:
- the Australian Government increase its funding for research into the use of new communication technologies and online help-seeking amongst young people to provide an evidence base for the engagement of youth in relation to health and other issues of concern.²

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

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

Safeguards

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

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

Recommendation 24

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

- 16.5 The Department of Broadband, Communications and the Digital Economy has introduced a number of initiatives such as the *Stay Smart Online* E-security education package, E-security Awareness Week and ScamWatch. Another example is *SpamMATTERS*, created by the Australian Communications and Media Authority (ACMA), enhancing the positive effect of the *Spam Act 2003* (Cth).⁴
- 16.6 The American Online Safety and Technology Working Group was established in 2008 and comprises representatives from the Internet industry, child safety advocacy organizations, educational and civil liberties communities, the government, and law enforcement communities. Technology is now available to address issues such as password security:

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

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

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

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

Some solutions

- 16.7 Participants in the Inquiry suggested many different solutions to cyber-safety abuses, demonstrating that many technologies are available but also that they are accompanied in most cases by in-depth cyber-safety policies.
- 16.8 As examples, four of these proposals, drawn from participants in Queensland, are outlined below.

Family Friendly Filter

- 16.9 From its experience in dealing with schools across Australia, Netbox Blue saw five cyber-safety threats:
- Access to inappropriate web content;
 - Access to online forums with a risk of predators;
 - Communication of bullying messages by email, social networking sites, or text;
 - The risk of 'cyber addiction' to online gambling, or social networking sites, and
 - The impacts of the proliferation of social media applications and other Internet-related activities on learning.
- 16.10 It believes that, for students' safety on the Internet, four pillars need to exist before there is any chance of combating these online threats.
- Up-to-date policies for all Internet, social networking sites, and mobile devices inside and outside schools need to be created and implemented. These must include clear consequences for inappropriate actions, must be kept up to date and communicated regularly to all stakeholders;
 - Stakeholders need education about dangers, and on ways of minimising or dealing with them;

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

- Technological enforcement is necessary, both inside and outside schools, on all school-owned equipment to help prevent or block any inappropriate use, and alert appropriate school authorities; and
 - Regular reviews of attempted policy breaches are necessary to improve education and manage individual behaviour, with clear consequences for offenders.⁶
- 16.11 For a school of 750 students and 100 staff, and depending on the features adopted, the cost of the Family Friendly Filter would be 6.4 cents per day per user.⁷

Throttling bandwidth

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

Central monitoring of access

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

Australian Protected Network

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

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

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

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

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

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

- 16.15 It has developed the Australian Protected Network (APN) that would put control in the hands of parents/carers, allowing them to set limits on sites accessed by their children. It is a framework which enables users to control and shape their 'online view', by putting in a basic level of protection. Users then modify the approach according to their needs.¹¹
- 16.16 If implemented, the APN would produce a point of contact for each Internet user in Australia, and information can easily be forwarded to them.¹²
- 16.17 Among its features, APN:
- Allows/disallows access to different classes of product or web site. One selection could be the blocking of all direct external ISP access and disallowing web access to chat web sites. Another selection might simply block criminal/fraud activity and online gambling;
 - Aggregates data from other services that provide information on compromised equipment and prevents access to that equipment; and
 - Seeks out compromised equipment and as far as possible attempts to inform owners of their problems, as well as providing links to possible solution providers, i.e. anti-virus solutions or patches for their operating system.
- 16.18 The safety and security of user information is maintained at all times. Users have full access to all data they supply into the system and are able to maintain or remove their information at any time. Under no circumstances is identifiable information collected or used without the full acknowledgement of the user. This means that proxy server access logs are not used as part of normal system operations at any time.¹³
- 16.19 There has been a lot of comment that there is no point in implementing safety measure because young people can get around them. Netbox Blue reaffirmed, however, that:

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

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

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

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

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

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

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

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

Industry advances

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

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

16.24 In 2010, Telstra, Optus and Primus, agreed to introduce voluntary filtering of child abuse URLs¹⁷ and this covers 70 percent of internet users in Australia. Work is also underway to obtain similar agreements with other

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

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

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

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

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

- 16.25 The Internet Industry Association referred to the Family Friendly ISP scheme which accredits ISPs that comply with best practice and under the present industry codes they are required to make filters available.¹⁹
- 16.26 Additionally, there are many free filtering options, and between 40 and 50 percent of parents/carers already use some type of filtering.²⁰ There are also relatively inexpensive filters available commercially.²¹

Mobile phones

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

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

- 16.28 Device Connections reported that:
- 99 percent of girls and 80 percent of boys aged 15-17 years own mobile phones;
 - 81 percent of girls and 70 percent of boys aged 12-14 years own mobiles; and

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

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

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

21 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS12.

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

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

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

16.29 Further, Device Connections stated that:

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

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

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

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

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

16.33 It added that:

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

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

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

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

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

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

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

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

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

- 16.35 Mr James Collins added that:

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

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

- 16.37 The NSW Secondary Principals' Council suggest that:

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

- 16.38 Introducing such changes would require the cooperation of suppliers.

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

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

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

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

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

Recommendation 25

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

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

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

- 16.40 BoysTown emphasised the importance of mobile phones:

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

Recommendation 26

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

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

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

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

Young people and technology

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

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

- 16.42 Netbox Blue advised that technological solutions encompassing everything for a school of 750 students and 100 teachers would cost 6.4 cents per day per user.³⁹ For a parent license to monitor five mobile phones, the cost would be \$14.95 per month.⁴⁰ Implementation of the Australian Protective Network costs 0.4 cents per day.⁴¹ The cost of these protections is not prohibitive.
- 16.43 Further, most companies producing technological solutions already have educational resources about cyber-safety for young people and parents/carers.

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

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

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

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

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

Proposal for a mandatory filtering system

- 17.1 A significant amount of attention in this Inquiry focused on a proposed national, mandatory filtering scheme so that internet service providers (ISPs), can remove access to Refused Classification material online. Other ways of restricting access will also be outlined. Refused Classification material includes child sex abuse, bestiality, extreme violence including rape, detailed instructions on crime or drug use, and advocating a terrorist act. The Government has stated that Refused Classification C content has no place in our society and therefore should not be available in the internet.
- 17.2 Significantly, three of Australia's largest ISP's, Telstra, Optus and Primus, have agreed to voluntarily block child abuse material at the server level. Webshield, and ItXtreme have also volunteered to block this content.

Background

- 17.3 The role of the Australian Communications Media Authority (ACMA) in regulating online content is to administer the co-regulatory scheme established under the *Broadcasting Act 1992* (the Act). Complaints about online content can be made to ACMA and, if the material is found to be prohibited or potentially prohibited, it must either:
- issue an interim or final take-down notice (for content hosted in Australia); or
 - refer the content to industry accredited Family Friendly Filters (for content hosted overseas) under a recognised alternative access-prevention arrangement outlined within a registered Code of Practice.

- 17.4 The online content co-regulatory scheme is under-pinned by the National Classification Scheme (NCS), applicable to films, computer games and certain publications. Determinations about prohibited/potentially prohibited material are made by reference to classification categories established under the NCS.
- 17.5 ACMA must refer Australian-hosted content that is potentially prohibited to the Classification Board for classification before it can take action. Content hosted overseas may be referred to the Board.
- 17.6 Prohibited or potentially prohibited content is assessed against the following classification categories:
- Refused Classification, including offensive depictions of children and material advocating terrorists acts;
 - X18+;
 - R18+ items not subject to restricted access systems; and
 - Certain limited MA15+ content classified MA15+, provided for profit or on payment of a fee and not consisting of one or more images and/or text.
- 17.7 There are no technical issues preventing the adoption of filtering a list of URLs, and many ISPs around the world have been doing so voluntarily 'for many years'.¹
- 17.8 Late in 2010, Telstra Corporation, Optus and Primus agreed to introduce voluntary filtering of child abuse URLs on ACMA's list of prohibited sites. These ISPs cover about 70 percent of all Internet users in Australia. About 30 percent of ACMA's black-listed sites included depictions of child abuse and child sexual abuse material.² Recently, Webshield, and ItXtreme have also volunteered to block child abuse material at the ISP level. The Government will continue to encourage other Australian ISPs to follow the example of these ISPs.
- 17.9 ACMA is working to develop measures to enable these prohibited sites to be transmitted to participating ISPs on an automated and secure basis. It

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

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

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

- 17.10 The Department of Broadband, Communications and the Digital Economy was hopeful of getting the cooperation of other ISPs to filter voluntarily material on ACMA's blacklist, by working with the Internet Industry Association. That body has announced that it will assist in encouraging a wider range of ISPs to adopt voluntary filtering.⁴ Until recently, ISPs have refused to take action on blocking Refused Classification material.
- 17.11 There is no evidence of reluctance by ISPs to take down Refused Classification material, and it is not clear that legislation would be any more effective than a voluntary arrangement. The user policies of large multi-national websites are 'very broad' and cover a 'much wider range' of material they can take down, compared to what is described as 'inappropriate' in the Act.⁵
- 17.12 Under its powers in the Act, ACMA also issues industry codes to ISPs, and these co-regulatory instruments are enforceable immediately they are registered. Compliance is 'close to universal' and probably as high as would be achieved by legislation.⁶
- 17.13 Mr Mark Newton made the point that about two-thirds of Australian households do not have school age children and applying restrictions to these households would be poor targeting.⁷
- 17.14 Further, according to ACMA surveys, between 40 and 50 percent of parents use filtering devices at home. Considerable evidence was presented to this Inquiry on the range of such devices.⁸ These devices more material than Refused Classification content.

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

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

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

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

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

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

- 17.15 There are many commercial and free filtering options available, at many levels:
- search engines, such as Bing, Yahoo! and Google;
 - browser level, including Microsoft; and
 - software applications, such as a product of a US company Blue Coat.⁹
- 17.16 However, there is a lack of awareness by parents.
- 17.17 While most participants concentrated on expressing views of the filtering of Refused Classification material, Symantec Corporation noted that less than 50 percent of small to medium businesses in Australia had security systems installed and operating. Only when they became victims of fraud or identity theft did such businesses seek out educational resources or assistance from government agencies, or the police.¹⁰

Support for the proposal

- 17.18 BraveHearts saw ISP filtering as part of a 'holistic' approach to online threats. It argued that material such as child pornography, already blacklisted by ACMA, breached Australian laws and it was illegal to produce, own and distribute it. It should not be available online. This organisation supported a second tier of filtering that would allow families, organisations or businesses to request optional filtering of other objectionable material, such as promotions of terrorism, suicide, drug use or adult pornography. It was aware that no filtering systems were foolproof, and that they can be circumvented.¹¹
- 17.19 The Victorian and Tasmanian Synod of the Uniting Church gave four reasons for requiring ISPs to block Refused Classification material:
- Sale and distribution of this category is already banned in all other media, including the Internet hosted in Australia;

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

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

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

- They have a ‘crucial role’ in preventing the domestic consumer from accessing it by accident, and in preventing those who do not know how to access it but are curious, as well as those who are at an early stage of developing or feeding a sexual interest in children;
 - It undermines the commercial trade in images of child abuse and actively disrupts its success; and
 - It is reasonable to expect ISPs to accept some responsibility for what their clients seek to view, and for the material to which they provide access.
- 17.20 The Synod did not see placing such obligations on ISPs as a replacement for education and awareness programs and law enforcement, but as a complementary measure to a wider cyber-safety strategy. Requiring ISPs to be socially responsible and not facilitate trans-national criminal activity would assist in providing increased cyber-safety to young people who would otherwise become victims of the demand for commercial child sexual abuse materials.¹²
- 17.21 Family Voice Australia supported the proposal for mandatory ISP-level filtering, noting that opponents’ arguments could be addressed because:
- There would be minimal degradation to Internet performance;
 - The right to free access to information has always been qualified by the need to protect the community, and there was no logical reason why the Internet should be different;
 - The implementation of any filtering scheme would be protected by scrutiny in the Parliament and in the media; and
 - Even if a total blockage of all Refused Classification material cannot be achieved, a significant reduction was a worthwhile goal.¹³
- 17.22 It believed that including some of the following features when the proposed scheme was implemented could improve cyber-safety:
- Providing an R18+classification for computer games;
 - Excluding X18+ material; and

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

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

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

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

Concerns about the proposal

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 17.30 The Victorian Office of the Child Safety Commissioner stated that it was important to strike the right balance between filtering harmful material, particularly for younger children, while still enabling older children access to information about issues relevant to them.²²
- 17.31 The Australian Library and Information Association opposed filtering on the basis of freedom of access of information and would like to find a balance between censoring adults and protecting children.²³

Other views

- 17.32 The Queensland Catholic Education Commission has online filtering, and there is monthly feedback to schools about sites that are accessed in each case. It believed, however, that the major focus should be on the development of positive e-security habits for all users, rather than on technological solutions such as filtering. These simply present a challenge to those who are 'computer savvy, and are rapidly superseded as technology advances. The Commission saw filtering as part of a package, and emphasises giving skills to students to have the right attitudes. It saw putting key values in place, and giving some specific skills and attitudes, as the most effective way of dealing with Cyber-safety.²⁴
- 17.33 Referring to 'problematic Internet use', Netbox Blue noted that if a filter was installed, many people would consider that their technological problem(s) had been solved.²⁵
- 17.34 The Safer Internet Group reiterated that the proposed filter would give parents/carers a false sense of security about online safety, and that it has changed the way the world viewed Australia.²⁶
- 17.35 Facebook has two concerns about the proposal:

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

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

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

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

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

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

- It will distract people from other things that need to be done to make the Internet safe; and
 - Filtering attracts social costs, as there may be a 'chilling effect' on expression. It also has economic costs, as some investment in innovative ways to use new information in Australia will go elsewhere if there is a government screen.²⁷
- 17.36 Professor Karen Vered did not think that the government needed to dictate 'a kind of blanket filtering', and believed that parents/carers should make their own decisions about purchases, installation and learning how to use it. Filtering would be costly and put Australia at an even greater disadvantage internationally. It would also make Australian ISPs responsible for problems they had not caused, as they are not responsible for 'unsavoury material' from foreign sites. If Australian ISPs were to be made responsible for filtering, their costs would be passed onto consumers.²⁸
- 17.37 Moreover, technological barriers are not a solution, as they are not going to help young people develop their ability to discriminate, evaluate and act under circumstances where they are required to exercise their own judgement.²⁹
- 17.38 While supportive of the Government's initiative in proposing to filter child pornography and extremely violent content, Symantec Corporation noted that filtering did not solve issues such as fraud, identity theft, or cyber-bullying.³⁰
- 17.39 The Alannah and Madeline Foundation confirmed that home filtering was not often applied, despite the widespread availability of systems. When it was applied, there was a risk that parents/carers were given a false sense of security about access to inappropriate content, or the risk of their children being contacted by strangers online. Parents/carers were then encouraged to think that their children could be left to go online

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

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

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

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

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

Feedback from young Australians

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

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

PART 6

Concluding Comments

Everywhere I go children and young people tell me they want to contribute. It is also my experience that children and young people often have a good understanding of what is best for their wellbeing, have unique insights into issues and can offer creative solutions to the problems under discussion.¹

It's not about being prescriptive as is implied by 'talk about it more' or 'learn about it'. It's about experience, adaptability, and interest. If people aren't interested in their safety, they won't be safe. If people don't know how to adapt to the internet, they won't be safe. If people don't have brushes with unsafe use that really affect them, they'll continue to act brazen and be unsafe.²

Input from young people

- 18.1 As demonstrated throughout this Report, the Committee values the input of young people into the development of new methods to promote cyber-safety and reduce cyber-bullying. Young Australians have a wealth of experience with new technologies and are more equipped to respond appropriately to online risks than is often assumed.³ Indeed, young people genuinely hold the key to their own security online; adults can learn as much from young people as they can learn from adults.
- 18.2 As Dr Helen McGrath from the Australian Psychological Society commented:

1 Commissioner for Children and Young People WA, *Submission 54*, p. 4.

2 Survey respondent, Male aged 17.

3 Third A et al, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 2.

Young people need to part of that process, because if we do not listen to what they have to say about what works and does not work, we are going to go down some dead ends.⁴

18.3 Furthermore, the Australian Youth Affairs Coalition suggested that:

That children and young people be directly engaged to share their experiences and help develop relevant solutions to cyber safety.⁵

18.4 The Alannah and Madeline Foundation commented that:

Young people are essential to the solution and must be involved in policy development, parent education and development of multi-media education materials.⁶

18.5 The Youth Affairs Council of South Australia believed that the inherent risks are largely within the competencies of young people to manage:

By framing young people's internet use in the language of "threats," it is easy to overlook the opportunities available to young people online, and also the fact that young people are usually able to understand and manage any risks they may take online.⁷

18.6 A recent report by the Cooperative Research Centre for Young People. Technology and Wellbeing argued that, by positioning cyber-safety:

within an online risk-management paradigm (particularly within policy) is inherently limiting given the substantial range and substantive benefits associated with online practise.

18.7 That report also found that the benefits of social networking are largely associated with the:

participatory nature of the contemporary digital environment, yet participation in creative content production, dissemination and consumption is largely overlooked in cybercitizenship frameworks. [This] should be informed by young people's own experiences and perspectives.⁸

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

5 Australian Youth Affairs Coalition, *Submission 28*, p. 3.

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

7 Youth Affairs Council of South Australia, *Supplementary Submission 25.1*, p. 3.

8 Collin, P et al, 2011, *The Benefits of Social Networking Services*, Cooperative Research Centre for Young People, Technology and Wellbeing, pp. 21-22.

- 18.8 Indeed, the apparent experience of young people participating in the Committee's *Are you safe?* survey was that current programs do not value their existing knowledge and consequently are delivered at a very basic level. This is demonstrated by the following comments, submitted in response to questions on what can be done to improve safety online:

Young people dont care about giving information out because they don't know what will happen. More talks need to be given at school by people that have gone through identity theft or something else on the internet, not just people that make up silly stories and tell us that our bluetooth names are wrong (Female aged 15).

[I am safe] because i belive that i do know what i am doing. i have the knowledge, on how to handle viruses and worms. i think it would be useful to teach people on how to handle these (Male aged 15).

- 18.9 Dr Barbara Spears commented:

young people want education from research, they want to know what is legal and what is not and they want to be involved in the educative process as well.⁹

- 18.10 The capacities, resilience and ability of young people to absorb information was also discussed by the National Children's and Youth Law Centre:

Children's positive engagement with the Lawmail service shows a yearning for information and support. In particular, there has been a growing interest in cyber-safety marked by a 50 per cent increase in Internet related questions in the past year since 2004.

Interestingly, these young people have had the initiative and forethought to ask the question. This is the kind of behaviour that in our view should be encouraged in young people:

thoughtfulness, critical thinking and openness to learning. This displays maturity, respect for the law and wisdom in their interactions with the world. This resourcefulness should be matched and supported by adults in providing appropriate services.¹⁰

9 Dr Barbara Spears, Senior Lecturer, School of Education, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS28.

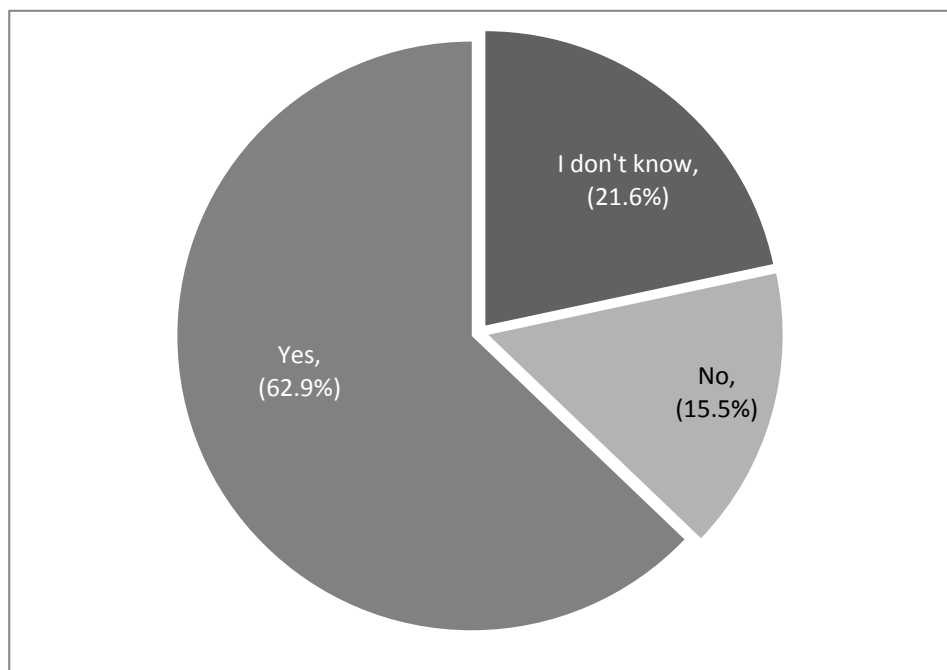
10 National Children's and Youth Law Centre, *Submission 138*, p. 5.

- 18.11 This sentiment was also reflected in comments submitted by survey respondents. An example was submitted in the final free-text space:

I think it should be monitored more and individuals should take more of a responsibility. Some teenagers don't realise what they put on may be detrimental to their future goals. In saying that, preaching to us about it makes the people who listened the first time more aware and those who don't listen care less (Female aged 15).

- 18.12 The clear message from both young people and other participants in the Inquiry is that programs should seek to value existing knowledge and build upon this with appropriate and resourceful strategies. Some of those strategies are discussed below, and in Chapter 19.
- 18.13 The Committee's *Are you safe?* survey also asked respondents aged 13 years and over whether they believe more can be done to make the Internet safer. 62.9 percent of respondents believe that more can be done.

Figure 18.1 Can more be done to make the internet safer? (*Aged 13 and over*)



- 18.14 The survey asked respondents what they believe can be done to make the internet safer. Respondents were able to select more than one of the following options, and Figures 18.1a and 18.1b indicate percentages of the collective total of responses to the question.

Figure 18.2 What can be done to make the online environment safer?

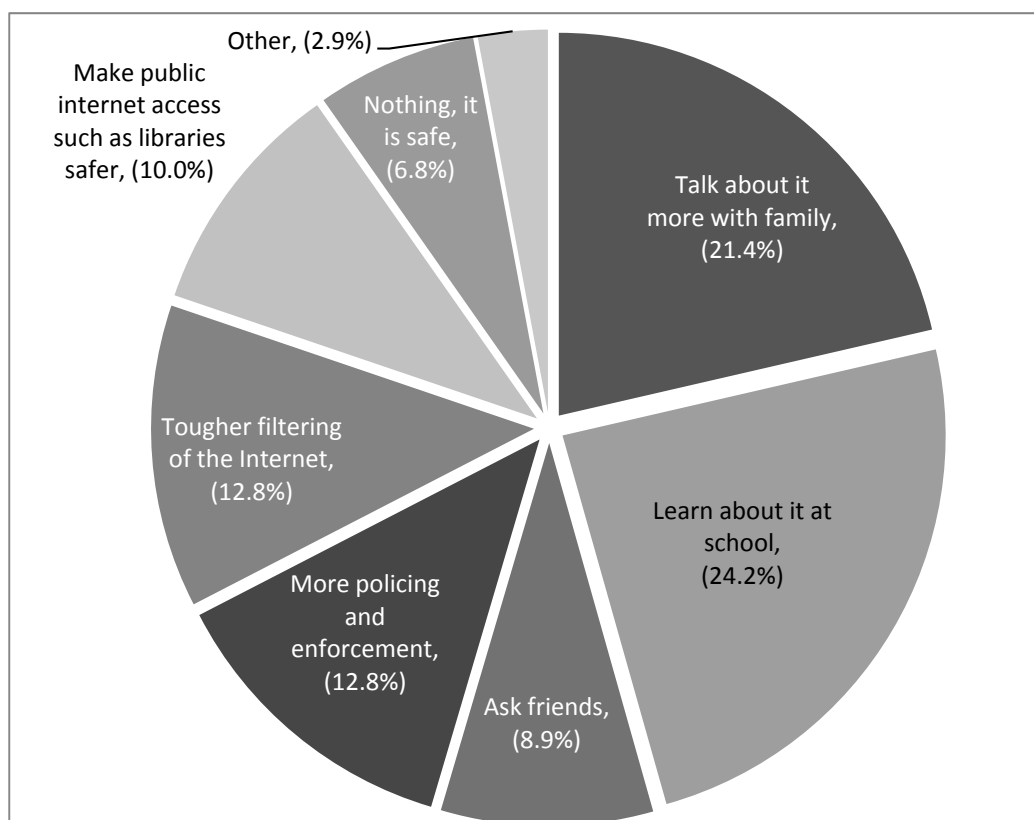


Table 18.1 What can be done to make the online environment safer?

	Sex	Talk about it more with family		Learn about it at school		Ask friends		More policing and enforcement		Tougher filtering of the internet		Make public internet access such as libraries safer		Nothing, it is safe now		other	
		%	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#
5 Years	M	45.3	34	46.7	35	28.0	21	20.0	15	22.7	17	21.3	16	25.3	19	21.3	16
	F	40.2	33	37.8	31	29.3	24	25.6	21	31.7	26	22.0	18	23.2	19	18.3	15
6 Years	M	54.2	26	60.4	29	31.3	15	33.3	16	12.5	6	25.0	12	6.3	3	8.3	4

	F	65.6	42	57.8	37	31.3	20	28.1	18	23.4	15	20.3	13	14.1	9	4.7	3
7 Years	M	69.1	76	64.5	71	31.8	35	35.5	39	16.3	18	20.9	23	10.9	12	4.5	5
	F	80.4	78	67.0	65	28.9	28	24.7	24	14.4	14	12.4	12	4.1	4	2.1	2
8 Years	M	64.2	272	56.8	241	25.2	107	31.1	132	19.6	83	20.5	87	6.6	28	3.8	16
	F	73.0	360	63.7	314	26.2	129	23.7	117	13.2	65	13.8	68	3.4	17	2.6	13
9 Years	M	70.4	707	60.4	606	24.1	242	26.6	267	19.6	197	19.3	194	6.1	61	4.9	49
	F	74.0	798	66.7	719	22.6	244	27.2	293	16.9	182	18.8	203	2.9	31	4.8	52
10 Years	M	66.7	1134	61.6	1048	22.4	381	25.9	440	23.6	402	21.3	362	5.8	99	2.9	49
	F	74.6	1342	70.8	1273	24.5	441	24.9	447	20.3	365	19.4	349	2.8	50	6.3	113
11 Years	M	65.8	1517	63.9	1473	23.0	530	26.9	620	30.9	713	25.1	579	5.7	132	4.4	102
	F	69.7	1745	69.6	1741	24.9	623	28.4	710	28.0	701	26.0	650	3.0	74	7.6	191
12 Years	M	59.0	1320	63.2	1414	24.9	557	28.8	644	35.0	783	25.3	567	9.2	205	6.0	134
	F	63.9	1446	70.7	1599	28.2	639	30.2	684	33.4	756	27.4	621	4.9	112	7.2	164
13 Years	M	40.2	760	49.0	926	20.3	384	25.6	672	35.8	676	28.6	540	3.4	64	10.2	192
	F	39.9	980	51.8	1272	20.3	498	24.3	842	38.8	953	28.3	696	2.3	56	9.8	241
14 Years	M	35.3	569	46.4	748	18.3	295	30.9	498	31.0	500	25.9	418	4.8	78	9.1	146
	F	33.7	667	48.1	954	17.7	350	35.2	698	37.4	741	25.0	495	2.2	44	7.8	155
15 Years	M	27.9	332	41.1	489	17.6	210	29.1	346	27.4	326	23.8	283	4.8	57	7.4	88
	F	31.9	438	49.5	680	18.4	253	37.1	509	39.5	543	26.9	369	2.8	38	6.2	85
16 Years	M	28.4	229	42.1	340	17.1	138	30.5	246	26.3	212	21.7	175	5.5	44	8.8	71
	F	27.2	271	48.1	480	14.9	149	37.3	372	36.7	366	24.2	242	1.7	17	6.1	61
17 Years	M	22.8	90	33.9	134	14.2	56	28.6	113	20.0	79	17.5	69	7.8	31	9.6	38
	F	26.8	152	50.9	289	14.3	81	41.2	234	40.8	232	28.2	160	2.5	14	6.2	35
18 Years	M	26.6	83	33.3	104	17.9	56	30.8	96	18.9	59	19.6	61	9.3	29	12.2	38
	F	30.5	79	37.8	98	18.5	48	36.7	95	32.4	84	24.3	63	9.7	25	11.2	29

Getting the message right

18.15 Although young people and the broader community are aware of risks online, it appears that the positive message of staying safe online and limiting exposure to risks is not being fully understood or communicated effectively.

18.16 Dr Julian Dooley highlighted the importance of getting the message right:

One thing that is very clear, not from cybersafety research but from social marketing research, is that, if the message is really obvious and transparent, young people are much less likely to pick it up. It is really important that we develop strategies that are attractive, that convey and develop positive messages and that promote positive behaviours. One of the strongest predictors of bullying behaviours is a smaller social response repertoire. So we need to encourage social behaviours but do it in a fun way in which the message is not so blatantly obvious that it turns people off.¹¹

18.17 Dr Roger Clarke commented:

Although the Slip, Slop, Slap example that keeps cropping up is a bit of giveaway, a bit of a stab in the dark, there is a benefit if you think through what objectives we are trying to reach. That kind of campaign did demonstrably reach parents and it also reached a proportion of those that are normally fairly hard to reach. That message got through. It got through to a lesser extent, I think, to young people, so if we are trying to target young people we have to find other channels. Advertisements are not the key thing for kids. They absorb their information in other ways. But mass media campaigns for parents, done the right way – it has to be really catchy; it has to be one of those ads that really clicks for the age groups we are trying to reach, which are current parents, not us grandparents – do have some merit in trying to reach a reachable part of those missing parents. As I say, the majority of kids are going to learn the majority of what they want from their peers and from their environment... is that with young people viral marketing is going to be the most important mechanism that you are going to need to use. I do not believe advertisements in the sense of billboards and billboards converted into other media are having a big impact on young people these days. I do not speak as

11 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS38.

an advertising executive or an advertising researcher, but that is my impression. Viral marketing is perceived to be within their community – that is the reason it works.¹²

18.18 Mr Darren Kane of Telstra Corporation warned, however, that:

one of the young children during one of the workshops, when they were speaking about Facebook, indicated, 'Facebook isn't that bad.' That is where we go back to that message that I spoke of earlier. We have got to be very, very careful around our educational programs to make sure that that is not the perspective young people have of Facebook. We have got to be careful about how we educate them to the risks of using Facebook without actually pushing them away from using a product that allows them to keep connected.¹³

18.19 Young people also commented on the need for an age-appropriate and positive message. When asked what can make the online environment safer, the following comments were submitted:

Everyone knows [about what they should and should not post online], they just dont think that these things will happen to them. so you dont need to tell us how to be safe, tell us more about what will happen if we aren't (Male aged 15).

i think people of higher, let me say, authority, need to come to schools and tell children, particularly teenagers about being safe on the internet. they cant just say 'please be safe whilst online' because that doesnt get through to us. they need to enforce laws and rules upon us. they need to get to the kids, not the parents or teachers. they dont run our lives and we are smart enough to know how to go behind their backs. we, as teens, must know the dangers and consequences and it must be told to us as a serious matter, not some light thing we can have a laugh about later (Female aged 15).

I think that more public awareness is needed to make Online Safety an issue of importance for the youth of Australia. Essentially, the only way this message will really be heard is if the Australian youth have a greater exposure to it, outside the typical environment of school. For example, seminars could be held for the broader community as a way of educating parents AND students about online safety. In this way, the

12 Dr Roger Clarke, *Transcript of Evidence*, 21 March 2011, pp. CS26-27.

13 Mr Darren Kane, Director, Corporate Security and Investigations, and Officer of Internet Safety, Telstra Corporation, *Transcript of Evidence*, 8 July 2010, p. CS25.

message would be reinforced in a positive way which would most probably be reflected in the statistics of online safety awareness (Female aged 17).

I think you just need to keep talking to everyone about it. There is no other way to enforce it, but to just keep talking about it (Female aged 13).

Just keep increasing awareness, sooner or later people will listen (Male aged 16).

Just to keep talking about it at school and making sure younger kids understand, and make sure everything is as private as it could be so strangers can't look you up (Female aged 14).

talking about it all the time just makes me annoyed the more paranoia of your parents and teachers that gets shoved down your throat the less you actually care, yeah theres bad people out there but everyone knows that it should e taught once or twice but after that it should only be reminded when someone is actually doing something stupid, bad people are everywhere not just on the net (Female aged 17).

18.20 They also commented on how these messages might be delivered:

pop ups on the web, featuring information on safety, but being etiquette and not coming up to often so it doesnt annoy anyone (Male aged 14).

Reminders when you ARE online. Everyone knows this information, but if someone was faced with a choice (eg, between giving information out and not) it is most usually the 'giving' side of the argument that wins because there is someone to persuade you. The 'safety' side needs to be persuasive too (Female aged 15).

Appropriate educational materials

18.21 Mr Nick Abrahams and Ms Ju Young Lee submitted that,

There is not enough educational material being produced or distributed that truly has an impact on teens. Much of the educational material being produced is in hardcopy, or is difficult for teens to relate to as it is usually presented from an older perspective. Educational materials that are relevant and produced from their peers' perspective are essential. Additionally, these

materials should be distributed through the mediums that teens function in (email, social media) to be effective.¹⁴

18.22 Similarly, Facebook commented:

One of the big frustrations that I see is that the government is thinking, 'I want people to come to the government website to look at X,' but few kids are going to do that and few parents actually do that.¹⁵

18.23 Respondents in the Committee's *Are you safe?* survey commented extensively on the current approach of education programs, and how they might be adapted. Some of the comments made throughout the survey are extracted below:

Educate adults as well as children, teenagers (Male aged 15).

educating people of incidents that have occurred with other people, so they know what has and can happen to them. It can also be seen as a scare tactic as this can work well for teens (Female aged 15).

Education about the repercussions, if you wouldn't do it in real life... Hence why filtering isn't the answer... (Male aged 17).

Education is the key, if kids know the dangers they know what to do. Force facebook to make privacy settings easier to understand for kids. Make parent liable for what happens to their kids online (if parent monitors then child will be safe). Provide free good filtering software for parents who can't afford to buy it (Male aged 18).

Get everybody to learn about safety on the internet and help each other and always make sure the site is safe and that all your settings are privately set. Make sure younger kids especially learn because they can just easily click on anything without any cyber-bullying knowledge or safety (Female aged 13).

Have more police officers come into the schools and share with students what penalties there are against offenders and what you could do if you were in that situation (Female aged 14).

I cannot stress enough, how important it is for children to be aware of the damage they can do with a single click. Education of the dangers of the internet and how to safely and responsibly use the internet needs to

14 Mr Nick Abrahams and Ms Ju Young Lee, *Submission 66*, p. 2.

15 Hon Mozelle Thompson, Chief Privacy Advisor, Facebook, *Transcript of Evidence*, 11 June 2010, p. CS36.

be a priority in solving cyber bullying issues. Also I am aware that no specific laws or policies are able to be enforced upon the perpetrators, so there is no deterrent for would-be cyber bullies to bully other peers online (Female aged 17).

I think it is important just to educate people about internet safety, and not focus so much on filtering instead. I think that students should be educated more on specifically what they can do to be safer on the internet, because at the moment we aren't really taught a lot and I know that a lot of other people know nothing about internet safety (Female aged 14).

I for one need a better understanding of viruses and online safety with the computer. A public body of informatio would be helpful (Male aged 14).

Most sites are safe, it's the users that tend to be the issue, whether they don't know what to do and get into trouble or someone who does bad things anyway takes advantage of them. I reckon educating people on how destructive their actions can be, whether they realise it or not, is the solution as well as teaching them about the philosophy behind the morals of their actions (Male aged 17).

not necessarily at school, we get a lot of lectures already, but deffinately something else.. maybe a website? or some kind of interesting game? or up-beat documentary, nothing corney. or posters? but all of them designed and influenced by children our age. not some random people in an office. its important that we feel involved in our own production of saftey. otherwise we will just see it as another boring lecture (Female aged 16).

To make things safer online, people should actually be realistic in seminars given about online safety. Usually they are lame. People usually know not to do stupid things on the internet anyway (Female aged 14).

We learn a little about it at school but not much. Make it more understandable for kids. alot of people make there age older so they make acctons for facebook ect (Female aged 14).

Parents should be educated about this topic more. If they are more aware about this topic, majority of parents would be able to prevent it and intervene (Female aged 16).

People just have to use there brains more. I mean its common sense to know if its a good idea or not. If it doesn't feel right then don't do it

(Male aged 15).

Teach people about the dangers, and how to avoid them and avert them with proper security. This would make people aware of the dangers but not scare them out of using the internet (Male aged 14).

Teachers can talk to students in small groups or by themselves so that they get the message quicker (Female aged 13).

teaching critical thinking skills to school students to improve common sense and make them think! But this would involve overhauling education curriculum and is probably beyond the scope of the parliamentary inquiry (Male aged 18).

I think there needs to be something done in teaching children morals; what is right and what is wrong, no matter who's beliefs this may infringe on (Female aged 18).

Recommendation 27

That the Minister for Broadband, Communications and the Digital Economy invite the Consultative Working Group on Cybersafety, in conjunction with the Youth Advisory Group, continue to advise Government on enhancing the effectiveness of cyber-safety awareness campaigns including targeted media campaigns and educational programs.

Empower young people to better assist each other

18.24 It is important that positive initiatives empower young people to promote their own safety, and that of their peers. The Youth Affairs Council of Victoria noted:

We know through our work with young people that they get most of their information from each other and that they share a lot of information. Not all of that is reliable information, so we need to be really careful about monitoring what young people are telling each other and listening to the stories that they are telling each other about their online experiences.¹⁶

16 Ms Georgie Ferrari, Chief Executive Office, Youth Affairs Council of Victoria, *Transcript of Evidence*, 11 June 2010, p. CS27.

18.25 Facebook's Chief Privacy Advisor also commented:

When they sense something is not right they will warn all their friends but not necessarily tell their parents or their teachers, and that is an important challenge.¹⁷

18.26 Dr Julian Dooley noted that:

So having peer driven student leadership based programs where there is open, engaged discussion about what happens online and what does not happen online is a great way to encourage positive uses.¹⁸

18.27 The Alannah and Madeline Foundation observed that:

if we are to be successful in developing those resources, we need to engage young people as the experts, because they are the only ones that know what is cool, what is now and what appeals.¹⁹

18.28 Ms Sonya Ryan noted young people's capacity and interest in working collaboratively:

I think it is about getting through to children through mediums that they can relate to, to really get them enthusiastic about coming together and taking a stand against this kind of crime. I find that the kids at high schools tend to get quite agitated about what has happened to my daughter – the way in which she was lured by the promise of love – and they are very keen to let all their friends know, to pass the information on, to talk to others about it, to talk to siblings about it and to talk to parents about it. There needs to be more information, more education and more awareness in the curriculum and also through different means. As I have said, it needs to go through avenues in which the children are already engaged and so they are in a place where they feel comfortable. Then we tend to see them come forward with information because they are in an environment where they feel as though they can.²⁰

18.29 Similarly, Ms Candice Jansz commented:

17 Hon Mozelle Thompson, Chief Privacy Advisor, Facebook, *Transcript of Evidence*, 11 June 2010, p. CS32.

18 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS44.

19 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. CS38.

20 Ms Sonya Ryan, Director, Carly Ryan Foundation, *Transcript of Evidence*, 3 February 2011, p. CS59.

The design and implementation of peer-run educational programs should also be a central facet of any such measure, as youth place great importance on the views and actions of their peers. This diversification of advice and information will ensure that messages concerning the permanency of actions, the gravity of choices and the dangers of online disclosure are reiterated and more comprehensively understood by young people in the long term.²¹

- 18.30 Indeed, young people completing the *Are you safe?* survey commented on their peer-support networks when feeling unsafe on the Internet. When asked who they would talk to if they saw something concerning online, the following comments were made:

I would say talk to someone you trust and make sure they know whats going on.its very hard for people to talk to there familys and others (Male aged 15).

I would talk to my sister, because she understands me, but not like anyone else in my family (Female aged 14).

Maybe a family friend...i dont trust those around me enough to not go back and tell my father what i may have accidently come across while on the internet and i know my dad would jump to conclusions (Female aged 15).

Think about it in depth by yourself, perhaps communicate on the appropriate forums (Male aged 16).

Peer education

- 18.31 A strategy that is likely to be the most effective in combating the negative effects of online interaction for children and young people is peer-run education. This could be through groups such as Privacy Victoria's Youth Advisory Group, or mentor groups within school and community environments. Groups such as these, composed of enthusiastic and dedicated young people, are more likely to be able to reach and connect with a young audience than older presenters. This is in spite of a lack of formal training and experience.

- 18.32 Ms Jansz stated that young people,
-

21 Ms Candice Jansz, *Submission 44*, p. 3.

are at an age where they are mature enough to understand and communicate the risks and issues involved in online communication, yet young enough to remember their childhood and teen years clearly, making them able to easily relate to and empathise with their audience's issues, concerns and communicative needs... Dynamic and enjoyable presentations on cyber-safety by young people in schools and community venues for children, young people, parents and teachers alike are more likely to be remembered than academic or expert testimonies, which can inspire message fatigue as old materials and slogans are constantly rehashed and reused... The use of young people to educate young people also means that messages can be dispersed through alternate delivery methods, for example peer-created artwork, merchandise and posters, concerts, dynamic websites (including vox pops, videos and competitions etc.) and even delivery on the mediums deemed problematic in the first place, for example, Facebook advertising, groups or fan pages.²²

- 18.33 Similarly, the Commissioner for Children and Young People in Western Australia commented:

Directly involving children and young people in decisions that impact on them and taking their views into account in the development of laws, policies and programs results in better outcomes for children and young people. This is true for all areas that impact on children and young people but is especially the case when considering their engagement with technology and the online environment – no one knows more about the ways they are engaged, the issues they face and, therefore it follows, solutions that are most likely to work for them.²³

Crossing the inter-generational divide

- 18.34 Young people's perceptions of what their parents/carers and other adults know about new technologies greatly impacts on the level of acceptance and value they place on the information and advice given to them. However, many young people do not believe that their parents in particular are fully aware of what happens on the Internet and,

22 Ms Candice Jansz, *Submission 44*, p. 6.

23 Commissioner for Children and Young People WA, *Submission 54*, p. 4.

consequently, often overstate dangers or misrepresent risks. The following comments were made in response to two different questions in the survey:

parents definitely do need some insight into what their child or children are doing on the internet and teachers should also be aware of what goes on. but they cant really stop or change things like they should, there are many ignorant parents out there. i would know as my dad is one of them. im not saying i act irresponsibly on the internet, because i dont, im not that....immature. but MANY people do the wrong thing on a regular basis (Female aged 14).

just a note that parents seem to follow after kids in exploring the internet, while professional development in some employment areas covers this if a parent asks their child "can you help me get facebook" the privacy responsibility is somewhat on the child to explain it to the parent thus school education is vital for families as a whole unit (Female aged 17).

18.35 Indeed, the Inspire Foundation reported that:

There was a prevailing attitude amongst young people that teachers, parents and youth workers didn't really understand technology/how young people use the Internet and therefore weren't in a position to (credibly) advocate safe Internet practices.²⁴

18.36 It has been argued in published papers that, as Australia moves into the future, the inter-generational divide is likely to become a key social issue. It is widely acknowledged that Australia needs a comprehensive plan for dealing with the effects of an ageing population, and that this planning needs to address inter-generational communication practices:

The rise of new technologies has led to the emergence of new patterns of communication and social connection between young people. If we don't act to enhance intergenerational communication, we risk generating a culture structured by a digital/communication divide between young people, their parents and older members of the community. It is vital that we harness the potential for intergenerational communication facilitated by social networking services. This will require a concerted effort to educate older Australians about [social

24 Inspire Foundation, *Submission 3*, p. 9.

networking and new technologies], and enable them to understand how young people identify and respond to the risks and opportunities they present.²⁵

- 18.37 One innovative way of crossing this divide is to invert traditional teaching relationships, so that young people become the teachers in adult education.

Inverting the teaching relationship

- 18.38 Dr Helen McGrath commented on this approach:

There could be more intensive opportunities for parents to become aware of the issues above and beyond what is already available. One very wise principal of my acquaintance said that the only way this could be done is to have kids present about the issues to parents. In doing so you get the double learning but, at the same time, parents are more likely to come and see their children perform. And if, for example, the children were doing a presentation about cybersafety and then they stopped, for a freeze frame, and said, 'What we had to check on before we did this was A, B, C and we were very careful not to do E and F,' then that could be a really engaging way of doing it. It would be getting the kids to teach the parents, but in an engaging way as opposed to a preachy way.²⁶

- 18.39 Importantly, recent studies have been conducted trailing this proposal. Released on 5 April 2011 by the Cooperative Research Centre for Young People, Technology and Wellbeing (YAW-CRC), the *Intergenerational Attitudes towards Social Networking and Cybersafety Report* was based on a Living Lab study.²⁷ The study reversed traditional teaching hierarchies: young people developed and delivered a cyber-safety education workshop to a group of parents.²⁸

25 Collin, P et al, 2011, *The Benefits of Social Networking Services*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 21.

26 Dr Helen McGrath, Psychologist, Australian Psychological Society, *Transcript of Evidence*, 9 December 2010, p. CS66.

27 A 'living lab' is a user-centric research methodology for sensing, prototyping, validating and refining complex solutions in multiple and evolving real life contexts. A living lab simulates a particular social context that allows researchers to observe and analyse 'authentic' interaction.

28 Third A et al, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing.

18.40 Significantly, the YAW-CRC's report found that this model of cyber-safety education established an inter-generational conversation between young people and adults that lead to four substantial outcomes:

- The dialogue leads to a demystification of social networking services and increased parental understanding of the role of these sites as communication tools;
- Adults become more familiar with these services and began to feel more comfortable with the technologies used by their children;
- As a result of this increased familiarity and understanding, parents became more aware of how they could assist their children to be smart, safe and responsible when online; and
- The study's young participants gained a sense of achievement and self-efficacy.²⁹

18.41 Furthermore, while the study's participants acknowledged the value of conventional cyber-safety education, they also emphasised that the majority of effective strategies they had developed for maintaining a safe online presence had been learnt informally. This is primarily conducted through consultation with their peers or a process of trial and error.³⁰

18.42 Adult participants reported that this insight into supportive peer relationships was comforting, with one parent noting, 'It was reassuring. If they don't know how to deal with it they reach out to parents or their friends'.³¹

18.43 Similarly, parents were reassured by the fact that the young participants' online safety was strongly informed by the knowledge and skills they use to remain safe and responsible in the offline world. As one participant commented, 'whenever I'm unsure, I fall back on the things my parents have told me about keeping safe generally'.³² One parent noted that 'my young person [participant] uses the same moral compass in her face-to-face world as in the online world'.³³

29 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 23.

30 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 24.

31 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 18.

32 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 18.

33 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 18.

- 18.44 In its recommendations, the Study advocates a series of guiding principles that should be applied in the development of future cyber-safety education models. According to the authors, education models should be:

developed in partnership with young people and acknowledge their expertise; be experimental as opposed to didactic; combine online and face-to-face delivery; have scope to meet the specific technical skills needs of adults, as well as providing capacity for high level conversations about the socio-cultural dimensions of young people's technology use; and be flexible and iterative so that they can keep pace with the emergence of new online and networked media technologies and practices.³⁴

- 18.45 Engaging young Australians in the study's learning lab reportedly provided participating parents with a supportive environment in which to explore technologies with which they would otherwise feel uncomfortable.³⁵ The Study quoted parent-participants who remarked that

Instead of having adults come to schools to talk about cybersafety, [we should] get young people to share their real life experiences.

and,

The young people have been there, done that, and can talk from experience.

and,

It was very refreshing to speak to someone who is young, open and frank.³⁶

- 18.46 This Study commented that the youth-led workshops inspired adults' confidence in 'young people's capacity to engage in online interactions in responsible and risk-minimal ways'.³⁷ Further, the study's model of cyber-safety education validated and strengthened young people's knowledge and experience in this area.

34 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, pp. 8- 9.

35 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, pp. 16-17.

36 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 17.

37 Third A *et al*, 2011, *Intergenerational Attitudes towards Social Networking and Cybersafety: A Living Lab*, Cooperative Research Centre for Young People, Technology and Wellbeing, p. 18.

18.47 The Committee proposed this idea to the participants of its High School Forum in Hobart:

Hayden-Other generations need to be enlightened as well. Those generations have perceptions. Our generation is the modern generation where everything is about technology and that kind of thing. My parents really do not understand that. They cannot comprehend where we are coming from. They need to be placed in the situation so they can understand where we are coming from.

CHAIR-So would it be better for adults to be taught by other adults or do you think you would do a better job of teaching them? Should it be you out the front teaching parents about it?

Hayden-I think that would be good because it would give the actual view.

Sally-I think that is an excellent idea because a lot of parents have views of internet sites and social networking that are not necessarily true. They have an idea. My dad still gets Facebook and YouTube confused, for example. Seeing that social-networking sites are used predominantly by young people they are probably the best people to inform their elders about that sort of thing.

Dylan-I would tell my parents. If you are close enough to tell your parents and you guys do not mind sharing then I would tell them what is happening and even log on and show them if I am getting bullied or whatnot so that if it comes to it dad or mum can talk to them. I do know a friend who was being bullied on Facebook and their mum logged on and talked to them all, which I suppose is good. We should also be educating the older generation about the things we are using so that when stuff happens they can get involved and help us.

CHAIR-So, rather than the parent going down to the school, they logged onto the technology and spoke through that?

Dylan-Yes, it probably would not be as confronting and if the other people are not willing to come and talk then yes.

Harris-Carrying on from where Sally and Hayden were, I agree it would be a good idea for younger people to educate adults on these things. I agree with a lot of people. We want private conversations like adults want to have conversations with their friends that they do not want children to hear. As a lot of people already know, there are some things that parents do not want their

children to know about, and there are things we do not want our parents know about.

...

Georgia-On the idea that the parents learn, they also have to want to learn. I know the Y generation is meant to be stubborn and to want it all and that sort of thing, and I really want to tread carefully here, but the parents and the adults need to realise that they are also very stubborn. Trying to explain to your mum or a relative or someone like that who is older than you what is going on Facebook is like talking to a brick wall. They do not understand that it is meant to be fun and that. although it does sometimes cause people emotional pain, it is not meant to. They cannot get that around their head--does that make sense?

CHAIR-Thanks.

Harris-Coming back to what I have been saying and following off what Georgia was saying, I think a lot of parents view us as pretty much rebellious: we want to do what we want and we are not going to listen to you. Of course, quite a lot of us do listen to our parents and talk to them, but we also have our views on things and we want to be able to express ourselves. In this sort of generation that we have, I suppose it is similar to when they were growing up as well, because they had their ways to communicate and talk to each other. In a way. you cannot really stop what we are doing. but I see their point: we need to be careful But we still also need to express ourselves in ways that we understand. We have grown up basically like this; we can just talk and be more communicative--communicate better. The internet has opened up a whole new world.³⁸

Recommendation 28

That the Minister for School Education, Early Childhood and Youth consult with the Minister for Broadband, Communications and the Digital Economy to develop measures to introduce:

- **youth leadership courses enabling students to mentor their school communities about cyber-safety issues, and**
- **courses on cyber-safety issues for parents/carers and other adults are developed in consultation with young people and delivered by young people.**

Other suggestions

18.48 As this chapter has already discussed, young people are eager to contribute to developing messages, programs and strategies to promote cyber-safety and ethical online behaviour. Thousands of comments were submitted, through free text spaces in the Committee's survey of how government, industry and other stakeholders can promote safe online practice. Some of these are included below.

Industry

18.49 Young people appear to appreciate the role that industry plays in contributing to safe online experiences. Survey respondents submitted the following comments regarding the possibilities for industry to have a greater role in making the online environment safer:

Put in mechanisms on chat rooms and social media so that anyone who is under 18 gets extra protection so their names don't come up unless being search by a friend and people don't have to use thier real names or ages on their page if they select privately that they want an under-age account or you make and age limit on how old a person can be to be friend wtih a minor or you make police more prolifty and send cyber-stafey instant messages to enveryone who is under 25 about cyberstalking. Have filters to pick up suspicious bejhaviur and make a board to monitor inappropriate pictures so that they can't be put up and allow people to request that slanderous or humiliating images cna be completely deleted off the server and the internet or request that they be buried deeper so that they cant be accessed on google images or searched for (Female aged

15).

Reminders when you ARE online. Everyone knows this information, but if someone was faced with a choice (eg, between giving information out and not) it is most usually the giving side of the argument that wins because there is someone to persuade you. The 'safety' side needs to be persuasive too (Female aged 15).

Site Administrators and Developers

- 18.50 Many comments were submitted by young people discussing the responsibility and opportunities for site administrators and developers in creating positive online environments. Some of the suggestions were broadly framed for site developers and administrators, and some specifically discussed privacy settings.

an easier 'reporting' system, for example on facebook it might take two and a bit weeks for actions to be examined and an account suspended when it should be a bit sooner (Female aged 14).

any complaints (that are valid) that there is a person that may be a stalker or dangerous or anything like that they should NOT be allowed to have access to social networks (Female aged 16).

before a child\adolescent activates a profile on facebook, there should be a page of information that must be read about the risks that they are putting themselves into from just one click of a button (Female aged 14).

Change default settings on social networking site to a higher setting (Male aged 13).

make websites that are the same as websites like facebook and myspace but make them only for kids and set a certain age group so unsafe adults cannot access it but make it with very high security standards (Female aged 14).

On social networking sites, it should be a rule to keep user's pages 16 and under on the highest privacy setting (Female aged 13).

Social Networking sites should make it so that people that are tagged, must agree for the photo to be posted (Male aged 14).

Social networking sites when creating an account should have a section where you have to fill in like a licence or other information and then complete the rest of the stuff. The networking sites could then send that information to the government and then check it and give approval to the

sites profile to go ahead and the permantlaly destroy/very highly protect that information (Female aged 13).

talk to the creators of facebook and ask them to enforce tougher filtering (Female aged 14).

Privacy settings

- 18.51 Young people are concerned about the privacy settings on social networking sites and gaming sites. It appears that they believe that enhanced services and knowledge of privacy settings would assist them to stay safe online.

Allow more choices for what you can allow people to see - both friends and strangers on your social network site (Female aged 14).

Alot more privacy settings on all the social sites (Male aged 13).

automatically have a privacy setting when you get a facebook etc. account (Female aged 13).

Easier to access or adjust privacy settings- some are hidden, it almost seems like they're trying to trick you (Female aged 16).

easier to understand privacy settings. They need to be a lot shorter then maybe more people will be willing to read them (Female aged 15).

giving you the option, when you set up an account, to have private settings instead of having to find the private settings yourself (Female aged 14).

have compulsory settings such as only your friends being able to see your photos or asking a question when you add someone on facebook and if it adds up to the answer the person you are adding has made the friend request will be sent (Male aged 17).

have higher quality privacy pages to allow only the people you chose to access it (Male aged 17).

I think tighter safety settings could be applied on social networking sites, etc, as these sites are used by so many people around the world. There are many ways to view people's private information and a very long & arduous process has to be gone through to get the settings on totally private, as if the website is trying to make it hard enough to set things on private so people won't be bothered to do so. Also there are times when these privacy settings go down, e.g. when new settings are being

updated, allowing everyone's information to become totally public no matter what their privacy settings were. I think this should be improved. I also think that the default security settings on social networking sites should be set at a higher privacy, instead of automatically being available to a large number of people (Female aged 16).

it needs to be easier to access the privacy settings, people who are not that good on computers might want to update the privacy but don't know how to (Female aged 13).

make sure that on sites such as habbo you can not put your full name and email address out there for everyone to see, because to sign up for those things you need to tell the network that stuff anyway so why can't they just monitor it and if you mention someone's full name have it not shown to everybody else?? (Female aged 14).

More privacy laws need to be enforced and implemented for all social networking sites (Female aged 17).

On social networks, you could be forced to read the privacy policy (Female aged 13).

privacy settings being easier to access on social networking sites and all settings being on private (Male aged 15).

Put in mechanisms on chat rooms and social media so that anyone who is under 18 gets extra protection so their names don't come up unless being searched by a friend and people don't have to use their real names or ages on their page if they select privately that they want an under-age account or you make an age limit on how old a person can be to be friend with a minor or you make police more prolific and send cybersafety instant messages to everyone who is under 25 about cyber stalking, have filters to pick up suspicious behaviour and make a board to monitor and inappropriate pictures so that they can't be put up and allow people to request that slanderous or humiliating images can be completely deleted off the server and the internet or request that they be buried deeper so that they can't be accessed on google images or searched for (Female aged 15).

Social networking sites need to make account and privacy settings more user-friendly as well as maybe giving 'recommended' settings according to one's age (Male aged 15).

stronger privacy settings on social networking websites (Female aged 17).

The privacy setting on Facebook should not be optional-it should be an

automatic requirement of the site (Female aged 15).

To have more privacy settings, more control over who can see what (Female aged 13).

When setting up an account on facebook etc apart of signing up you have to look though the settings (Female aged 15).

with facebook, twitter or myspace. many people can still get past your safety, so i feel that internet sites should enable i higher security level for people and a higher age in which they can make the account. theres too many creeps/pedofiles out there (Female aged 15).

With the privacy settings on social networks such as facebook, people you aren't friends with should not be able to see all your information - the setting where they are allowed to should be de-activated. Default security settings - you should only be able to raise them, not lower them (Female aged 15).

you should have easier access to privacy settings. many websites like facebook make it difficult to find them (Male aged 16).

Technology

- 18.52 Young people also submitted comments in the *Are you safe?* survey regarding possible developments in technology that would assist them to feel safer.

A button you can click on to make the site reported on the web if your scared (Male aged 13).

Also having web 'hubs' with most of the things that children enjoy doing on the internet is another way of ensuring safety on the web (roller coaster website is a good example), so a list of website 'hubs' that comply with set guidelines could be a way to help make the internet safer for children, as parents can ensure t(guidelines could include not allowing links to outside webpages and forum areas that are screened and/or policed by administrators - or just have a general age specific section of the website to visit) (Male aged 16).

Design a proper internet filter to stop both internet criminals, hackers and viruses. Make sure the filter is nationally introduced and recognised aswell as free or cheap so it is available for everyone (Male aged 18).

Develop better anti-virus and anti-malware programs and make them

available freely to the public (Male aged 14).

I think that more comprehensive virus-protection should be easier to download and cheap for everyone. I also think that there should be tougher laws on people doing inappropriate things on the internet (Female aged 15).

make programs able to block unsafe websites and ads available free or come with new computers (Female aged 17).

Maybe, there could be a filter that could detect these things and warn the person adding this information on the internet and warn them about what would happen if they did do that (Female aged 14).

Pre-install computers with anti-virus programs to prevent viruses (Female aged 13).

Community

- 18.53 Comments were also submitted discussing broader community awareness and appreciation of cyber-ethics. Notably, when asked how the online environment can be made safer, the following comments were made:

The morals of people themselves need to change. Many people are not perceptive or don't care about awareness advertising. If we are to fix this problem we need to fix societies problems in general. I think manners need to be improved among young people. We also need to spend more time outdoors and not on the internet. Too much technology is a very bad thing. The reason why I did not choose the options of 'learning about it at school' is because most kids just don't listen, it's as simple as that (Female aged 16).

If a difference is to be really made we must look at the problem holistically - as I said, it's all linked. Really what must be done is a whole paradigm shift - changing Australian culture and moving away from the materialistic western way of life to create a more happier harmonious society. I'm not being idealistic, probably the easiest and most effective way to do it (and its possible) is to overhaul school curriculum to make critical thinking skills the focus and centre-piece of education in Australia. Of course it involves a lot more than that, but it's a good start! (Male aged 18).

Without an entire attitude shift to a school or community, no amount of education is going to change the values of a bully, or prevent bullying from being a recurring behavior throughout their life. Perhaps its a

pessimistic view, but i think its partly human nature to bully the weak, (survival of the fittest, etc), but added to that is the representation of teenage life on American television shows which portray bullying as a social necessity to become popular and liked (Female aged 17).

The community as a whole has to take action to ensure that children are not left in these unstable and emotionally damaging environments and do not learn from the bad examples of their parents or carers. To rid the world of bullying, children must comprehend that being cruel is an inappropriate way to act and that bullying is wrong (Female aged 15).

Legislation and law enforcement

- 18.54 Young people also recommend amendments to legislation and law enforcement.

Stronger laws should be passed in Australia to punish (if not internationally then domestically) those involved in cyberfraud, virus writing, identity theft and hacking (Male aged 15).

A better reaction to internet based crime, rather than just leaving it (Female aged 13).

Tackling cyber-bullying

- 18.55 Through its *Are you safe?* survey, the Committee received thoughtful and considered views by young people how cyber-bullying can be reduced. Survey participants made the following suggestions about how cyber-bullying might best be addressed.

Education programs and awareness campaigns

- 18.56 The following comments were made by respondents when asked what can be done to reduce cyber-bullying in the Australian community. They highlight young people's assessment on the successes of education programs:

The procedures in place to reduce bullying seem like a joke to me, and bullying is only increasing so they aren't working. I never listened to the bullying advice seriously, neither did any of my friends, as the way it

was presented to us was laughable (Female aged 17).

I think bringing children up to accept others better will help solve the problem better, a prevention is better than a cure. if students learnt to be more accepting then we wouldnt have to worry about such strict online policies. i know thats unrealistic but it would be nice :) (Female aged 16).

Cyberbullying is a serious matter and should be a major part of learning in schools, whether in primary or secondary. Even though things are being taught in school older people don't realise that even if cyberbullying is being reported to an adult it will still be continued (Female aged 13).

we learn to much about cyber bulling. its really boring because i keep hearing the same thing. Stop with learning. BORING!!!!!!!!!!!!!!!!!!!! (Female aged 13).

We should have programs where we learn about it that is more effective, for example sometimes the only way to make people more aware of cyber bullying is to scare them and show them the results of cuber bullying (Female aged 13).

show those 'cold-truth' stories about cyber bullying and especially stalking. definitely make some videos about cyber stalking and danger (Male aged 17).

I think that schools where children are more educated about cyberbullying usually tend to have less incidences. For example I know that my school has speakers come at least once a year to inform students of the consequences of cyber bullying (Female aged 16).

Again I think it really all depends on people being smart. I think our education on staying safe online is fantastic, however it doesn't target the one thing that can really stop cyber-bullying, and that is peoples attitudes and values to others (Female aged 15).

Changing the infrastructure (e.g. by filtering) will not address the root of the problem. It is more important that people learn to treat one another with humanity and compassion (Male aged 17).

Educate people about the serious consequences of it. People have committed suicide over cyberbullying incidents, it's a pretty serious topic (Male aged 18).

Educate people on how to not make fools of themselves at school. Usually, within our generation, someone with a lack of intelligence is often targeted (Female aged 16).

Educate the common Australian to accept people from different backgrounds instead of judging, naming and inflicting slander on those that are of a minority instead of being ignorant and uneducated racists (Male aged 18).

Educating children about acceptance and tolerance of others who are different to themselves (Female aged 14).

Education about ways to improve self esteem without affecting others (Female aged 15).

Education with the right sources, having a boring government site or spokesperson is hardly an effective education tool. Find a way to educate people of the consequences of cyber bullying and misuse of the internet, be it social or legal (Male aged 17).

Helping kids to understand what it is so they don't end up playing a 'bad joke' and getting in trouble when they didn't know something was wrong in what they were doing (Female aged 14).

if someone came into my school to teach me how to get along better with other people I truthfully wouldn't listen you need to approach it with a different angle (Female aged 15).

just get people to be more socially aware of what cyber-bullying effects are and to teach young ones how to show respect to others yet to still have fun (Male aged 17).

just talking to students about cases where cyber bullying has happened and how much it has affected a person and stuff like that might show more meaningfulness if someone sees how much it can actually hurt and affect someone's life (Female aged 14).

more publicity about people getting in trouble over cyber bullying, so possible bullies know what trouble they will get in (Female aged 15).

scare campaigns. Education about the possible ramifications of cyber bullying e.g. not being able to get a job (Female aged 17).

Teach people that there are actually block buttons on things like Facebook and Youtube that will stop communications altogether. This should be done instead of trying to make up with the person as it blocks ALL contact with the bully. People should be more aware of this (Male aged 14).

Teach people to actually have some respect for others. It'd fix more problems than just cyberbullying (Female aged 16).

Teach stronger school/community spirit - a prevention instead of cure (Female aged 16).

To reduce cyber bullying people actually need to experience what it is like. I think what worked best for me was seeing videos put together about kids taking their lives because of it (Female aged 15).

When most people come and educate us about cyber bullying, it really doesn't stop or reduce it at all. I think what might help is by a speaker coming in and talking to us and saying something like 'if you are cyber bullying, why don't you do a decent thing and apologise or just STOP' (Female aged 13).

- 18.57 Nathan submitted to the Committee that site administrators should exhibit greater awareness and utilisation of existing technological services.

It may seem like a big deal, but as people may not notice, websites such as Facebook and YouTube provide a very good service to stop Cyber-Bullying. First of all, YouTube for example. YouTube provides a "block" button that immediately stops ALL contact with the person that is causing the havoc. People actually see through this "block" button. They may not notice it, or may have the need to actually confront the person when this is not necessary. Blocking a person is a very proficient way of stopping all contact with the person and/or ever speaking to them again. Bullying at school is a different matter, and not related to the Cyber-Bullying in these cases. Facebook on the other hand, goes even further. They provide a "block" button similar to YouTube, which completely blocks ALL contact online, but goes a step further. If the person being harassed may want to keep this person as a friend; they can stop them from posting on their wall, liking their status', and commenting on anything relating to them. This is the quickest way to block ALL contact online, and is an easy way to stop this Cyber-Bullying problem.³⁹

Greater support networks

- 18.58 The following comments about the need for more support were made by respondents:

39 Nathan, *Submission 129* p. 1.

Counselling to cyber-bullies and victims of cyber bullying; support networks for youths (Female aged 16).

Ensuring that children who are bullied are offered support, so that they do not bully others and ensuring children are not allowed to stay in homes where they are abused and consequently wish to abuse others (Female aged 15).

More actions by site administrators

- 18.59 Young people also submitted that site administrators need to become more involved in delivering appropriate support services:

The amount of times that I have reported people to the Facebook Admins and nothing has been done- the only way to make them care is to legislate, but I realise that isn't a practical measure (Male aged 15).

abusive language should be flagged by facebook and if they see that the language was used to offend someone not just as a joke to a friend their facebook account should be terminated (Male aged 15).

clearer report functions and punishments (bans or fines) depending on how bad offence is (Male aged 14).

For website managers to keep a much closer, stricter eye on what is being posted on their site (Female aged 15).

Forcing websites like Facebook to simplify privacy settings so its easier for parents/kids to lock down aspects of their accounts (Male aged 18).

Have people who monitor sites and if they see cyber bullying they report it to authorities (Male aged 14).

Make website administrators respond effectively and timely (Male aged 15).

More information about what cyberbullying is and how to report it (Female aged 14).

More privacy options on social networking sites and a way to change your mobile number easily (Female aged 13).

On social networking sites, I think a reputation system would help (Female aged 16).

Provide manger contact details so that if it does happen you could email

them and they would be removed (Female aged 13).

the people that own websites like facebook, myspace or anything else should have a program that when someone is caught cyber-bullying they should be banned from the website for a couple of hours or a certain amount of time (Female aged 13).

there should be a minimum age requirement for possession of a phone or access to social networking sites. People should know and appreciate its value and recognise that they can hurt people by misusing it. The technology is becoming available to children at a younger and younger age and they are not responsible enough to hand this technology and its dangers (Female aged 16).

Why not make a system that recognises cyberbullying or an online fight and it suspends the students involved from using facebook for 24 hours (Male aged 15).

18.60 A similar comment was made during the Committee's High School Forum, with Ebru commenting that:

When you first get on Facebook there are terms and conditions about bullying, and everyone here has obviously accepted that. It is strange that there can be so much bullying and harassment on Facebook but no-one at Facebook sees it. In the terms and conditions it says that they check to see what we are doing and what kinds of photos we have up, and that if there are harassment reports they will check them. But nothing happens with it at all.⁴⁰

Innovative suggestions

18.61 The following suggestions were made by respondents:

Why not make a system that recognises cyberbullying or an online fight and it suspends the students involved from using facebook for 24 hours (Male aged 15).

Let these bullies do something creative with their time and hence they can achieve. Eg Making Flash movies, rating Flash movies, drawing, making music etc (Male aged 18).

40 Ebru, *Transcript of Evidence*, 20 April 2011, p. CS20.

General comments

18.62 The following general comments were made:

Cyber bullying is an inevitable problem that should not be seen as something that can be completely eradicated. It is a natural exponent of adolescence and will be an inevitable feature of the internet as we know it. Filtering or restricting will not solve the problem, and though prevention and education can help the problem, the underlying cause (adolescence, stupid people doing stupid things etc.) will not go away. Treating these underlying problems will, in the long run, prove to be more beneficial than merely reducing the prevalence of cyber bullying (Male aged 17).

You guys think you know a lot about cyber bullying, but it has been around for a LONG time, you need to work WITH young people about cyber bullying (Female aged 15).

In todays society technology is so easily accessible. Currently i am on my laptop with my phone just by my side. These tools can be used to our advantage or they can be easily abused and mistreated. ... Like anything there are positives and negatives and with Facebook for example it keeps everyone in touch and up-to-date with our friends or families lives, it also can be used as source to find a bullies next victim and so easily done. [Cyber-bullying] is a problem and does need to be fixed. but the problem comes [from] the bullies themselves, because in all honesty who has the time or motives to get on the internet and for their own pleasure make someones life horrible? ... So my theory is don't treat the symptom treat the disease... For example don't have a panadol every time you get a headache, its better to think- why have i got a head ache, oh im dehydrated, then have a glass of water to treat the hydration and then the headache will sort itself out. if we sort out the problems of these bullies the rest of it will all sort itself out (Female aged 16).

I think that cyber-bullying can be prevented by the victim, each of the activities listed above that supposedly cyber-bullying can be prevented. for example unwanted emails can be blocked from the specific sender. if the victim doesnt want to talk to someone on the internet then they can do things to prevent it (Male aged 16).

No one stands up for them... teachers talk big but when you report it... they really dont take action (Male aged 14).

There aren't really any consequences for bullying online, its hard for the

victim to fight back (Male aged 17).

Cyber bullying only happens if you respond. If you block all contact then it cannot happen, the kids need to learn to just not respond. Responding feeds the "trolls", an internet term to describe someone that acts in a way to annoy someone ect (Male aged 17).

cyber-bullying has existed since the beginning of the internet - there is little that can be done to prevent it. but, maybe it would decrease in frequency if social networking sites (deviantart etc.) could be accessible in learning environments, children would not be so inclined to bully, for teachers could assist in the prevention (Female aged 14).

cyber-bullying is the manifestation of bullying in the internet age, so the failures to reduce playground bullying and aggression in Australian society might be the same failures we will begin to see occurring in the attempts/efforts/initiatives to reduce cyber-bullying (Male aged 18).

DISCOURAGE the use of social networking sites. Yes, they are gerat in keeping in contact with friends and for other necessary communication, but people are using them far too frequently and they are taking over other aspects of life. People, particularly younger people, need to recognise how superficial they are, and that they are NOT an essential part of life (Female aged 17).

I don't think anything can really be done, but maybe raising awerness can help a little (Female aged 17).

I think teenagers have to grow up to the fact that what they say/do/post to/about someone can actually hurt (Female aged 15).

If a student ect reports something DO SOMETHING ABOUT IT - not just get the student to 'appologise' because they NEVER mean it (Male aged 14).

Not very much. Trying to control behaviour intrudes personal freedom and independence unless they were taught to be well behaved from the very beginning (kindergarten) and they understand the value of being a warm hearted person. Forcing one to learn may cause inconsistency of leading a positive life, and may backfire as a result of self independence and rebellion. That is a danger (Male aged 16).

Tell kids that it's okay to block or report people that make them feel uncomfortable. It doesn't make them weak if they do (Female aged 16).

Conclusion

- 18.63 It is important that cyber-safety initiatives value the contributions, ideas and existing knowledge of young people, and seek to build upon that knowledge. They have a wonderful capacity to adapt, learn and inform their peers, and this capacity should be harnessed in initiatives that government, industry and non-profit organisations develop.

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, *Submission 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 Principals' 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 location⁴⁵

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 Dalglish, 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, *Submission 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-safety⁵⁶. 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 Dalglish, 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

Appendices



Appendix A — Submissions

- 1 Australian Communications Consumer Action Network
- 2 Yahoo!7
- 2.1 Yahoo!7
- 2.2 Yahoo!7
- 3 Inspire Foundation
- 4 Armorlog International Ltd
- 4.1 Armorlog International Ltd
- 5 beyondblue
- 6 Stride Foundation Ltd
- 7 CyberValues.Org
- 8 Catholic Education Office, Archdiocese of Canberra and Goulburn
- 9 South Australian Commission for Catholic Schools
- 10 Australian Parents Council Inc.
- 11 Australian Education Union
- 12 Safer Internet Group
- 13 Google Australia Pty Ltd
- 14 Telstra Corporation Ltd
- 15 Mr Mark Newton
- 16 Australian Library and Information Association

- 17 Netbox Blue Pty Ltd
- 18 Childnet International
- 19 Association of Independent Schools of South Australia
- 20 Australian Council for Education Research
- 21 Queensland Teachers' Union
- 22 Alannah and Madeline Foundation
- 23 Civil Liberties Australia
- 24 Catholic Education Office of W.A.
- 25 Youth Affairs Council of South Australia
- 25.1 Youth Affairs Council of South Australia
- 26 Tutoring Australasia Pty Ltd
- 27 Association of Principals of Catholic Secondary Schools
- 28 Australian Youth Affairs Coalition
- 29 BoysTown
- 30 Victorian Office of the Child Safety Commissioner
- 31 Centre for Children and Young People
- 32 NSW Secondary Principals' Council
- 33 Queensland Secondary Principals Association
- 34 BraveHearts Inc
- 35 Association of Children's Welfare Agencies
- 36 Australian Direct Marketing Association
- 37 The Brainary
- 38 Family Online Safety Institute
- 39 Australian Institute of Family Studies
- 40 Mr Johann Trevaskis
- 41 ACT Council of P&C Associations Inc.
- 42 Singtel Optus Pty Ltd
- 43 NSW Parents Council Inc.

-
- 44 Ms Candice Jansz
- 45 Australian Toy Association
- 46 Telecommunications Industry Ombudsman
- 47 Office of the Director of Public Prosecutions, NSW
- 48 Peer Support Australia
- 49 Commonwealth Director of Public Prosecutions
- 50 Family Voice Australia
- 51 Device Connections Pty Ltd
- 52 Mental Health Council of Australia
- 53 Australian and New Zealand Ombudsman Association
- 54 Commissioner for Children and Young People WA
- 54.1 Commissioner for Children and Young People WA
- 55 Simon Fraser University
- 56 Australian Institute of Criminology
- 57 Commissioner for Children, Tasmania
- 58 Attorney-General's Department
- 58.1 Attorney-General's Department
- 59 Office of the Victorian Privacy Commissioner
- 60 Mr Bruce Arnold
- 61 Privacy NSW
- 62 Australian University Cyberbullying Research Alliance
- 63 Communications Law Centre
- 64 Australian Federal Police
- 65 Western Australia Office of Commissioner for Police
- 66 Mr Nick Abrahams and Ms Ju Young Lee
- 67 Queensland Catholic Education Commission
- 68 Associate Professor Karen Vered
- 69 NSW Primary Principals' Association Inc

- 70 Community Technology Centres Association
- 71 System Administrators Guild of Australia
- 72 Australian School Library Association Inc.
- 73 New South Wales Teachers' Federation
- 74 Council of Australian University Librarians
- 75 Australian Council on Children and the Media
- 76 Federation of Parents and Citizens' Associations of NSW
- 77 Catholic Primary Principals' Association of WA
- 78 Western Australia Office of Commissioner for Police
- 78.1 Western Australia Office of Commissioner for Police
- 79 Cancelled and accepted as Submission No 36
- 80 Australian Communications and Media Authority
- 81 Mr Paul Myers
- 82 ACT Government
- 82.1 ACT Government
- 83 Australian Privacy Foundation
- 84 Northern Territory Government
- 85 Tasmania Police
- 86 South Australia Police
- 86.1 South Australia Police
- 87 Microsoft Australia Pty Ltd.
- 88 Internet Industry Association
- 89 Timesavers International Pty Ltd
- 90 The Australian Psychological Society
- 91 ninemsn Pty Ltd
- 92 Office of the Privacy Commissioner
- 93 Uniting Church in Australia, Synod of Victoria and Tasmania
- 93.1 Uniting Church in Australia, Synod of Victoria and Tasmania

-
- 93.2 Uniting Church in Australia, Synod of Victoria and Tasmania
- 94 NSW Government
- 95 Berry Street
- 95.1 Berry Street
- 96 Web Management InterActive Technologies Pty Ltd
- 97 National Association for the Prevention of Child Abuse and Neglect
- 98 South Australian Office for Youth
- 99 Queensland Council of Parents and Citizens' Associations Inc.
- 100 Roar Educate
- 101 iKeepSafe
- 102 Brilliant Digital Entertainment Pty Ltd
- 103 Name withheld
- 104 Name withheld
- 105 Mr Geordie Guy
- 106 Name withheld
- 107 Child Sexual Abuse Prevention Program
- 108 Inspire International Research Institute
- 109 Australian Customs and Border Protection Service
- 110 Interactive Games & Entertainment Association
- 111 Murdoch Children's Research Institute
- 112 Victorian Government
- 113 Australian Government's Consultative Working Group on CyberSafety
- 114 Department of Education, United Kingdom
- 115 WA Department of Education
- 116 Mr Alex James
- 117 Australian Mobile Telecommunications Associations
- 118 Western Australia Government
- 119 Australian Curriculum, Assessment and Reporting Authority

- 120 The Royal Australian & New Zealand College of Psychiatrists
- 121 Australian Clearinghouse for Youth Studies
- 122 Associate Professor Bjorn Landfeldt
- 123 Dr Roger Clarke
- 124 Australian Regional Media
- 125 Association of Heads of Independent Schools of Australia
- 126 Rachel
- 127 headspace National Office
- 128 The Australian Council for Computers in Education
- 129 Nathan and James
- 130 Name withheld
- 131 Jodie
- 132 Abbie
- 133 Jedidiah
- 134 Ms Annette Atkins
- 135 Department of Education, Employment and Workplace Relations
- 136 Mr Stewart Healley
- 136.1 Mr Stewart Healley
- 136.2 Mr Stewart Healley
- 136.3 Mr Stewart Healley
- 137 Australian Education Union Tasmanian Branch
- 138 National Children's & Youth Law Centre
- 139 Jayme
- 140 Name withheld
- 141 Vodafone Hutchison Australia
- 142 Verity
- 143 Parents Victoria Inc.
- 144 Tiger

- 145 Lisa
- 146 Vincent
- 147 Baily
- 148 Electronic Frontiers Australia Inc
- 149 Australian Christian Lobby
- 150 Department of Education, Employment and Workplace Relations
- 151 Australian and New Zealand Policing Advisory Agency
- 152 Catholic Education Office, Diocese of Wollongong
- 152.1 Catholic Education Office, Diocese of Wollongong

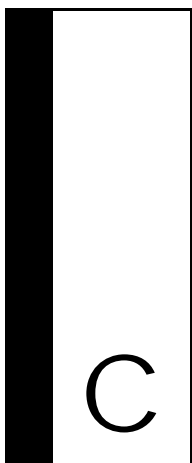


Appendix B — Exhibits

- 1 Australian Communications and Media Authority
Online risk and safety in the digital economy: Third annual report to the Minister for Broadband, Communications and the Digital Economy on developments in internet filtering and other measures for promoting online safety
- 2 Australian Communications and Media Authority
Developments in internet filtering technologies and other measures for promoting online safety: Second Annual Report to the Minister for Broadband, Communications and the Digital Economy
- 3 Australian Communications and Media Authority
Developments in internet filtering technologies and other measures for promoting online safety: First Annual Report to the Minister for Broadband, Communications and the Digital Economy
- 4 Australian Communications and Media Authority
cyber[smart:]: Cybersafety Outreach, Professional development for educators
- 5 Australian Communications and Media Authority
cyber[smart:]: Cybersafety Outreach, Pre-service teacher pilot program
- 6 Australian Communications and Media Authority
cyber[smart:]
- 7 SuperClubsPLUS
SuperClubsPLUS, Its role in cybersafety education and learning in young children
- 8 ArmorLog International Ltd
A System To Secure User Login Credentials (Related to Submission No. 4)

- 9 Youthbeyondblue
Youthbeyondblue Fact sheet 20, Bullying (Related to Submission No. 5)
- 10 Youthbeyondblue
Youthbeyondblue Fact sheet 23, Cyberbullying (Related to Submission No. 5)
- 11 The Alannah and Madeline Foundation
Navigating the maze: cybersafety and wellbeing solutions for schools
- 12 Principals Australia
Student Empowerment: Information book
- 13 Stride Foundation Limited
Cyber-Bullying: A youth empowerment and prevention program (Related to Submission No. 6)
- 14 CyberValues.Org
John Bellavance Community Involvement Profile (Related to Submission No. 7)
- 15 ROAR Film Pty Ltd
US Online Next Generation: Enabling ICT and Safeguarding for Contemporary Learning and Life (Related to Submission No. 100)
- 16 iKeepSafe
C3Matrix Digital Citizenship: A Companion to the Augmented Technology Literacy Standards for Students (Related to Submission No. 101)
- 17 CONFIDENTIAL
- 18 Jane Fae Ozimek
The Register: Academics challenge moral consensus on sex and the net
- 19 Department of Education, United Kingdom
Safer Children in a Digital World: The Report of the Byron Review (Related to Submission No. 114)
- 20 Department of Education, United Kingdom
Do we have safer children in a digital world?: A review of progress since the 2008 Byron Review (Related to Submission No. 114)
- 21 UK Council for Child Internet Safety
Click Clever Click Safe (Related to Submission No. 114)
- 22 UK Council for Child Internet Safety
Children's online risks and safety (Related to Submission No. 114)

-
- 23 Australian Mobile Telecommunications Association
Mobile phones and bullying: what you need to know to get the bullies off your back.
(Related to Submission No. 117)
- 24 Australian Mobile Telecommunications Association
Bullying with Mobile Phones. Is your child a victim? What you can do to help.
(Related to Submission No. 117)
- 25 Australian Mobile Telecommunications Association
Developing an acceptable use policy for mobile phones in your school (Related to Submission No. 117)
- 26 Mr Clive Alsop
The Menace of the Internet: An Australian Perspective
- 27 Commissioner for Children and Young People, Western Australia
Speaking out about wellbeing: The views of Western Australian children and young people (Related to Submission No. 54.1)



Appendix C — Witnesses

Friday, 11 June 2010 - Melbourne

Individuals

Dr Julian Dooley

Australian Federal Police

Superintendent Bradley Shallies, National Coordinator Child Protection Operations

Facebook Inc

Hon Mozelle Thompson, Chief Privacy Advisor

Internet Industry Association

Mr Peter Coroneos, Chief Executive Officer

Principals Australia

Mr Jeremy Hurley, Manager, National Education Agenda

The Alannah and Madeline Foundation

Dr Judith Slocombe, Chief Executive Officer

University of South Australia

Dr Barbara Spears, Senior Lecturer, School of Education

Youth Affairs Council of Victoria Inc.

Ms Georgie Ferrari, Chief Executive Officer

Wednesday, 30 June 2010 - Sydney

Association of Parents and Friends of ACT Schools

Ms Kate Lyttle, Executive Officer

Australian Education Union

Ms Catherine Davis, Federal Women's Officer

Deakin University

Dr Helen McGrath, Senior Lecturer, Faculty of Education

Federation of Parents and Citizens Associations of New South Wales

Ms Dianne Butland, Executive Member - State Council

Independent Education Union of Australia

Mr Chris Watt, Federal Secretary

Queensland University of Technology

Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Faculty of Education

Thursday, 8 July 2010 - Melbourne

Safer Internet Group

Mrs Sue Hutley, Executive Director, Australian Library and Information Association

Internet Industry Association

Mr Peter Coroneos, Chief Executive Officer

Internode Pty Ltd

Mr John Lindsay, General Manager Regulatory and Corporate Affairs

Netbox Blue Pty Ltd

Mr John Pitcher, Director of Strategic Business Development

Symantec Corporation

Mr Craig Scroggie, Vice President and Managing Director, Asia Pacific Region

Telstra Corporation Ltd

Mr Darren Kane, Director, Corporate Security & Investigations and
Telstra's Officer of Internet Trust & Safety

Yahoo!7 Australia and New Zealand

Ms Samantha Yorke, Acting General Counsel

Thursday, 9 December 2010 - Melbourne**Australian Council for Educational Research**

Dr Paul Weldon, Research Fellow

Dr Gerald White, Principal Research Fellow

Berry Street

Ms Sherree Limbrick, Director – Statewide Programs

Ms Lauren Oliver, Internal Consultant, Youth Empowerment and
Participation

beyondblue

Ms Michelle Noon, Program Manager - Youth

Australian Psychological Society

Dr Helen McGrath, Psychologist

FamilyVoice Australia

Mr Richard Egan, National Policy Officer

Cyber Safe Kids

Ms Robyn Treyvaud, Founder

Office of the Victorian Privacy Commissioner

Dr Anthony Bendall, Deputy Victorian Privacy Commissioner

Privacy Victoria

Ms Helen Versey, Privacy Commissioner

Stride Foundation Limited

Ms Kelly Vennus, Program and Training Manager

Murdoch Children's Research Institute

Associate Professor Sheryl Hemphill, Department of Paediatrics

Victorian Office of the Child Safety Commissioner

Mr Bernie Geary OAM, Child Safety Commissioner

Ms Megan Scannell, Senior Project Manager

Thursday, 3 February 2011 - Adelaide

Association of Principals of Catholic Secondary Schools

Mr Philip Lewis, Chair

Australian Council on Children and the Media

Ms Barbara Biggins OAM, Hon CEO

Ms Lesley-Anne Ey, Executive Committee Member

Prof Elizabeth Handsley, President, Board Member and Chair of Executive Committee

Carly Ryan Foundation Inc

Mr Daniel Orr, Editor and Committee Member

Ms Sonya Ryan, Director

Catholic Education Office SA

Ms Mary Carmody, Senior Education Adviser, Learning and Student Wellbeing

Department of Education and Children's Services, South Australia

Mr Greg Cox, Senior Policy Officer, Student Wellbeing

FamilyVoice Australia

Mr David d'Lima, South Australia State Officer

Mrs Roslyn Phillips, National Research Officer

Flinders University

Associate Professor Karen Vered, Head, Department of Screen and Media

Office for Youth, Attorney-General's Department, South Australia

Mrs Tiffany Downing, Director

Ms Suellen Priest, Policy and Programs Officer

Mrs Sandy Dawkins, Manager, Engagement and Wellbeing

The Australian University Cyberbullying Research Alliance (AUCRA)

Associate Professor Marilyn Campbell

Prof Phillip Slee

Dr Barbara Spears

Youth Affairs Council of South Australia

Ms Anne Bainbridge, Executive Director

Mr Lucas de Boer, Project Officer

Thursday, 3 March 2011 - Canberra

Australian Communications and Media Authority

Ms Jonquil Ritter, Acting General Manager, Consumer, Content and Citizen Division

Ms Sharon Trotter, A/g Executive Manager, Security Safety and e-Education Branch, Digital Economy Division

Ms Andree Wright, A/g General Manager, Content, Security, Safety and e-Education Branch, Digital Economy Division

Department of Broadband, Communications and the Digital Economy

Mr Simon Cordina, Assistant Secretary, Cyber-Safety and Trade Branch, Digital Economy Strategy Division

Ms Deborah Masani, Manager, Cybersafety Programs, Cybersafety and Trade Branch

Mr Abul Rizvi, Deputy Secretary, Digital Economy & Services Group

Mr Richard Windeyer, First Assistant Secretary, Digital Economy Strategy Division

Thursday, 17 March 2011 - Brisbane

Australian School Library Association Inc.

Ms Karen Bonanno, Executive Officer

Mrs Christine Kahl, Treasurer

BoysTown

Ms Tracy Adams, Chief Executive Officer

Mr John Dagleish, Manager, Strategy and Research

Ms Megan Price, Senior Research Officer

Bravehearts Inc

Ms Hetty Johnston, Founder and Executive Director

Brisbane Catholic Education

Ms Anita Smith, Senior Education Officer, Student Wellbeing, Learning
And Teaching Services

Department of Education and Training, Queensland

Mr Michael O'Leary, Executive Director, Information And Technologies
Branch, Web And Digital Delivery

Ms Patrea Walton, Acting Deputy Director-General

Device Connections Pty Ltd

Mr Geoffrey Sondergeld, Director

Netbox Blue Pty Ltd

Mr John Fison, Chairman

Queensland Catholic Education Commission

Mr Gavin Carmont, IT Manager

Mr Robert Knight, Executive Office, Education

Mr Michael Wilkinson, Executive Secretary

Queensland Secondary Principals Association

Mr Norm Fuller, President

Mrs Julie Tabor, Executive Member

Queensland Teachers Union

Mr Mark Anghel, Assistant Secretary, Legal Services, Welfare

System Administrators Guild of Australia's

Ms Donna Ashelford, President

Mr Burke Scheld, Executive Officer

Web Management InterActive Technologies Pty Ltd

Mr James Collins, Managing Director

Monday, 21 March 2011 - Canberra**Individual**

Dr Roger Clarke, Private capacity

Facebook Inc

Hon Mozelle Thompson, Advisor Board and Policy Adviser

Microsoft Australia Pty Ltd.

Mr Stuart Strathdee, Chief Security Advisor

ninemsn Pty Ltd

Ms Jennifer Duxbury, Compliance, Regulatory and Corporate Affairs
Director

Yahoo!7 Australia and New Zealand

Ms Samantha Yorke, Legal Director, Asia Pacific Region

Thursday, 24 March 2011 - Canberra**Attorney General's Department**

Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law
Enforcement Branch

Australian Federal Police

Commander Grant Edwards, Acting National Manager, High Tech Crime
Operations

Australian Institute of Criminology

Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program

University of Sydney

Associate Professor Bjorn Landfeldt, School of Information Technologies

Wednesday, 20 April 2011 - Hobart

Australian Parents Council Inc.

Mr Ian Dalton, Executive Director

Department of Education Tasmania

Ms Liz Banks, Acting Deputy Secretary (Early Years and Schools)

Mr Trevor Hill, Director, Information Technology Services

ROAR Educate Pty Ltd

Mr Craig Dow Sainter, Managing Director

Ms Melinda Standish, Education Writer



Appendix D – Survey Methodology

The intention of the Committee's *Are you safe?* survey was to gather the opinions and experiences of young people on the topics of cyber-safety, cyber-bullying and their strategies to mitigate online dangers. Other issues explored included who are the main support networks of young people, the rate of cyber-safety awareness and the types of information young people divulge online. The survey's respondents also had valuable and numerous proposals as to how cyber-safety can be promoted and cyber-bullying reduced.

A combined qualitative and quantitative approach was adopted. The online survey form included a series of set answers that respondents could choose from as well as a free text space for most questions. The Committee received almost 60,000 comments from its total participants (33,751).

The survey was advertised extensively. It was circulated to approximately 7,000 primary and secondary schools throughout Australia. Senators and Members of Parliament were also contacted to request that they place a link to the survey on their websites, social networking profiles and in constituent newsletters. Similarly, submitters to the inquiry were contacted to promote the survey through their networks.

Due to the target audience and subject-matter, the Committee realised that online advertising would be essential. Consequently, the survey was advertised on Facebook and Google following previous success with these sites. In addition to Committee-directed advertising, the survey was advertised online by industry leaders and on state governments as a result of the Committee's continued engagement and outreach to these groups. These included Microsoft's GovTech, Bravehearts, the Tasmanian Police and others.

Sample

The analysis sample consisted of 33,751 self-selected and school-selected participants aged between 5 and 18 years of age. Self-selected participants were sourced from a series of online and printed media campaigns. Participants were also sourced as a result of the Committee's invitation to some 7,000 schools around Australia.

The majority of participants were aged between 10 and 15 years of age (80.7%). Of the total respondents that identified their gender, 53.2% were female and 46.8% were male.

Content

It was important to the Committee to hear from young Australians from a broad age group: 5 to 18 years of age. The breadth of this target group required the Committee to develop two streams that were age appropriate.

The first stream was for children up to 12 years of age, and the second was for young people aged between 13 and 18 years of age. The two age groups mirror the national average age of primary school students and high school students respectively. To ensure their suitability, questions were framed in accessible language and developed in partnership with an external consultant with expertise in social research.

The first, younger stream consisted of 16 to 18 quantitative questions of which 10 had a supplementary qualitative question. Certain questions were omitted if respondents answered in the negative to earlier questions. Similarly, the older stream consisted of 22 to 24 web-based questions, with 13 qualitative questions. Again, questions were omitted if respondents answered earlier questions that would have made later questions redundant.

The combination of both qualitative and quantitative questions allowed flexibility in the data collection as well as providing the survey's young participants an opportunity to clarify their selections in quantitative questions. The qualitative questions also allowed the Committee to receive in-depth descriptions of experiences as well as suggestions directly from young people on how governments, industry, schools and parents might best tackle issues of cyber-safety and cyber-bullying.

Both streams asked questions about privacy, prevalence of cyber-safety concerns, awareness of resources and avenues of assistance, and existing education programs. Also included were questions specifically on cyber-bullying, including

its perceived frequency, motivations, how those involved responded, and methods for reducing its prevalence.

Once the respondent completed the survey, they were invited to make further recommendations to the Committee. The Committee received 11 submissions as a result of this invitation.

While responses to the survey were anonymous, respondents were asked to provide some basic demographic information (age and gender) to assist with the analysis of responses.

Data analysis

Due to the fact that many of the questions offered multiple responses, reported percentages often do not equal 100%.

Some survey respondents did not provide details of their age and/or their gender. Where tables and graphs present data on either of these two particulars, the unstated figures are specifically identified (where appropriate) or discounted from the analysis.

Importantly, the survey methodology relied on a degree of self-selection rather than strict cross-sectional population sampling. The survey was intended to be descriptive and findings should not be used to extrapolate to the general youth population. Furthermore, as responses to the survey were anonymous the authenticity of input cannot be guaranteed.

Online Survey for 12 years and younger

The survey for 12 years and younger included the following preamble:

Are you 12 years or under? Please tell us how you stay safe online!

Information you and your parents might want to know:

The Australian Parliament is holding an inquiry into cyber-safety issues facing young Australians, and would like to hear your views. We are particularly interested in young Australian's views about the dangers online including cyber-bullying, stalking, identity theft and breaches of privacy.

This survey will be completely anonymous and we will not know who you are. By clicking the link below, you will be taken to a secure survey website.

The information you give us will be used to tell the Commonwealth Parliament's Joint Select Committee on Cyber-Safety about the experiences young people have with cyber-safety and cyber-bullying. It will also be used to help write the final report, which will contain recommendations to the Australian Government on what can be done about these issues.

Questions for 12 years and younger

1. Do you think that you are anonymous when you are online?
 - Yes
 - No
2. What information about yourself is ok to put up on a webpage or over the internet that strangers might read?
 - Your name
 - ⇒ Yes / No / I don't know
 - Your address
 - ⇒ Yes / No / I don't know
 - Your telephone number
 - ⇒ Yes /No / I don't know
 - Your age or birthday
 - ⇒ Yes / No / I don't know
 - Bank account information about you or your family
 - ⇒ Yes / No / I don't know
 - The school you attend
 - ⇒ Yes /No /I don't know
 - Nude or semi-nude photos to others via text message or email
 - ⇒ Yes /No /I don't know
 - If you are going on holiday
 - ⇒ Yes /No / I don't know
 - Your passwords or email addresses
 - ⇒ Yes /No /I don't know
 - Post photos of others without their permission
 - ⇒ Yes /No /I don't know

Would you like to tell us more?

3. Have you ever felt unsafe on the internet?

- Yes
- No

Would you like to tell us more?

4. Who do you feel you could talk to if you were worried about something you saw on the internet?

- Your family
- Your friends
- Your teacher
- The police
- The administrators of the site
- Talk to no one
- Other [free text option]

Is there anything more you would like to tell us?

5. Does anyone in your family talk about how to stay safe when you are on the Internet?

- Yes
- No

6. Are you about your safety when you are on the Internet?

- Yes, I'm worried a lot
- Yes I'm worried a bit
- No, I'm not worried

7. Where did you learn about safety when using the Internet?

- At school
- Information on internet
- From family
- From friends
- Never learnt about it
- Other [free text option]

8. What do you think can be done to make you safer online?

- Talk about it more with family
- Learn about it at school
- Ask friends
- More policing and enforcement
- Tougher filtering of the Internet
- Make public internet access such as libraries safer
- Nothing, it is safe now

Anything else that can be done to make it safer online? [free text option]

DEFINITION GIVEN ON CYBER-BULLYING

Cyber-bullying is when these things happen AGAIN AND AGAIN to someone who finds it hard to stop it from happening:



When you answer the next questions, please think about cyber-bullying in this way. You can look back at this definition to remind yourself of what cyber-bullying is by clicking the links in the questions.

9. Of the following groups, who do you think is most often cyber-bullied?

- Boys
- Girls
- Strangers
- Other [free text option]

10. In the last year, do you know anyone who was cyber-bullied?

- Yes
- No

Want to tell us more?

11. In the last year, has someone cyber-bullied you?

- Yes
- No

12. You told us that during the past year, somebody has cyber-bullied you.
Who did you tell?

- I did not tell anyone
- I told.... [free text space]

13. When you were cyber-bullied, what did you do about it?

- Block the bully or removed as a friend from Facebook or other similar sites
- Spoke to the bully
- Told a friend
- Stayed offline
- Told adult or family member
- Got back at them
- Did nothing
- Other [free text space]

14. Why do people cyber-bully?

- Mixing with the wrong crowd
- People looking for a fight
- Fighting over girls or boys
- Copy cat of news stories
- Boredom
- Bad home life
- Lack of respect for others
- Don't like people with disabilities
- Don't like people from different backgrounds
- Other [free text option]

15. What can be done to stop cyber-bullying?

- Teach people how to get along better
- Teach people how to control their anger
- Better education on staying safe online

- Provide more policing and enforcement
- Provide more safe youth centres with entertainment and recreational facilities
- Increasing Internet filtering options
- Other? [free text option]

Want to tell us more?

16. Are you a...

- Boy
- Girl

17. How old are you?

- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12

Message on completed page

Thank you for completing our survey!

If you ever feel unsafe online, or need help with cyber-bullying logon to <http://cybersmart.gov.au/report.aspx> to get help or report what you have seen.

Online Survey for 13 years and older

The survey for young people aged between 13 and 18 was preceded by the following preamble:

Are you aged between 13 and 18 and want to have your say in the development of safer online environments?

The Australian Parliament is holding an inquiry into cyber-safety issues facing young Australians, and would like to hear your views. We are particularly interested in your views about the dangers online including cyber-bullying, stalking, identity theft and breaches of your privacy.

This survey will be completely anonymous and it will not be possible for us to identify anybody who participates in this survey. By clicking the link below, you will be taken to a secure survey website.

The information you provide will be used to inform the Commonwealth Parliament's Joint Select Committee on Cyber-Safety about the experiences young people have with cyber-safety and cyber-bullying. It will also be used to help write the final report, which will contain recommendations to the Australian Government on what can be done about these issues.

Questions for 13 years and older

1. Do you think that you are anonymous when you are online?
 - Yes
 - No
2. What information about yourself is ok to put up on a webpage or over the internet that strangers might read?
 - Your name
 - ⇒ Yes / No / I don't know
 - Your address
 - ⇒ Yes / No / I don't know
 - Your telephone number
 - ⇒ Yes /No / I don't know
 - Your age or birthday
 - ⇒ Yes / No / I don't know

- Bank account information about you or your family
⇒ Yes / No / I don't know
- The school you attend
⇒ Yes /No /I don't know
- Nude or semi-nude photos to others via text message or email
⇒ Yes /No /I don't know
- If you are going on holiday
⇒ Yes /No / I don't know
- Your passwords or email addresses
⇒ Yes /No /I don't know
- Post photos of others without their permission
⇒ Yes /No /I don't know

Would you like to tell us more?

3. Have you ever felt unsafe on the internet?
- Yes
 - No

Would you like to tell us more?

4. Who do you feel you could talk to if you were worried about something you saw on the internet?
- Your family
 - Your friends
 - Your teacher
 - The police
 - The administrators of the site
 - Talk to no one
 - Other [free text option]

Is there anything more you would like to tell us?

5. Does anyone in your family talk about how to stay safe when you are on the Internet?
 - Yes, frequently
 - Yes, sometimes
 - Yes, when I ask about it
 - No, never

6. How worried are you about your safety when you are on the Internet? Would you say...
 - Worried all of the time
 - Worried most of the time
 - Worried some of the time
 - Not worried at all

7. Where did you learn about your personal safety when using the Internet?
 - At school
 - Information on internet
 - From family
 - From friends
 - Never learnt about it
 - Other [free text option]

8. If you have a facebook page, myspace account or other webpage on a social networking site, have you explored the privacy settings provided by these sites?
 - Yes
 - ⇒ I have left them at the default setting
 - ⇒ I have increased them to the highest setting
 - ⇒ I like everybody being able to access my page, so I don't have any privacy settings enabled

- No
 - I don't know
 - I don't have a social networking page
9. Do you think more can be done to make it safer online?
- Yes
 - No
 - I don't know
10. What do you think can be done to ensure safety online?
- Talk about it more with family
 - Learn about it at school
 - Ask friends
 - More policing and enforcement
 - Tougher filtering of the Internet
 - Make public internet access such as libraries safer
 - Nothing, it is safe now
 - Anything else that can be done to make it safer online?
11. Of the following activities, what do you think is cyberbullying?
- Posting or sending embarrassing photos of someone else
 - Teasing someone in
 - ⇒ emails
 - ⇒ chat rooms
 - ⇒ discussion groups
 - ⇒ online social networking sites
 - ⇒ instant messaging services
 - Spreading rumours online
 - Sending unwanted SMS or emails

- Sending hurtful SMS or emails
- Creating fake profiles or websites
- Are there any other things that are cyber-bullying?

12. Is repeatedly searching someone's facebook page or blog, stalking?

- Yes
- No
- I don't know

13. Would you say that cyber-bullying

- Seems to be increasing
- Seems to be decreasing or
- Has not changed

14. Of the following groups, who do you think is most often targeted by cyber-bullies?

- Boyfriends
- Girlfriends
- Other friends
- Others at school or at your job
- Strangers
- Other [free text option]

15. In the last 12 months, have you seen (but not been involved in) cyber-bullying among young people?

- Yes
- No
- Could you tell us something about that? [free text option]

16. In the last 12 months, have you been the victim of cyber-bullying?

- Yes
- No

17. You told us that during the past 12 months, you have been cyber-bullied.
Who did you tell?

- I did not tell anyone
- I told...
 - ⇒ Family
 - ⇒ Friends
 - ⇒ Teacher
 - ⇒ Police
 - ⇒ Manager of the website
 - ⇒ The Australian Communications and Media Authority (ACMA)
 - ⇒ Other [free text option]

18. What did you do about it?

- Block the bully or removed as a friend from Facebook
- Confronted the bully
- Told a friend
- Stayed offline
- Told adult or family member
- Sought revenge or paid them back
- Ignored it
- Other [free text space]

19. In the last 12 months, have you been directly involved in cyber-bullying?

- Yes
- No

20. What do you think are the three main factors that lead to cyber-bullying?

- Mixing with the wrong crowd
- People looking for a fight and/or have an aggressive personality
- Fighting over girls or boys
- Copy cat of news stories
- Boredom
- Bad home life
- Lack of respect for others
- Not liking people with disabilities
- Not liking people from different backgrounds
- Other [free text option]

What do you think can be done to reduce cyber-bullying?

- Teach people how to get along better
- Teach people how to control their anger
- Better education on staying safe online
- Provide more policing and enforcement
- Provide more safe youth centres with entertainment and recreational facilities
- Increasing Internet filtering options
- Nothing more can be done
- Any other things, please tell us? [free text option]

Want to tell us more?

Finally, are you male or female?

- Male
- Female

How old are you?

- 13
- 14
- 15
- 16
- 17
- 18

Message on completed page

Thank you for completing our survey!

If you wish to provide us with more information about your experiences, or have an idea of what we can do to promote cyber-safety and reduce cyber-bullying, please send an email to cybersafety@aph.gov.au. For more information about the inquiry please visit aph.gov.au/cybersafety.

If you ever feel unsafe online, or need help with cyber-bullying logon to <http://cybersmart.gov.au/report.aspx> to get help or report what you have seen.



Appendix E – Online Offences

Table Online Offences (I): Sexual offences committed online against minors

OFFENCE		JURISDICTIONS								
Type	Elements	Cth ¹	ACT ²	NSW ³	NT ⁴	Qld ⁵	SA ⁶	Tas ⁷	Vic ⁸	WA ⁹

¹ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act 1995 (Cth)*

² Unless otherwise noted, offence provisions in this column are located in the *Crimes Act 1900 (ACT)*

³ Unless otherwise noted, offence provisions in this column are located in the *Crimes Act 1900 (NSW)*

⁴ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act (NT)*

⁵ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act 1899 (Qld)*

⁶ Unless otherwise noted, offence provisions in this column are located in the *Criminal Law Consolidation Act 1935 (SA)*

⁷ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act 1924 (Tas)*

OFFENCE		JURISDICTIONS								
Type	Elements	Cth ¹	ACT ²	NSW ³	NT ⁴	Qld ⁵	SA ⁶	Tas ⁷	Vic ⁸	WA ⁹
Grooming	<i>Citation</i>	s474.27	See 'depravity'	s66EB(3)			s63B(3)	s125D		
	<i>Age limits</i>	Victim must be under 16		Perpetrator must over 18; victim under 16			Victim must be under 16	Victim must be (or believed to be) under 17		
	<i>Definition</i>	Uses a carriage service to transmit a communication with the intention of making it easier to procure the recipient to engage in sexual activity with the sender or another person		Any conduct (including communicating by telephone or internet) that exposes a child to indecent material with the intention of making it easier to procure the child for unlawful sexual activity			Makes a communication with a prurient purpose and with the intention of making a child amenable to a sexual activity	Makes a communication by any means with the intention of procuring a person to engage in an unlawful sexual act		
	<i>Penalty¹⁰</i>	12 years		12 years (victim under 14); or 10 years			10 years (basic); 12 years (aggravated) ¹¹	21 years and/or fine		
Procuring	<i>Citation</i>	s474.26	See 'depravity'	s66EB(2)	s131	s218A	s63B(1)	s125C	s58	s204B
	<i>Age limits</i>	Victim must be (or believed to be) under 16, perpetrator over 18		Victim must be under 16, perpetrator over 18	Victim must be under 16	Victim must be (or believed to be) under 16, perpetrator over 18	Victim must be under 16	Victim must be under 17	Victim must be under 16, perpetrator over 18	Victim must be (or believed to be) under 16; perpetrator over 18

⁸ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act 1958 (Vic)*

⁹ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act Compilation Act 1913 (WA)*

¹⁰ References to 'years' indicate maximum possible term of imprisonment.

¹¹ Aggravating circumstances listed in *Criminal Law Consolidation Act 1935 (SA)* s5AA

OFFENCE		JURISDICTIONS								
Type	Elements	Cth ¹	ACT ²	NSW ³	NT ⁴	Qld ⁵	SA ⁶	Tas ⁷	Vic ⁸	WA ⁹
	<i>Definition</i>	Uses a carriage service to transmit a communication to another person; with the intention of procuring the recipient to engage in sexual activity with the sender or another person		Intentionally procures for unlawful sexual activity with that or any other person	Attempts to procure to have sexual intercourse or commit, perform or engage in any act of gross indecency	Knowingly entice or recruit for the purposes of sexual exploitation	Incites or procures the commission of an indecent act; or, acting for a prurient purpose, causes or induces to expose any part of the body	Procures to have unlawful sexual intercourse or to commit an indecent act	Solicits or procures to take part in an act of sexual penetration, or an indecent act	Uses electronic communication with intent to procure a person to engage in sexual activity
	<i>Penalty</i>	15 years		15 years (child under 14) or 12 years	3 years; if perpetrator is an adult 5 years	10 years (victim under 12) or 5 years	10 years (basic); 12 years (aggravated)	21 years and/or fine	10 years	10 years (child under 13) or 5 years
Child abuse material ¹²	<i>Citation</i>	ss474.19 – 474.23	s64; s64A	s91H	s125B	s228C	s63; s63C	s130B	s57A	s60 ¹³
	<i>Age limits</i>	Person depicted is or appears to be under 18 ¹⁴	Person depicted under 18	Person depicted under 16	Person depicted is or appears to be under 18	Person depicted is or appears to be under 16	Person depicted is or appears to be under 16	Person depicted is or appears to be under 18	Person depicted is or appears to be under 18	Person depicted is or appears to be under 16

¹² Offences relating to the production or possession of child abuse materials/ pornography have been omitted

¹³ *Classification (Publications, Films and Computer Games) Enforcement Act 1996 (IVA)*

¹⁴ Attorney-General's consent needed to commence proceedings against an individual aged under 18 at the time of the offence

OFFENCE		JURISDICTIONS								
Type	Elements	Cth ¹	ACT ²	NSW ³	NT ⁴	Qld ⁵	SA ⁶	Tas ⁷	Vic ⁸	WA ⁹
	<i>Definition</i>	Transmits or supplies child pornography or child abuse material. Must intend to commit act, but need only be reckless as to whether material constitutes abuse material or pornography	Publishes, offers or sells child pornography	Disseminates child abuse material; includes sending, exhibiting, transmitting or communicating to another person	Distributes, sells or offers or advertises for distribution or sale child abuse material	Distributes child exploitation material; includes communicating, exhibiting, sending, supplying or transmitting to someone, whether to a particular person or not	Disseminates, or takes any steps in disseminating, child pornography knowing of its pornographic nature	Distributes, or does anything to facilitate the distribution of, child exploitation material; and knows, or ought to have known, that the material is child exploitation material	Knowingly uses an on-line information service to publish or transmit, or make available for transmission, objectionable material	Sells or supplies, or offers to sell or supply, or displays, exhibits or demonstrates, child pornography
	<i>Penalty</i>	15 years, 25 years if conduct repeated on 3 occasions and commission involves multiple offenders ¹⁵	1200 penalty units and/or 12 years	10 years	10 years	10 years	10 years basic, 12 years aggravated	21 years and/or fine	10 years	5 years for displaying/ exhibiting; 7 years for selling/ supplying; and/or fine of any amount
Indecency	<i>Citation</i>	474.27A	S66		S132	S218A		S125D(3)	S58 ¹⁶	S204B
	<i>Age limits</i>	Recipient must be (or believed to be) under 16; perpetrator must be over 18	Recipient must be under 16		Recipient must be under 16	Recipient must be (or believed to be) under 16		Recipient must be (or believed to be) under 17	Recipient must be under 18	Recipient must be (or believed to be) under 16, perpetrator over 18

¹⁵ Aggravated offence provisions were introduced to combat pornography/ child abuse material rings

¹⁶ *Classification (Publications, Films and Computer Games) Enforcement Act 1995 (Vic)*

Table Online Offences (II): Offences against the person committed online where age is not an element of the offence

NB These offences may be committed by an adult or a minor against any person, including another minor)

OFFENCE		JURISDICTIONS								
Type	Elements	Cth ¹⁷	ACT ¹⁸	NSW ¹⁹	NT ²⁰	Qld ²¹	SA ²²	Tas ²³	Vic ²⁴	WA ²⁵
Stalking	Citation		s35	s13 ²⁶	s189	Ch33A	s19AA		s21A	s338E(1)
	Definition		Specified conduct repeated on at least two occasions, which can include sending electronic messages to or about the stalked person. Must be intent to cause apprehension; or to	Stalks or intimidates another person with the intention of causing the other person to fear physical or mental harm	Specified conduct repeated on at least two occasions which can include telephoning, sending electronic messages to or otherwise contacting the stalked person.	One 'protracted' incident or multiple instances of specified conduct intentionally directed at a person; which can include any form of contact that would cause apprehension	Specified conduct repeated on at least two occasions, which can include publishing or transmitting offensive material to the person by electronic means; or	A course of conduct made up of one or more specified actions, which can include contacting the person by any means; publishing or transmitting offensive material by electronic	A course of conduct which can include contacting the victim by post, telephone, fax, text message, e-mail or other electronic communication; publishing on the Internet material	Pursues another person with intent to intimidate. ²⁷ Repeated communication can constitute pursuit

¹⁷ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act 1995 (Cth)*

¹⁸ Unless otherwise noted, offence provisions in this column are located in the *Crimes Act 1900 (ACT)*

¹⁹ Unless otherwise noted, offence provisions in this column are located in the *Crimes Act 1900 (NSW)*

²⁰ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act (NT)*

²¹ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act 1899 (Qld)*

²² Unless otherwise noted, offence provisions in this column are located in the *Criminal Law Consolidation Act 1935 (SA)*

²³ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act 1924 (Tas)*

²⁴ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act 1958 (Vic)*

²⁵ Unless otherwise noted, offence provisions in this column are located in the *Criminal Code Act Compilation Act 1913 (WA)*

²⁶ *Crimes (Domestic and Personal Violence) Act 2007 (NSW)*

²⁷ Alternative charge for 'pursues another person in a manner that could reasonably be expected to intimidate, and that does in fact intimidate, that person or a third person' carries maximum 12 year sentence or \$12,000 fine (*Criminal Code Act Compilation Act 1913 (WA) s338E(2)*)

OFFENCE		JURISDICTIONS								
Type	Elements	Cth ¹⁷	ACT ¹⁸	NSW ¹⁹	NT ²⁰	Qld ²¹	SA ²²	Tas ²³	Vic ²⁴	WA ²⁵
			harm/ harass		Must intend to cause physical or mental harm; or arouse fear or apprehension	or fear, or detriment (reasonably arising in all the circumstances)	communicating with or about the other person by way of the internet in a manner that could reasonably be expected to arouse apprehension or fear. Must intend to cause serious physical or mental harm ; or serious apprehension or fear	means; or using the internet or any other form of electronic communication in a way that could reasonably be expected to cause apprehension or fear. Must intend to cause physical or mental harm; or arouse apprehension or fear	relating to or purporting to originate from the victim; and tracing the victim's use of the Internet. Must intend to cause physical or mental harm; or arouse apprehension or fear	
	<i>Penalty</i>		2 years (5 years if contravene injunction)	5 years and/ or fifty penalty units	2 years (5 years if involves weapon or contravening injunction)	5 years (7 years if contravene injunction)	3 years (basic), 5 years (aggravated)	21 years and/or fine	10 years	3 years (basic), 8 years (aggravated)
Bullying	<i>Citation</i>			S60E						
	<i>Definition</i>			Assaults, stalks, harasses or intimidates a school student or member of staff while victim is attending a school						
	<i>Penalty</i>			5 years						
Assault/ threats	<i>Citation</i>	s474.15	s26	s61	s188	s335	s20	Words alone cannot constitute an assault (s182)	s31	s338A
	<i>Definition</i>	Uses a carriage service to make a threat to kill or cause serious harm to the second person or a third person, intending	(Common law)	(Common law)	(Common law)	(Common law)	Threatens to apply force to the victim ; and there are reasonable grounds for the victim to believe that the		Threatens direct or indirect application of force to the victim with intent to commit assault	Makes a threat to cause detriment of any kind to any person, with intent to

OFFENCE		JURISDICTIONS								
Type	Elements	Cth ¹⁷	ACT ¹⁸	NSW ¹⁹	NT ²⁰	Qld ²¹	SA ²²	Tas ²³	Vic ²⁴	WA ²⁵
		the second person to fear that the threat will be carried out					person is in a position to carry out the threat and intends to do so; or there is a real possibility that the person will carry out the threat			cause a detriment ²⁸
	<i>Penalty</i>	10 years for threat to kill, 7 years for threat to cause serious harm	2 years	2 years	1 year, 5 years if male to female or adult to person under 16	3 years	2 years		5 years	7 years (10 years if threaten to kill)
Harassment ²⁹	<i>Citation</i>	s474.17								
	<i>Definition</i>	Uses a carriage service in a way (whether by the method of use or the content of a communication) that reasonable persons would regard as being menacing, harassing or offensive	Harassment in certain circumstances is unlawful, but not a criminal offence, under the <i>Discrimination Act 1991 (ACT)</i> (see s71)	Sexual harassment in certain circumstances is unlawful, but not an offence, under the <i>Anti-Discrimination Act 1977 (NSW)</i> (s22B)	Harassment in certain circumstances is prohibited, but not a criminal offence, under the <i>Anti-Discrimination Act (NT)</i> s22	Sexual harassment in certain circumstances contravenes but does not give rise to criminal sanctions under the <i>Anti-Discrimination Act 1991 (Qld)</i>	Sexual harassment in certain circumstances contravenes but does not give rise to criminal sanctions under the <i>Equal Opportunity Act 1984 (SA)</i> (see s99)	Harassment in certain circumstances is prohibited, but not a criminal offence, under the <i>Anti-Discrimination Act 1998 (Tas)</i>	Sexual harassment in certain circumstances contravenes but does not give rise to criminal sanctions under the <i>Equal Opportunity Act 1995 (Vic)</i> (see s209)	Sexual and racial harassment in certain circumstances contravenes but does not give rise to criminal sanctions under the

²⁸ Alternative charge for 'person who makes a threat to unlawfully cause detriment' carries maximum 3 year sentence, or 6 years if the conduct was racially motivated (*Criminal Code Act Compilation Act 1913 (WA)* s338B(b))

²⁹ Note that stalking laws may apply to online harassment

OFFENCE		JURISDICTIONS								
Type	Elements	Cth ¹⁷	ACT ¹⁸	NSW ¹⁹	NT ²⁰	Qld ²¹	SA ²²	Tas ²³	Vic ²⁴	WA ²⁵
	Penalty	3 years								<i>Equal Opportunity Act 1984 (WA) (see s154)</i>
Vilification	Citation		s67 ³⁰	s20D; s38T; s49ZTA; s49ZXC ³¹		s131A ³²	s4 ³³		s24; s25 ³⁴	s77; s78 ³⁵
	Definition	The Racial Discrimination Act (Cth) makes certain conduct unlawful; but excludes criminal liability for unlawful conduct under the statute (with limited exceptions unrelated to online conduct) (see s26)	By a public act incite hatred, serious contempt or severe ridicule on the ground of race, sexuality, gender identity, or HIV/AIDS status	By a public act incite hatred, serious contempt or severe ridicule on the ground of race, transgender identity, HIV/AIDS status, or homosexuality		By a public act, knowingly or recklessly incite hatred, serious contempt or severe ridicule on the ground of the race, religion, sexuality or gender identity in a way that includes threatening or inciting physical harm	By a public act incite hatred, serious contempt or severe ridicule on the ground of race	Inciting hatred by a public act against specific groups is prohibited, but does not attract criminal sanctions, under the Anti-Discrimination Act 1998 (Tas) (s 19)	Intentionally engage in conduct on the grounds of race (including use of the internet or email) that the offender knows is likely to incite hatred, serious contempt or revulsion; or threaten, or incite others to threaten, physical harm	Engages in any conduct, otherwise than in private, by which the person intends to create, promote or increase animosity towards, or harassment of, a racial group; or that is likely to

³⁰ *Discrimination Act 1991 (ACT)*

³¹ *Anti-Discrimination Act 1977 (NSW)*

³² *Anti-Discrimination Act 1991 (Qld)*

³³ *Racial Vilification Act 1996 (SA)*

³⁴ *Racial and Religious Tolerance Act 2001 (Vic)*

³⁵ *Equal Opportunity Act 1984 (WA)*

