
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 Committeexx

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



Membership of the Committee

Chair Senator Dana Wortley

Deputy Chair Mr Alex Hawke MP

Members Mr Ed Husic MP

Senator Guy Barnett

Mr Paul Fletcher MP (to 28 March 2011)

Senator David Bushby

Ms Nola Marino MP (from 28 March 2011)

Senator Scott Ludlam

Mr Graham Perrett MP

Senator Louise Pratt

Ms Amanda Rishworth MP

Mr Tony Zappia MP

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.

