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

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

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

Cover image courtesy of Thinkstock

Contents

APPENDICES

LIST OF TABLES

LIST OF FIGURES

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 Luschtinetz
	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 Minster 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.