15

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]

[24] NSW Secondary Principals’ Council, *Submission 32*, p. 2