Australian Government

Government Statement of Response

Joint Select Committee on Cyber-Safety
Interim Report
High-Wire Act: Cyber-safety and the Young

December 2011

Government Statement of Response

This statement is the Government's response to the Joint Select Committee on Cyber-Safety's interim report *High-Wire Act: Cybersafety and the Young.*

Introduction

The Australian Parliament established the Joint Select Committee on Cyber-Safety (JSCC) in early 2010 as a part of the Government's commitment to investigate and improve cybersafety measures.

The Committee's inquiry is based on the Terms of Reference finalised in November 2010. In summary, these require that the JSCC inquire and report on:

- the online environment in which Australian children currently engage
- cybersafety risks, such as exposure to illegal content and breaches of privacy
- responses to current cybersafety risks, such as regulation and enforcement
- opportunity for cooperation between stakeholders dealing in cybersafety issues
- examining how new technologies may present opportunities and economic benefits
- ways to support schools in dealing with cyberbullying incidents
- analysing information on world's best practice safeguards
- the merit of establishing an Online Ombudsman
- other matters on cybersafety referred by the Minister for Broadband, Communications and the Digital Economy or either House of Parliament.

The JSCC undertook a range of consultation activities in order to investigate these Terms of Reference, including roundtable discussions, public hearings, school forums and online surveys. The committee tabled an interim report *High-Wire Act: Cybersafety and the Young* on 20 June 2011 containing thirty two recommendations.

Key messages of the report

The *High-Wire Act* report provides an overview of current cybersafety concerns, such as defining the 'online environment' and the concept of cybersafety. It outlines the roles of current stakeholders in the cybersafety field. The report also describes the Committee's concerns with educational strategies, law enforcement issues and cybersafety approaches undertaken by Australian and international governments, industry and non-government organisations.

The report's recommendations relate to options for improving the safety of the online environment. In particular, they reflect the key messages that were received through the consultation process: that better education, knowledge and skills would assist young people in participating online with confidence and a sense of control; that privacy in an online environment needs to be improved through tighter provisions; that research into emerging technologies and the interactions of young people online is required; and that parents, carers, teachers and all those who engage with young people need to gain an understanding of the online environment and its benefits and risks.

Addressing the issues raised in the report requires a multifaceted approach. Australian governments, schools, families and communities all have a responsibility to provide safe online environments and teach children how to use technology in positive and productive ways that will support 21st century learning and living, both in and out of school.

The Government understands there is a need for strengthening an understanding of cybersafety issues and promoting the safety of children online, and is actively pursuing measures to address these issues.

Government Cybersafety Initiatives

The Australian Government is committed to improving the cybersafety of Australian children and young people. The Government's Cybersafety Plan was established in May 2008 with funding of $125.8 million committed over four years to combat online risks and help parents and educators protect children from inappropriate material. Measures include increased funding towards cybersafety education and awareness raising activities, content filtering and law enforcement.

The Australian Government has also established a Consultative Working Group on Cybersafety (CWG) to bring together representatives from industry, the community and the government with a close involvement in cybersafety issues faced by children. The CWG's role is to provide advice to government to ensure properly-developed and targeted programs and policy initiatives are undertaken.

Examples of Australian Government cybersafety initiatives include:

- the Youth Advisory Group which provides advice to government on cybersafety issues from a young person's perspective
- the Teachers and Parents Advisory Group (TAP) that provides a forum where members can share ideas on how to protect children online and promote cybersafety messages
- the Cybersafety Help Button which provides internet users, particularly children and young people, with easy online access to cybersafety information and assistance available in Australia
- the development of an Easy Guide to Socialising Online which provides information and step by step instructions about how to use the safety features of popular social networking sites, search engines and online games
- the Cybersmart website which provides a single access point for cybersafety advice across a range of target audiences
- the Cybersmart Outreach program which provides free Professional Development programs for teachers in schools and universities focusing on teaching students to have safe and positive online experiences
- funding for the Alannah and Madeline Foundation to conduct a national pilot of an approach to cybersafety for Australian schools (eSmart)

- the revised and nationally endorsed National Safe Schools Framework to assist in creating learning environments that are free from bullying and harassment
- the Bullying. No Way! website that provides information for parents, students and teachers on strategies to address bullying, harassment and violence
- the Think U Know Internet safety program that delivers interactive training to parents, carers and teachers through primary and secondary schools across Australia using a network of accredited trainers
- $2.3 million for ongoing research into the changing digital environment to identify issues and target future policy and funding. A key component of this ongoing work is surveying the changes in levels of cybersafety awareness and behaviour.

The Government is also looking at building upon its current cybersafety initiatives to address serious issues which arise when engaging online. This includes mechanisms to strengthen the existing co-operative arrangements with social networking sites.

The responses to the recommendations take into account existing government activities on cybersafety and cybersecurity issues and are provided in the context of the inquiries on related issues such as the House of Representatives' Standing Committee on Communications report *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*.

The responses also reflect the Governments announcement that it will develop a Cyber White Paper. In developing the White Paper the government will examine the full spectrum of cyber issues such as better coordination of awareness raising activities, development of skills, more centralised reporting of cyber incidents and a more coherent approach to cyber education. Public consultation for the Paper commenced mid-September 2011, and many of the topics that will be explored in this consultation are relevant to the Committee's recommendations.

Government Response on Individual Recommendations of the Report

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.

Government Response

The Australian Government accepts this recommendation in principle, pending the outcomes of the Cyber White Paper process which will conclude in mid-2012.

The Australian Government through the Department of Education, Employment and Workplace Relations (DEEWR), will write to the Directors General and Chief Executive Officers of the education authorities to refresh awareness and encourage take-up of all Australian Communications and Media Authority (ACMA) programs, including Cybersmart for Young Kids.

The Government supports the ACMA's Cybersmart for Young Kids program. This is an ideal program for the Australian Government and education authorities to support and expand access to preschools and kindergartens.

In addition, the Government has provided $3 million to the Alannah and Madeline Foundation for a national pilot of its eSmart cybersafety initiative which addresses cyberbullying in schools. The Victorian Government has announced the eSmart program will be rolled out in Victorian schools and the Queensland Government has also announced that the eSmart program will be rolled out to all its state government schools.

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.

Government Response

The Australian Government accepts this recommendation.

The Safe and Supportive School Communities (SSSC) is a Working Group of the Australian Education, Early Childhood Development & Youth Senior Officials Committee (AEEYSOC). The Working Group includes nominated representatives of all Australian education jurisdictions - all state, territory and federal education departments as well as national Catholic and independent schooling representatives.

The SSSC working group has developed the following definition of cyberbullying:

> "Bullying is repeated verbal, physical, social or psychological behaviour that is harmful and involves the misuse of power by an individual or group towards one or more persons. Cyberbullying refers to bullying through information and communication technologies."

The Department of Broadband, Communications and the Digital Economy (DBCDE) has invited the Consultative Working Group on Cybersafety (CWG), the Youth Advisory Group (YAG) and the Teachers and Parents Advisory Group (TAP) on cybersafety to provide comment on this definition. CWG comments will be forwarded to the SSSC for further consideration.

The definition will be discussed and agreed by state and territory governments through AEEYSOC.

The definition of cyberbullying agreed through these consultation processes will be promoted nationally via government programs and resources such as the Cybersafety Help Button the Easy Guide to Socialising Online and the Cybersmart website.

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.

Government Response for Recommendations 3 and 28

The Australian Government accepts these recommendations in principle pending the outcomes of the Cyber White Paper process which will conclude in mid-2012.

The ACMA piloted a Cybersmart student mentoring program in March this year. Students were trained and then guided to develop and deliver their own presentations and workshops building on content from the Outreach program's internet safety awareness presentations. The pilot program was well received.

DEEWR will seek AEEYSOC agreement that education authorities work with the ACMA to investigate the feasibility of expanding the ACMA student mentoring pilot.

The Government notes that ultimately the implementation of any student mentoring programs is a matter for state and territory, independent and non-government education authorities.

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.

Government Response

The Australian Government notes this recommendation. The Australian Law Reform Commission Report (ALRC) 108, *For Your Information: Australian Privacy Law and Practice* (R39-1 at page 1358 – Volume 2) recommended that the Act be amended to remove the small business exemption.

The Government will take the Committee’s recommendation into account when it is considering the ALRC’s recommendation to remove the small business exemption.

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).

Government Response

The Australian Government notes this recommendation. The Government will consider this recommendation in conjunction with its deliberations on recommendation 4 above.

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.

Government Response

The Australian Government supports this recommendation in principle. The Government agrees that guidelines would be useful and notes that it has previously supported the ALRC recommendation 19 – 1 (i.e. develop and publish further guidance about what is required of agencies and organisation to obtain an individual's consent under the *Privacy Act 1988*) as part of its stage one response.

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.

Government Response

The Australian Government notes this recommendation and will consider this recommendation in conjunction with its deliberations on recommendations 4 and 5 above.

Further, the draft Australian Privacy Principle (APP) 8 will provide a framework for the regulation of cross-border disclosures of personal information. Before a cross-border disclosure can occur, the draft APP 8 imposes minimum obligations on an organisation to take such steps as are reasonable in the circumstances (for example, by imposing contractual obligations) to ensure that the overseas recipient does not breach the draft APPs.

In addition, an organisation will remain accountable for the acts and practices of the overseas recipient, unless an exemption applies.

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.

Government Response

The Australian Government notes this recommendation. As part of its stage one response to the ALRC recommendations, the Government has announced that it supports the development of binding and mandatory codes.   It will be a matter for the Commissioner to consider whether a code is necessary.

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).

Government Response

The Australian Government notes this recommendation. The Government will consider this aspect as part of the stage one response to the ALRC recommendations currently being undertaken.

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.

Government Response

The Australian Government notes this recommendation. The Government will consider this aspect as part of the stage one response to the ALRC recommendations currently being undertaken.

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.

Government Response

The Australian Government notes this recommendation. The Government will consider this as part of the stage one response to the ALRC recommendations currently being undertaken.

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.

Government Response

The Australian Government accepts this recommendation. The Government has been and will be continuing to work with appropriate international bodies including in particular regional bodies to further privacy protections.

The Government actively participates in the work of the Organisation for Economic Cooperation and Development (OECD) and Asian Pacific Economic Council (APEC) on international privacy issues. Australia has played a leading role in the development of the APEC Cross-Border Enforcement Arrangement (CPEA), which allows participating privacy regulators to share information and provide assistance in relation to privacy matters that have a cross-border aspect. The APEC CPEA commenced in July 2010 and the privacy regulators of Australia, Canada, New Zealand, Hong Kong China, and the United States are currently participants.

The Office of the Australian Information Commissioner (OAIC) continues to foster strong ties with other privacy authorities in the region via the Asia Pacific Privacy Authorities group.

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.

Government Response

The Australian Government accepts this recommendation in principle.

The Government notes that state and territory government and non-government education authorities currently bear legal responsibility for the duty of care of their students. This includes ensuring that appropriate measures are in place so that students can learn in a safe and supportive school environment, and in some instances this responsibility may extend beyond school hours.

DEEWR will investigate the feasibility of this recommendation further with state and territory education authorities.

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.

Government Response

The Australian Government accepts this recommendation, pending the outcomes of the Cyber White Paper process which will conclude in mid-2012.

The Government, through DEEWR, will consult with the AEEYSOC to seek agreement to address these issues, by building on work underway through the National Safe Schools Framework and agreeing to promulgate key cybersafety messaging through existing and expanded ACMA and Australian Federal Police (AFP) activities.

The SSSC working group promotes key messaging through activities of the annual National Day of Action Against Bullying and Violence and is working directly with the ACMA to include cybersafety as a key element of these activities.

The Government notes that in regards to Information and Communication Technology (ICT) policies the state and territory education authorities have primary responsibility for decisions about design, purchase, distribution and the use of educational hardware and software to meet the specific needs of their schools.

In regard to Acceptable Use Agreements, the National Safe Schools Framework articulates the importance of safety and wellbeing policies and procedures and states that “a responsible technology usage agreement should be in place” in all schools.

The Government will continue to promote cybersafety resources and assistance through the Cybersafety Help Button. The Help Button provides internet users with a ‘one-stop shop’ for access to cybersafety information and advice. It offers counselling, reporting and educational resources to assist children deal with online risks including cyberbullying, unwanted contact, scams and fraud, and offensive or inappropriate material.

Since the Cybersmart portal’s launch in June 2009 the School Gateway area of the site has received more than 600,000 views. Since May 2011 there have been 7,000 downloads of Cybersmart teaching resources. The portal links to other cybersafety resources such as ThinkUKnow, the Help Button, Stay Smart Online and relevant state and territory policies.

The Ministerial Council for Education, Early Childhood Development and Youth Affairs funded Bullying. No Way! Website is being refreshed to provide key messaging, current information and best practice resources. The rebuilt Bullying. No Way! website will be officially launched on the National Day of Action Against Bullying and Violence on 16 March 2012.

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.

Government Response

The Australian Government supports this proposal in principle, but it will need to be considered against competing priorities in the budget context.

The ACMA’s online professional development program, Connect.*ed*, was designed in consultation with cybersafety experts, teachers and students to specifically meet the needs of practising teachers. Connect.*ed* currently consists of four modules that guide teachers in how to integrate an effective cybersafety process and policy into their school.

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.

Government Response

The Australian Government accepts this recommendation in principle, pending the outcomes of the Cyber White Paper process.

The Government supports the recommendation that Ministers continue to work together to ensure professional development training for teachers is made widely available in the face of growing demand and interest. The Government notes significant funding was provided in the 2008-09 Budget and in December 2009 for expanded outreach activities.

Under the Government's Outreach program, the ACMA offers a range of programs to meet the professional development needs of Australian teachers including the Professional Development for Educators face-to-face workshops, online professional development program Connect.*ed* and internet safety presentations. The programs are available for all teachers across Australia and count towards professional development accreditation.

Since the Outreach program's inception in January 2009, over 45,000 teachers have already attended a professional development workshop or presentation with a further 2,800 teachers having registered to do Connect.*ed.*

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.

Government Response

The Australian Government accepts this recommendation in principle, pending the outcomes of the Cyber White Paper process.

While the Australian Government funds Australian universities, they are autonomous institutions and are able to make decisions on pre-service teacher training course content to suit their own individual needs and industry requirements.

Guidance on course content and graduate outcomes will be articulated through the National Professional Standards for Teachers, a key facilitation reform under the Smarter Schools - Improving Teacher Quality National Partnership. It will include the expectation that graduate teachers will be able to "use ICT safely, responsibly and ethically" (Standards 4.5) in both learning and teaching.

The ACMA is currently delivering a teacher training course across Australian universities on Cybersafety. Thirty-three of the 45 universities with a dedicated faculty or school of education have registered or completed the ACMA's program since it was launched in June last year.

The ACMA has worked closely with universities to raise awareness of the importance of incorporating cybersafety in their teacher training courses. The ACMA's Pre Service Teacher program which consists of a lecture and tutorial for final year student teachers has been well received by universities across Australia. Consideration could be given to expanding this program to include first, second and third year students as well as the Vocational Education and Training and Technical and Further Education sectors.

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.

Government Response

The Australian Government accepts this recommendation in principle.

The ACMA provides advice to teachers on this issue through its Cybersmart program. With the increase of teachers reporting to Outreach trainers that they have been cyberbullied by students, the ACMA in 2010 incorporated a component on this issue in its Outreach presentations and the Cybersmart portal. The Cybersmart program focuses on equipping teachers with the skills and knowledge to help students stay safe online.

The Government is working with states and territories through the Safe and Supportive Schools Community to improve accessibility to resources for teachers that will be provided via the Bullying. No Way! website rebuild.

The Government notes that school principals are responsible for the wellbeing of the whole school community and for ensuring that all members of that community, including teaching staff, are safe, supported and respected.

The implementation of policies such as the ‘reputation management’ model is a matter for state and territory governments.

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.

Government Response

The Australian Government supports this proposal in principle, but it will need to be considered against competing priorities in the budget context and the outcomes of the Cyber White Paper process.

The Government currently funds several multi-platform training programs for teachers and students that addresses bullying and cyberbullying.

As articulated in the response to Recommendation 17, the National Professional Standards for Teachers includes the expectation that teachers will develop and employ practical strategies to promote the safe, responsible and ethical use of ICT in learning and teaching.

Teachers will be able to use the range of support materials currently being developed by the Australian Institute for Teaching and School Leadership alongside resources from agencies such as the ACMA to develop student awareness and understanding of appropriate ICT practice.

In addition, the ACMA’s current Connect.*ed* program provides teachers with information and guidance on a broad range of cybersafety issues, such as cyberbullying, sexting, privacy and digital reputation, and offers effective strategies and resources to assist in keeping students safe when they go online. Connect.*ed* is accredited or endorsed by State and Territory Education Departments and counts towards continuing professional development for teachers.

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.

Government Response

The Australian Government accepts this recommendation, pending the outcomes of the Cyber White Paper process.

Australian communities have a responsibility to provide safe online environments and teach children how to use technology in positive and productive ways.

The Government is currently working collaboratively with education authorities through the SSSC Working Group to ensure schools are learning environments where every student and school community member is safe, supported, respected and valued.

The National Safe Schools Framework is the nationally endorsed key safe school policy document that all schools are encouraged to adopt with a “whole of school” approach and commitment. The Frameworks resource manual includes a school audit tool which helps schools to objectively assess the effectiveness of existing safe school policies and to identify and address any gaps.

In the Australian Curriculum students will develop understandings about cybersafety through the ICT competence general capability which will have students learn to apply appropriate social and ethical protocols and practices to operate and manage ICT when investigating, creating and communicating ideas and information at school, at home, at work and in their communities.

This will be reinforced through the teaching of ICT as a key aspect of the *Australian Curriculum: Technologies* learning area.

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.

Government Response

The Government accepts this recommendation in principle, pending the outcomes of the Cyber White Paper process.

The Government agrees that it is essential for Australian Police Forces to receive appropriate training to effectively investigate online crimes and deal with cyber-safety issues. A range of work is currently underway to address the need for appropriate training, including through the National Cyber Crime Working Group (NCWG), which was established by the Standing Committee of Attorneys-General (SCAG) in May 2010. The NCWG is comprised of representatives from police and justice agencies in each jurisdiction, the Australia New Zealand Policing Advisory Agency (ANZPAA), the Australian Crime Commission and CrimTrac.

The NCWG noted the work of ANZPAA in developing the following products:

- an online training calendar for specialist technology investigators
- education and training guidelines for technology crime investigators and digital evidence practitioners.

The NCWG is also working with ANZPAA to undertake a scoping study to assess law enforcement capabilities across jurisdictions in relation to cyber crime for consideration by Police Ministers.

In addition, the AFP conducts Technology Enabled Crime Awareness Training, which is mandatory for all AFP staff. The training program aims to give staff a greater awareness of the concept of technology enabled crime, the impact it has on law enforcement, and how members can more efficiently and effectively investigate such crimes. The AFP also runs a more advanced training program for e-crime investigators that provides participants with the ability to extract sound forensic digital evidence.

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.

Government Response

The Government accepts this recommendation in principle, but notes that it is not possible for the executive Government to specify mandatory training for judicial officers.

The AFP runs an education and awareness program for the legal fraternity. Workshops have been run with Victorian judges and barristers of the NSW Bar. A workshop for NSW Supreme Court judges is scheduled for late September. The AFP's High Tech Crime Operations works closely with the Judicial Colleges in each jurisdiction when designing and delivering these workshops.

The AFP has also commissioned the building of an eCourt facility at the AFP's Canberra Headquarters. The eCourt is designed to place the AFP at the forefront of electronic evidence presentation and provide the legal fraternity with the tools and education they need to address the challenges of complex electronic evidence. It is due to become operational in September 2011.

The NCWG is also considering existing arrangements for judicial and legal practitioner training throughout Australia, to determine whether a national or State-based approach is preferred and consider the need for guidelines in this area.

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.

Government Response

The Government accepts this recommendation in principle.

The Government recognises the importance of effective and comprehensive offences relating to online criminal activity, including conduct directed at children.

The Government will refer this recommendation to the NCWG for its consideration of whether any review of relevant legislation in Australian jurisdictions is necessary.

The Commonwealth has enacted comprehensive legislation to protect children from online sexual exploitation. The Criminal Code sets out a range of offences directed at use of a carriage service, such as the internet, for child pornography material, using a carriage service to procure a child for sexual purposes or using a carriage service to 'groom' a child for sexual activity.

In 2010, the Commonwealth Parliament passed the *Crimes Legislation Amendment (Sexual Offences Against Children) Act*, which extended the coverage of child pornography offences, improved the operation of the grooming and procuring offences, introduced new offences for using a carriage service for indecent communications with a child or for sexual activity with a child. The Act also introduced a new aggravated offence directed at a child pornography network. These amendments ensure that Commonwealth offences reflect contemporary offending and that internet-related child sexual exploitation is comprehensively covered in light of rapidly changing technologies and the anonymity that the Internet provides. These reforms followed a comprehensive review of Commonwealth child sexual exploitation legislation.

The Criminal Code also criminalises the use of a carriage service to make threats, or to menace, harass or cause offence. These offences target the kind of behaviour that underlies serious cases of cyber bullying and cyber stalking. In 2010, the NCWG considered whether new nationally consistent offences were necessary to combat this kind of conduct. It was agreed that that existing offences are adequate and no further work is currently required on a national basis.

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.

Government Response

The Government accepts this recommendation in principle, pending the outcomes of the Cyber White Paper process.

The Government notes that it currently provides a number of targeted self assessment tools on the ACMA's Cybersmart portal.

At present the Cybersmart program has a number of self-assessment tools developed for parents, teachers and students. For example:

- the students' technology audit on the Schools' Gateway
- "How Cybersmart am I" quiz on Cybersmart kids and teens pages
- "Your child's online safety" quiz for parents.

The ACMA will continue to monitor the take-up and responses to these tools and update these as appropriate.

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.

Government Response

The Government accepts this recommendation in principle, pending the outcomes of the Cyber White Paper process.

The CWG is working closely with the Government to consider options for providing information to parents at the point of sale of computers and mobile phones.

The Australian Mobile Telecommunications Association (AMTA), a member of the CWG, is working with DBCDE to investigate the provision of information about cybersafety resources, e.g. the Cybersafety Help Button, at the point of sale for mobile devices. AMTA will also investigate the possibility of pre-loading cybersafety material on mobile devices.

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.

Government Response

The Government accepts this recommendation in principle.

The Government has provided financial assistance over three years to Lifeline to increase the capacity of the organisation to respond to more calls and to support free calls from mobiles. As of 1 July 2011, mobile phone calls to Lifeline from anywhere in Australia are also available free of charge under an agreement with Telstra, Optus and Vodafone Hutchison Australia.

Kids Helpline provides a free online counselling service for young people aged between five and twenty five. The Helpline is promoted through a number of channels, including the ACMA's Cybersmart initiative, and it is a prominent feature in the Cybersafety Help Button. Kids Helpline is a service provided by Boystown.

The Government will continue to work with AMTA and the Communications Alliance on the issue of accessibility to crisis help lines.

The Government also notes that during 2010 and 2011 the ACMA has been examining a wide range of issues related to the regulatory framework for telephone numbers including the cost of calls from mobile phones to freephone (180) and local rate (13/1300) numbers which many organisations use to provide crisis help and to provide other key community services.

The ACMA is currently considering responses to the numbering work program and is expected to release a directions paper in late 2011 that examines changes needed to improve the efficiency and effectiveness of the numbering arrangements, including the issue of how calls from mobile phones to freephone and local rate numbers are charged.

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.

Government Response

The Government supports this recommendation in principle, pending the outcomes of the Cyber White Paper process.

The CWG and the YAG were established in 2009 as part of the Government’s Cybersafety Plan. The CWG and the YAG have provided advice to Government on a range of cybersafety issues and informed key initiatives including the Cybersafety Help Button, the TAP and the Easy Guide to Socialising Online.

DBCDE will continue to facilitate consultation with these groups to enhance the effectiveness of cybersafety campaigns and 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.

Government Response

The Australian Government accepts this recommendation in principle, pending the outcomes of the Cyber White Paper process. Please see response to Recommendation 3.

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.

Government Response

The Government accepts this Recommendation in principle, pending the outcomes of the Cyber White Paper process.

The Cybersafety Help Button provides internet users, particularly children and young people, with a 'one-stop shop' for access to counselling, reporting and educational resources to assist children deal with online risks including cyberbullying, unwanted contact, scams and fraud, and offensive or inappropriate material. The Cybersafety Help Button is available from the DBCDE website (*www.dbcde.gov.au/helpbutton*), and promoted through the ACMA's Cybersmart website and many other sites.

The Cybersafety Help Button is expanding to include a new section called *Cybersafety Resources* which contains a comprehensive range of cybersafety information, educational programs, research and events. The expanded Cybersafety Help Button will be promoted widely through organisations represented on the CWG member organisations, and education networks.

The ACMA's Cybersmart website is a key source of cybersafety advice and information for teachers, parents, librarians and students of all ages, from kindergarten through to university.

As well as its own substantial body of resources, this web portal links to other cybersafety program providers such as ThinkUKnow, Stay Smart Online, the Cybersafety Help Button, and state school cybersafety websites and resources. It also links to the Kids Helpline for online counselling advice. The portal has seen large volumes of traffic with more than 1,138,050 visits to date.

Promotion of the portal is a primary consideration for the ACMA and it will continue to explore mechanisms for expanding its reach to difficult-to-reach audiences, such as young people and people with disabilities.

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.

Government Response

The Government accepts this recommendation in principle.

DBCDE is working with the CWG and a number of social networking sites to assist in developing mechanisms to streamline complaints processes and their resolution.

The Cybersafety Help Button and the Easy Guide to Socialising Online are two government projects that have been developed specifically to improve accessibility to reporting abuse and complaints assistance mechanisms for social networking sites. A significant number of social networking sites (and online game sites) participate in the Cybersafety Help Button initiative and Easy Guide to Socialising Online initiative.

The Internet Industry Association (IIA) has been consulted on this Recommendation. The IIA and its members indicated that they are committed to ensuring that users of social networking sites should have an understanding of acceptable behaviour, as well as access to visible and effective complaints handling mechanisms. They have also offered to work with industry, in particular social networking sites, to develop recommendations and best practice guidelines for the lodgement and resolution of user complaints.

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.

Government Response

The Government accepts this recommendation in principle.

The issue of establishing a protocol with overseas social networking sites is currently being pursued through the CWG, of which leading social network sites are members.

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.

Government Response

The Government accepts this recommendation in principle.

The Government will work with service providers and the States and Territories to reduce costs for law enforcement agencies in collecting evidence against online offenders.

Under the *Telecommunications Act 1997* (Cth), agencies must compensate service providers on a no profit/no loss basis for help given by service providers.

List of Abbreviations

APEC	Asian Pacific Economic Council
ANZPAA	Australia New Zealand Policing Advisory Agency
ACMA	Australian Communications and Media Authority
AEEYSOC	Australian Education, Early Childhood Development & Youth Senior Officials Committee
AFP	Australian Federal Police
ALRC	Australian Law Reform Commission Report
AMTA	Australian Mobile Telecommunications Association
APP	Australian Privacy Principle
CWG	Consultative Working Group on Cybersafety
CPEA	Cross-Border Enforcement Arrangement
DBCDE	Department of Broadband, Communications and the Digital Economy
DEEWR	Department of Education, Employment and Workplace Relations
ICT	Information and Communications Technologies
IIA	Internet Industry Association
JSCC	Joint Select Committee on Cyber-Safety
NCWG	National Cyber Crime Working Group
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Cooperation and Development
SSSC	Safe and Supportive School Communities
SCAG	Standing Committee of Attorneys-General
TAP	Teachers and Parents Advisory Group