11

Legislative basis

Australian law and the online environment

11.1 Responsibility for combating crime in the online environment is shared between the Commonwealth, the States and the Territories. The Commonwealth has responsibility for matters across or outside Australian jurisdictions, while the States and Territories generally have domestic responsibilities.

11.2 Appendix E contains additional information on other relevant laws of each State and Territory and those of the Commonwealth.

Australian Government responsibilities

Attorney-General's Department

11.3 In May 2010, the Standing Committee of Commonwealth and State/Territory Attorneys-General agreed to establish a National Cyber-Crime Working Group to enable jurisdictions to work cooperatively to combat cyber-crime. Since its first meeting in July 2010, the National Cyber-Crime Working Group has conducted a scoping study of existing mechanisms for reporting online crime. It has also prepared a discussion paper on options to improve current reporting arrangements, including the creation of a centralised online reporting facility. Setting up such a body will be the subject of a feasibility study.[1]

---

1 Attorney-General's Department: *Submission 58*, pp. 2-3.

11.4 This is an example of work being done to consolidate material, so that those in the online environment receive consistent messages delivered centrally about cyber-safety.[2]

11.5 During the 2010 National Cyber Security Awareness Week, the publication *Protecting Yourself Online – What Everyone Needs to Know* was launched. Over 120,000 copies of the book and 270,000 copies of the pamphlet have since been distributed. This material has been updated for National Cyber Security Awareness Week in 2011.[3]

11.6 The Attorney-General's Department has also produced *ID Theft – Protecting your Identity*. It provides practical strategies for Australians to protect themselves against becoming a victim of identity theft, and what to do if it happens. Since it was launched in 2009, over 60,000 copies have been distributed to individuals and police agencies for use in crime prevention. It is also used in training courses run by the private sector and by non-government organisations.[4]

11.7 On 30 April 2010, Australia announced its intention to accede to the Council of Europe *Convention on Cybercrime (2001)*. This is the only multilateral treaty in force that specifically addresses cyber-crime. Its main objective is to pursue a common criminal policy aimed at the protection of society against cyber-crime, through the adoption of appropriate legislation and fostering international cooperation.

11.8 The Convention requires participating countries to create offences for certain activities. It establishes procedures to make investigations more efficient, and promotes greater international cooperation using existing regimes, including mutual assistance and police-to-police assistance.

11.9 The Department noted that the *Criminal Code Act 1995* (Cth) already contains comprehensive offences dealing with the misuse of telecommunications, and cyber-crime. These offences were framed in 'technology-neutral' language to ensure that they would remain applicable as the online environment evolves. Thus, 'computer' was not defined so that offences would encompass such new developments as mobile phones with Internet access. Offences such as hacking into another person's Facebook account, altering it, or using malicious software to steal personal information, are also included.[5]

---

2 Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch, Attorney-General's Department, *Transcript of Evidence*, 24 March 2011, p. CS19.

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

4 Attorney-General's Department, *Submission* 58.1, p. 1.

5 Attorney-General's Department, *Submission 58*, p. 2.

11.10 Other offences criminalise the inappropriate use of telecommunications, including the Internet. These offences include using a 'carriage service' in the online environment to menace, harass or cause offence, threats to kill or cause harm to a person, or to use such a service for child pornography.[6]

11.11 Further amendments to Australian legislation are required to enable compliance with the Convention, including those which:

- clarify that domestic law enforcement agencies can apply for the preservation of stored communications information;
- enable the preservation of stored communications and associated telecommunications data at the request of foreign law enforcement agencies, and
- require confidentiality in relation to the preservation of, access to and disclosure of stored communications and telecommunications data.[7]

11.12 The Australian Federal Police (AFP) noted that the Convention provides benefits to law enforcement authorities, as it contains procedures to make investigations more efficient. It also provides systems to facilitate international co-operation, including:

- helping authorities from one country to collect data in another;
- empowering authorities to request the disclosure of specific computer data;
- allowing authorities to collect or record traffic data in real-time;
- establishing a 24 hour/seven days per week network to provide immediate help to investigators, and
- facilitating extradition and the exchange of information.[8]

11.13 However, the Convention cannot be seen as a quick solution to the difficult problem of international evidence and criminal intelligence sharing. The AFP commented that more work needs to be done on ensuring that international law enforcement has the ability to exchange evidence and intelligence in a timely fashion.[9] The capacity to collect evidence in Australia is arguably more limited than some other jurisdictions.[10]

---

6 Attorney-General's Department, *Submission 58*, p. 2.

7 Attorney-General's Department, *Submission 58*, p. 9.

8 Australian Federal Police, *Submission 64*, p. 14.

9 Australian Federal Police, *Submission 64*, p. 14.

10 Mr Chris Watt, Federal Secretary, Independent Education Union of Australia, *Transcript of Evidence*, 30 June 2010, p. CS14.

Australian Federal Police

11.14 The AFP is a member of the Consultative Working Group on Cybersafety. It works closely with other law enforcement and government agencies, industry, non-government organisations, content service providers, banks, education agencies and community groups.

11.15 It has a number of roles in cyber-safety issues:

- to target and investigate technology crime including child pornography and paedophile behaviour in the online environment;
- to provide a police presence in social networking sites, and
- to contribute to broader prevention strategies such as educational campaigns.[11]

11.16 Specific objectives are to enhance its contribution to combating technology crime impacting Australian families by:

- actively targeting the production and distribution of online child sex exploitation images;
- creating a hostile environment on the Internet for online offenders through the development of active and innovative methods of informing potential offenders of the risks involved in their activity;
- increasing research into the evolving digital landscape and emerging threats to better predict trends and capabilities and develop active targeting, prevention and disruption strategies for online crimes, especially those involving child victims;
- promoting community awareness through active liaison with government and non-government organisations such as educational agencies and community groups;
- developing and implementing an Australian National Victim Image Library; and
- developing and implementing a training and welfare strategy to deal with identified risks associated with teams working within the online child sex exploitation arena.[12]

11 Australian Federal Police, *Submission 64*, p. 9.

12 Australian Federal police, *Submission 64*, p. 10.

11.17 The AFP is also responsible for the development and implementation of a covert capacity to identify, target and investigate online predators, including:

- purchasing software similar to that used by offenders;
- purchasing software for the collection of evidence;
- implementing and maintaining a *covert* and an *overt* police presence on the Internet;
- purchasing non-government specification hardware from non-government suppliers;
- maintaining an online presence including warnings in chat rooms relating to potential predatory behaviour, utilising the Virtual Global Taskforce as appropriate, and
- 'deterrence initiatives', such as redirection of all 'take down' sites to warning sites requiring the development, implementation and installation of the software required.[13]

11.18 Community education remains one of the most important elements of crime prevention. Through initiatives such as *Cybersafety* and the *Thinkuknow* program, the AFP engage with community groups, parents/carers and school-aged children. In the first nine months of 2010/2011, it delivered 51 *Cybersafety* presentations to 8,130 participants, and 118 *ThinkuKnow* presentations to 4,450 participants.[14]

11.19 *ThinkuKnow* involves presentations by trained volunteers, and a comprehensive website which provides additional information and resources. The themes of 'Have fun', 'Stay in control' and 'Report' form its focus in both the presentations and on the website launched in February 2010. It aims to open lines of communication between parents/carers and children, so that the Internet is as much a topic of discussion as events at school that day. The *ThinkuKnow* button forwards the contact details to the police and this can be followed up.[15]

11.20 The AFP also embarks on a program of cyber-safety awareness presentations at schools in regional NSW and Victoria, and the ACT. This Youth Education Program is designed to make young people think of the consequences of what they do online. The presentations are backed up by

13 Australian Federal Police, *Submission 64*, p. 10.

14 Commander Grant Edwards, Acting National Manager, High Tech Crime Operations, Australia Federal Police, *Transcript of Evidence*, 24 March 2011, p. CS5, 4.

15 Australian Federal Police, *Submission 64*, p. 22.

Fact Sheets made available on the AFP website, and in hard copy. This program also makes young people aware of the need to protect their images and reputations by being careful of with whom they communicate.[16]

11.21 Older computer users are also at risk online. The AFP delivers sessions to such users on how they can protect personal and financial information, secure wireless connections and conduct secure banking online.

11.22 The AFP is also involved in annual National Cyber Security Awareness Weeks, which demonstrate the importance of working together to achieve a safe online experience for all.[17]

11.23 Online crime is borderless and evidence can be transitory, highly 'perishable' and often located overseas. A key issue for law enforcement is therefore an effective and efficient legal framework for the exchange of information and evidence with overseas authorities.

11.24 There are two ways the AFP can engage with overseas law enforcement agencies for the provision of information:

- on a police-to-police basis, or
- via the *Mutual Assistance in Criminal Matters Act 1987* (Cth).[18]

11.25 For evidence to be used, the latter approach is required. While its operations are under review, this Act is based on the historical legal framework and its operations 'can be cumbersome', unlike online technology which acts very quickly.[19]

11.26 The Virtual Global Taskforce is among the international forums of which the AFP is a member. In December 2009, the AFP became the Chair of this body, made up of police forces from around the world working to fight online child abuse. Its objectives are:

- to make the Internet a safer place;
- to identify, locate and help children at risk, and
- to hold perpetrators to account.

11.27 The AFP hosted a conference of the Virtual Global Taskforce in December 2010. A key outcome was an agreement for international law enforcement

16 Australian Federal Police, *Submission 64*, p. 23.
17 Australian Federal Police, *Submission 64*, p. 24.
18 Australian Federal Police, *Submission 64*, p. 13.
19 Australian Federal Police, *Submission 64*, p. 13.

agencies to work with international industry partners, non-government organisations and the academic sector to find ways of increasing child safety in the online environment, and to remove children from harm. The Virtual Global Taskforce is working towards developing an effective method for the exchange of information and evidence with overseas partners, including sharing international 'hash values' given to identify every child abuse image seized.

11.28 The AFP also has regional alliances via such bodies as the Australia and New Zealand Police Advisory Agency Child Protection Committee, and the Jakarta Centre for Law enforcement Cooperation, to combat online child sex exploitation.[20]

11.29 The AFP has had a senior member seconded to work in an information and communications technology company in the United States to learn from industry.[21]

11.30 Mr Mark Newton commended the AFP:

> The AFP retains world-recognized expertise in tackling criminals who groom children, online and off. Their Online Child Sexual Exploitation Taskforce (OCSET) is capable and effective, and deserves significant expansion ... An adequate response to sexual grooming would be to increase the resources available to the AFP so that they are better able to investigate and arrest child abusers.[22]

11.31 As the Australian Institute of Criminology noted, mutual assistance treaties present problems for all trans-national police investigations, so that there is 'probably' a need to improve the speed of undertaking inquiries. Nonetheless, gathering evidence across jurisdictions and conducting prosecutions is 'bound to be difficult'.[23]

11.32 Ms Sarah Chidgey from the Attorney-General's Department commented:

> In terms of the proposed reforms to mutual assistance in criminal matters laws, as I mentioned, there was the release of a second exposure draft of those reforms. Our consultation period has just run for six weeks; it concluded on 14 March. Those reforms are designed to promote more responsible and flexible measures to

20 Superintendent Bradley Shallies, National Coordinator, Child Protection Operations, Australian Federal Police, *Transcript of Evidence*, 11 June 2010, p. CS40.

21 Superintendent Bradley Shallies, National Coordinator Child Protection Operations, Australian Federal Police, *Transcript of Evidence*, 11 June 2010, p. CS29.

22 Mr Mark Newton, *Submission 15*, p. 8.

23 Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS9.

> secure international crime cooperation. Some of the things that those proposed reforms would do are to streamline the process for providing lawfully intercepted material and covertly accessed stored communications, to allow for covert access to stored communications and surveillance devices, and provide existing telecommunications data on a police-to-police basis. It is particularly valuable, as Commander Edwards mentioned, as the police-to-police mechanisms can operate a lot faster than the more formal mutual legal assistance mechanisms.
>
> Finally, those reforms would also enable collection and transmission of prospective telecommunications data. In terms of where that process is at, a number of submissions have been received as part of the consultation process. [24]

11.33 The South Australian Police Force noted that, because applications for assistance must often go to foreign regulators, the current process for the administration of applications under such treaties 'rarely' produces timely investigative outcomes.[25] It further commented:

> Whilst Facebook have stated that they can respond to a Mutual Assistance request in 10 days, the Attorney-General's office has stated that it will take them at least 6 months to process the request before it is forwarded to Facebook. The uptake in the use of social networking dictates that law enforcement will require content from overseas providers on an ever increasing basis. There is a very real need to improve the process for obtaining information or court outcomes could likely be affected.[26]

11.34 There is a substantial fee incurred for law enforcement agencies requesting details of accounts in situations which are not life threatening.[27] Mr Stewart Healley commented:

> Reluctance from experience of doing all the investigation work for a brief to have the Offenders Solicitor convince the Magistrate to treat the incident lightly with a warning and no penalty or even dismissed the Charges, reinforcing the Court Message to the Offender "go do what you like" and to the Victim – "SORRY".[28]

---

24 Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch, Attorney General's Department, *Transcript of Evidence*, 24 March 2011, p. CS20.

25 South Australia Police Force, *Submission 86*, p. 2.

26 South Australia Police Force, *Supplementary Submission 86.1*, p. 2.

27 Mr Stewart Healley, *Submission 136*, p. 45.

28 Mr Stewart Healley, *Submission 136*, p. 45.

11.35 In one situation, the Victorian Police were able to contact an online bully via Facebook in a situation where they could not physically locate them to serve an appropriate warning.[29]

State and Territory responsibilities

11.36 The various codes criminalise some abuses, making them punishable by lengthy periods of imprisonment.

New South Wales

11.37 Offences under NSW legislation include:

- Stalking or intimidation intending to cause fear of physical or mental harm. It explicitly catches conduct involving the use of devices such as 'telephone, telephone text messaging, emailing and other technologically assisted means'; and
- Grooming a child under 16 years of age for unlawful sexual activity. It also makes provision to capture online conduct and similar means of communication.[30]

11.38 The Communications Law Centre noted that NSW is currently the only Australian jurisdiction that explicitly criminalises cyber-bullying by school children. While section 60E of the *Crimes Act 1900* (NSW) makes it an offence when a person 'assaults, stalks, harasses or intimidates' any school staff or student while attending school, it does not cover bullying outside school premises.[31]

Victoria

11.39 While Victoria does not directly regulate social networking, under the *Crimes Act 1958* (Vic) it has the power to prosecute crimes which may arise from actions taken on such sites, such as:

- threats to kill;
- stalking, including repeatedly using the Internet to publish material designed to make someone else apprehensive;

29 Mr Stewart Healley, *Submission 136*, p. 84.

30 NSW Government, *Submission 94*, p. 19.

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

- abduction with intent to rape, and
- sexual penetration of a child under 16 years.[32]

11.40 A *Personal Safety Intervention Orders Bill* has been introduced. If enacted, this will provide better protection against stalking and behaviours such as bullying and Cyber-bullying.[33]

11.41 Under amendments made to the *Sex Offenders Registration Act*, registered sex offenders must provide additional persona details such as Internet, instant messaging, Facebook and chat room user names, or any other user names or identity used by the person on the Internet or through other online applications.[34]

South Australia

11.42 South Australian Police noted that the State's laws did not specifically mention the online environment. They are, however, designed to deal with the opportunities that the Internet and other platforms provide for predatory criminal behaviour.[35]

11.43 As cyber-bullying is not a criminal offence, South Australian Police does not maintain statistics of the complaints it received.[36] Some of the associated behaviour, such as cyber-stalking and unlawful threats, are criminal and are investigated. Anecdotal evidence suggested that cyber-bullying is rising with the increasing use of technology, although bullying appears to be decreasing in South Australian schools.[37]

11.44 South Australian Police regularly received reports of privacy breaches, generally from concerned parents who were aware of images of their children placed on social networking sites without permission. Because of restrictive legislative provisions, most of these incidents were not criminal. South Australian Police investigated where the intent was to commit a serious offence, such as the posting of intimate images without permission, stalking or identity theft.[38]

---

32 Victorian Government, *Submission 112*, p. 5.

33 Victorian Government, *Submission 112*, p. 5.

34 Victorian Government, *Submission 112*, p. 5.

35 South Australia Police, *Submission 86*, p. 1.

36 South Australia Police, *Submission 86*, p. 2.

37 Mr Greg Cox, Director, Student Wellbeing Department of Education and Children's Services, SA, *Transcript of Evidence*, 3 February 2011, p. CS70.

38 South Australia Police, *Submission 86*, p. 2.

11.45 Use of social networking sites by young people regularly required South Australian Police to obtain information from sites such as Facebook to identify criminal activity and safeguard children. It also had some concerns about mutual assistance treaties.[39]

11.46 South Australian Police regularly cooperated with other agencies, inside and outside the State, including the Australian Communications and Media Authority (ACMA) and the Australian Competition and Consumer Commission. While material from such bodies was of a high standard, more agencies were developing their own strategies and South Australian Police believed that there was a risk that messages about safety and security in the online environment would become confused.

11.47 Through the WatchSA Program, South Australian Police personnel trained in aspects of Internet safety, including issues for parents/carers and adolescents about computer security, scams, etc. The force had developed related packages about the use of technology, including a document on cyber-bullying and e-crime that was distributed to all schools in South Australia in 2009.[40]

Western Australia

11.48 There is no specific cyber-bullying legislation in Western Australia but, depending on the case, there may be scope for police involvement as threats and stalking are covered in the State's Criminal Code.[41]

11.49 Western Australian Police drew attention to the use of technology to identify known images to prevent their distribution on peer-to-peer networks. For it to be successful, this initiative would require the cooperation of ISPs across Australia. If adopted, this technology would automatically be able to filter out child exploitation material.[42]

11.50 Identification of this material is being addressed through a national information technology project which would allow police to compare automatically seizures of child exploitation material against a known data base. This would speed up the assessment of unknown images, potentially identify victims and contact likely offenders.[43]

---

39 South Australia Police, *Submission 86*, p. 2.

40 South Australia Police, *Submission 86*, pp. 2-3.

41 Western Australia Office of the Commissioner of Police, *Submission 78*, p. 2.

42 Western Australia Office of the Commissioner of Police, *Submission 78*, pp. 1-2.

43 Western Australia Office of the Commissioner of Police, *Submission 78*, p. 2.

11.51 Law enforcement agencies have been built around traditional physical or imaginary boundaries and dealing with the physical world. Western Australian Police noted, however, that the online environment had broken these boundaries between jurisdictions, both nationally and internationally.

11.52 There has also been fragmentation of agencies across Australia, and within agencies, so that ACMA used one cyber-safety program (*CyberSmart*) and the AFP another (*ThinkUKnow).* The reporting of online offences is fragmented between the West Australian Crime Squad, ACMA and the AFP. Western Australian Police also drew attention to duplications and gaps in services offered by existing agencies, citing different approaches to investigation of online offences by State police forces.[44]

11.53 In Western Australia, although there is scope for further reductions, this fragmentation had been partially addressed, as its Online Exploitation Squad is now co-located with the AFP's Child Protection team.[45]

11.54 Within Western Australian Police, the Office of Crime Prevention is exploring the role of crime prevention officers in cyber-safety, while for operational reasons the Online Child Exploitation Squad has retreated from cyber-safety presentations.

11.55 Related to fragmentation is the fact that technological advances within the online environment are outstripping law enforcement agencies' abilities adequately to resource investigations. The ever-increasing capacities of platforms is a major challenge for police forces, and an argument for a centralised agency within Australia with broad powers to investigate, advocate and act on cyber-safety issues.

11.56 The Force believed that there is an argument for a centralised national agency within Australia with broad powers to investigate, advocate and act on cyber-safety issues.[46]

Tasmania

11.57 Tasmanian Police regularly engage with school communities in a range of educational campaigns which included general information on online safety. They supported the Tasmanian 2010 Crime Stoppers Youth Challenge which targeted e-safety, in which children examined crime and

44 Western Australia Office of the Commissioner of Police, *Submission 78.1*, p. 1.

45 Western Australia Office of the Commissioner of Police, *Submission 78.1*, p. 1.

46 Western Australia Office of the Commissioner of Police, *Submission 78.1*, p. 2.

community safety-related issues and developed strategies to address them.[47]

11.58 While people have been charged with online offences, few cases have involved children. There have been several instances of sexual grooming of children, but the extent of this abuse in the State is difficult to gauge as it is likely that many of these incidents are not reported.[48]

11.59 This force did not see cyber-bullying as primarily an issue for police. Where it became stalking, there is a role for law enforcement but, in less serious cases, it is a parental and educational issue because police involvement can make incidents more difficult to resolve.[49]

Sanctions against cyber-bullying

11.60 As observed in Chapter 3, there has been little detailed examination of the legal issues associated with bullying, and even less of those involving cyber-bullying. In particular, schools' responsibilities under civil law, and the criminal ramifications of this conduct, are not well understood.[50]

11.61 The Attorney-General's Department advised that serious instances of cyber-bullying may constitute an offence under Commonwealth law. It is an offence to use the Internet or a mobile phone in a way that a reasonable person would consider to be menacing, harassing or offensive, and it carries a maximum penalty of three years imprisonment. The Criminal Code sets the age of criminal responsibility for Commonwealth offences at 14 years. A child aged ten years or more, but less than 14 years old, can only be criminally responsible if she/he knows that the conduct is wrong. The onus is on the prosecution to establish awareness of wrongdoing beyond a reasonable doubt.[51]

11.62 Professor Marilyn Campbell expressed the view that:

> Even though there are not so-called specific anti-cyberbullying laws, there are enough criminal justice laws on cyberstalking, harassment and telecommunications that, if you wanted to criminalise a child's behaviour, the laws are there—except that, as

47 Tasmania Police, *Submission 85*, p. 2.

48 Tasmania Police, *Submission 85*, p. 1.

49 Tasmania Police, *Submission 85*, p. 2.

50 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 27. See Chapter 11.

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

> you know, children under 10 are not held criminally responsible for their actions no matter what they do. Between 11 and 14, it is up to the court to decide whether they intended to commit a criminal act. So it is not about knowing it was naughty and knowing it was wrong and responding to something and not thinking before they clicked. It is about whether they intended to commit a criminal act and whether they then went ahead realising that it was a criminal act.[52]

11.63 She added that:

> Where we need to use the law is in civil litigation, and that is not going to be against the kids and not against the parents; that is going to be against the schools because they are the ones that have got the money.[53]

11.64 The Attorney-General's Department also noted that criminal legislation at State/Territory level allows for the prosecution of harassing, threatening and intimidatory behaviour through a combination of assault, threatening and stalking offences. These jurisdictions can also rely on offences in the Commonwealth Criminal Code which directly address these abuses.[54]

11.65 The Alannah and Madeline Foundation believed that, because the relationship of bullying to cyber-bullying is integral to the abuse, responses would be best focused on behavioural change in the school and beyond. These would be most effective when developed collaboratively, involving school personnel, parents/carers, young people, the Internet industry and the wider community.[55] The Family Online Safety Institute:

> stresses the importance of differentiation between teasing or mean comments and actual criminal harassment. Instead of criminalization, the solutions should include education, empowerment and the use of website tools and services to mitigate the likelihood that children will fall prey to cyberbullying. The Cybersmart Hero program that is being run by the Australian Communications and Media Authority (ACMA) is a good example of a way to engage children in working towards a solution. The Cybersmart Hero program requires children to work together online, with professionals, to solve a real time cyberbullying-

52 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS26.

53 Associate Professor Marilyn Campbell, School of Learning and Professional Studies, Queensland University of Technology, *Transcript of Evidence*, 30 June 2010, p. CS26.

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

55 Alannah and Madeline Foundation, *Submission 22*, p. 19.

> themed problem. Since it is often children who are witnesses to cyberbullying, this education initiative is vital to lowering these occurrences. It also emphasizes the importance of education rather than criminalization.[56]

11.66 The Communications Law Centre noted that Australia's reluctance to legislate more specifically against cyber-bullying is reflected in the United States where some States encompass it in general anti-harassment laws, or within computer crime statutes. The right to freedom of speech is also seen as a barrier to extensive cyber-bullying legislation, as it may curb the bullies' rights.[57]

11.67 It also argued that Australian legislation should provide 'clear and adequate recourse', particularly for victims of cyber-bullying.[58]

Sanctions against cyber-stalking

11.68 All Australian jurisdictions have laws dealing with cyber-stalking. Victoria and Queensland have explicitly extended the definition of the crime to include the sending of electronic messages.

11.69 Mr Stewart Healley commented that:

> The anti-stalking legislation has a number of advantages as a means of addressing cyber bullying. First, a wide range of hostile behaviour falls within its ambit which in itself need not be criminal. For example, a threat which is merely implicit rather than explicit would still be caught. Secondly, while there are differences between jurisdictions in relation to the offender's requisite intent and the required state of mind (if any) of the victim, it is usually sufficient that the offender, by means of repeated conduct (other than in Queensland, which refers to 'at least one occasion'), intends to induce in the target an apprehension or fear of violence or harm (which in most Australian jurisdictions includes the intention to cause the target either physical or mental harm). Accordingly this offence is well suited to cases of cyber bullying, where the purpose is normally to cause emotional, rather than physical, harm and distress.[59]

56 Family Online Safety Institute, *Submission 38*, p. 6.
57 Communications Law Centre, *Submission 63*, p. 6.
58 Communications Law Centre, *Submission 63*, p. 6.
59 Mr Stewart Healley, *Submission 136*, p. 96.

11.70 The *Criminal Code Act 1995* (Cth) also includes offences relating to cyber-stalking, including:

- Using a telecommunications network intending to commit a serious offence. This is intended to be broad and cover the use of the Internet or other applications to commit such offences as fraud or stalking;
- Using a carriage service to make a threat. This is intended to cover threats made over the Internet to kill or cause serious harm; and
- Using a carriage service to menace, harass or cause offence. This is intended to cover online conduct that a reasonable person would find to be menacing, harassing or cause offence.[60]

11.71 The Australian Institute of Criminology noted that there are difficulties in drafting anti-stalking legislation because not all behaviour is criminal.[61] Mining information about a potential victim from publicly available information, such as profiles on social networking sites, is not illegal, nor is posting non-threatening messages. Ms Sonya Ryan believed that young people need to be encouraged to use links to certified sites to avoid people who, to seek to entrap them for criminal purposes, pose as celebrities online.[62] When such activities are repeated over a period in an unwelcome way, these seemingly inoffensive acts acquire menacing overtones for the target.[63]

11.72 Mr Healley commented:

> All Australian jurisdictions now have stalking legislation proscribing behaviour calculated to harass, threaten or intimidate ...Common examples include following the target, sending articles to the target, waiting outside or driving past the target's home or place of work, and repeated contact by phone, email or text ... They are therefore of particular relevance to cyber bullying where, like all cases of bullying, there is a similar exploitation of power imbalance.[64]

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

61 Australian Institute of Criminology, *Submission 56*, p. 10.

62 Ms Sonya Ryan, Director, Carly Ryan Foundation, *Transcript of Evidence*, 3 February 2011, p. CS64.

63 Australian Institute of Criminology, *Submission 56*, p. 10.

64 Mr Stewart Healley, *Submission 136*, p. 95, citing Butler D, Kift S and M Campbell, 'Cyber Bullying in School and the Law Is there an effective means of addressing the Power imbalance?' eLaw Journal: *Murdoch University Electronic Journal of Law*: 16(1) p. 84.

Sanctions against sexual grooming

11.73 Responsibility for combating sexual exploitation of children is shared between Australia's jurisdictions. The States and Territories are generally responsible for offences related to this abuse within their jurisdictions. The Commonwealth has traditionally enacted laws dealing with these offences occurring across or outside these jurisdictions, e.g. child sex tourism and offences involving the online environment.

11.74 In 1995, the Commonwealth first enacted legislation targeting the use of a carriage service, the Internet or mobile phone for sexual activity with children. This included grooming and procuring. The operation of this legislation was enhanced in 2010 by including increased penalties, and it now covers the following offences:

- Using a carriage service to transmit a communication with the intention of procuring a person who is, or who the sender believes to be, under 16 years of age to engage in sexual activity (procuring);
- Using a carriage service to transmit a communication with the intention of making it easier to procure a person who is, or who the sender believes to be, under 16 years of age to engage in sexual activity (grooming); and
- Using a carriage service to transmit an indecent communication to a person who is, or who the sender believes to be, under 16 years of age.[65]

11.75 Over 400 predators are arrested by police each year and this number if increasing.[66] Ms Ryan commented:

> Not all of these people are always prosecuted, because of legal loopholes or different things that happen. But that is a statement that the cybersafety police in WA made, that they are just scratching the surface and they do not have the manpower on the ground to be able to really penetrate this problem.[67]

11.76 The ACT Council of P&C Associations called for the Australian Government to:

---

65 Attorney-General's Department, *Submission 58*, pp. 5-6.

66 Ms Sonya Ryan, Director, Carly Ryan Foundation, *Transcript of Evidence*, 3 February 2011, p. CS60.

67 Ms Sonya Ryan, Director, Carly Ryan Foundation, *Transcript of Evidence*, 3 February 2011, p. CS63.

> follow a similar action as the USA in pressuring SNS to delete known sex offenders registered in Australia. In February 2009, MySpace deleted 90,000 profiles of sex offenders registered in the USA which was made possible as part of an agreement between the website and state attorneys general. It is recommended that the Australian Government introduce a similar agreement with popular social-networking sites to restrict access for known sex offenders in Australia.[68]

Sanctions against sexting

11.77 Under Commonwealth legislation, there are only criminal implications for sender and receiver if an image constitutes child pornography. Distributing other images can be a form of cyber-bullying if a young person is coerced into posing, or if images are distributed without consent.[69]

11.78 Images distributed in this way may also be picked up by pornographers and could be used to blackmail the subject. Originators could be charged with making child pornography, and the person receiving it with the e-crime of disseminating that material.[70]

> Under proposed changes to the Sex Discrimination Act to be introduced by the Australian government, young people who have experienced cyberbullying and online sexual harassment will be given legal protection, and victims under the age of 16 allowed to use sexual harassment laws to pursue their persecutors.[71]

11.79 The Victorian Office of the Child Safety Commissioner added that:

> We support strong and effective sanctions against adults who produce and distribute child pornography or otherwise use technology to groom or abuse children. The more challenging issue for legislative and policy reform is how to respond to children who engage in such behaviours.[72]

11.80 The Commissioner would like to see consideration given to:

68 ACT Council of P&C Associations, *Submission 41*, p. 12.

69 NSW Government, *Submission 94*, p. 9.

70 Dr Helen McGrath, School of Education, Faculty of Arts and Education, Deakin University, *Transcript of Evidence*, 30 June 2010, p. CS24.

71 Alannah and Madeline Foundation, *Submission 22*, p. 29.

72 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 3.

> whether criminal sanctions are the most appropriate response to such conduct, if so under what circumstances they should be used, and what other options might be most effective.[73]

11.81 Family Voice Australia argued that laws should be applied to the possession of child pornography in the context of sexting, provided law enforcement authorities had discretion to dissuade one-time offenders from repeating the offence.[74]

11.82 In Australia, 32 Victorian teenagers were charged with child pornography offences resulting from sexting.[75] Many young people are unaware that sexting may be considered a criminal offence.[76]

Sanctions against illegal or inappropriate content

11.83 The Australian Library and Information Association also called for more funding to increase the effectiveness of policing of illegal material on the internet.[77]

Promotion of suicide

11.84 It is an offence to use a carriage service to access, transmit, make available, publish or otherwise distribute material that:

- counsels or incites committing or attempting to commit suicide;
- promotes a particular method of committing suicide, or
- provides instruction on a particular method of committing suicide.

11.85 For the offence to be made out, the person must intend to use the material to counsel or incite suicide, or for it to be used by another person to counsel or incite committing or attempting to commit suicide.

---

73 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 3.

74 Mr Richard Egan, National Policy Officer, Family Voice Australia, *Transcript of Evidence*, 9 December 2010, p. CS55.

75 BoysTown, *Submission 29*, p.15.

76 BoysTown, *Submission 29*, p.14, citing Lenhart A, 2009, *Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging*, Pew Internet and American Life Project.

77 Australian Library and Information Association, *Submission 16*, p. 13.

11.86 A preparatory offence has been created if a person possesses, produces, supplies or obtains suicide-related material with the intention that it be used in committing an offence.[78]

Breaches of privacy and identity theft

11.87 Recognition of the threats posed by identity crime has led to a number of measures directed at preventing online identity crime through systematic improvements to the national identity management system.[79]

11.88 The centrepiece of this response is the National Identity Security Strategy, endorsed by the Council of Australian Governments in 2005. This Strategy is a cross-jurisdictional, whole-of-government approach which emphasises the following six elements:

- Development of a national document verification service to combat the misuse of false and stolen identities;
- Improving standards and procedures for enrolment and registration for the issue of proof of identification documents;
- Enhancing the security features on proof of identification documents to reduce the risk of incidence of forgery;
- Improving the accuracy of personal identity information held on organisations' databases;
- Enabling greater confidence in the authentication of individuals using online services; and
- Enhancing the national interoperability of biometric identity security measures.[80]

11.89 These measures are intended to make it more difficult for criminals to create new identities or incorporate fabricated or inaccurate information into false identification credentials.[81]

11.90 In March 2011, the *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011* (Cth) inserted three new identity crimes into the Criminal Code:

78 Attorney-General's Department, *Submission 58*, p. 6.
79 Attorney-General's Department, *Submission 58*, p. 6.
80 Attorney-General's Department, *Submission 58*, pp. 6-7.
81 Attorney-General's Department, *Submission 58*, p. 7.

- Dealing in identification information with the intention of committing, or facilitating the commission of a Commonwealth indictable offence;
- Possession of identification information with the intention of committing, or facilitating the commission of, conduct that constitutes the dealing offence; and
- Possession of equipment to create identification documentation with the intention of committing, or facilitating the commission of, conduct that constitutes the dealing offence.[82]

11.91 That Act also contains measures to assist victims of identity crime, allowing a person who has been the victim of identity crime to approach a magistrate for a certificate to show they have had their identity information misused. The certificate may assist victims of identity crime in negotiating with financial institutions to remove fraudulent transactions, and other organisations such as Australia Post, to clear up residual problems with identity theft.[83]

11.92 The Communications Law Centre commented that opportunities for criminal acts in the online environment will continue to increase, as it becomes further intertwined with the everyday lives of both adults and children/young people.[84]

Information requests

11.93 One of the biggest frustrations identified by some school principals is the inability to trace cyber-bullying when bullying has an impact in a school. Compounding this is the inability, even with police support, to have harmful and inappropriate content removed from websites. This also has implications for cyber-bullying of teachers, and this is considered in Chapter 9.[85]

11.94 Part 13 of the *Telecommunication Act 1997* (Cth) allows law enforcement agencies to make certified and uncertified requests for the disclosure of customer information. Mr Stewart Healley commented that:

> For an uncertified request, the ISP must be satisfied that the disclosure of information is reasonably necessary for the enforcement of criminal law... Certified requests are those where a

82 Attorney-General's Department, *Submission 58*, p. 8.
83 Attorney-General's Department, *Submission 58*, p .8.
84 Communications Law Centre, *Submission 63*, p. 6.
85 New South Wales Secondary Principals' Association, *Submission 32*, p. 3.

> senior officer of a criminal law enforcement agency that the disclosure is reasonably necessary.[86]

11.95 The South Australia Police raised the issue of information required for evidence:

> Access to mobile Internet Profile (IP) data which can be used to identify an Internet user is now also impacting upon law enforcements ability to investigate matters. Companies such as Optus and Telstra have informed that IP data is not available after relatively short periods of time (up to one month only). In many cases, IP data is not requested until after the expiration of such a short period. Mandated requirements for retaining information pertaining to communication would be of direct benefit to law enforcement in investigations.[87]

11.96 Western Australia Police also raised this issue:

> One challenge currently being experienced by the WA Police is obtaining quicker and easier access to companies' information (Facebook, MySpace, Microsoft etc) either for a law enforcement purpose or when bullying needs to be reported. Advice is often provided to users on reporting abuse / bullying to the companies, however, it often takes many weeks before the companies resolve the issues reported.[88]

11.97 Further, some service providers were critical of the adequacy of response by law enforcement agencies. Of note was the lack of knowledge in relation to seeking legal evidence.[89] For example, the Australian Council for Computers in Education commented that:

> To date, police responses to risks associated with SNS use in all Jurisdictions studied for this report have tended to be fragmented and insufficiently coordinated.[90]

Community education

11.98 Young people are not necessarily aware of the legal options:

---

86 Mr Stewart Healley, *Supplementary Submission 136.1*, p. 53

87 South Australia Police, *Supplementary Submission 86.1*, p. 2.

88 Office of Commissioner of Police, WA *Submission 78*, p. 3.

89 Mr John Lindsay, General Manager, Regulatory and Corporate Affairs, Internode, *Transcript of Evidence*, 8 July 2010, p. CS11.

90 Australian Council for Computers in Education, *Submission 128*, pp. 2-3.

> that despite the comfort with which they use these technologies, teens are unaware of their legal options in the context of these technology rich areas, particularly those relating to privacy and their personal information. Additionally, many teens are still unaware of the practical and very realistic consequences of their actions.[91]

11.99 The Association of Independent Schools of South Australia called for:

> A promotional campaign put in place to inform school communities what constitutes an e-crime. Many students may not be aware that what they are doing is not only bullying, but it may also be against the law.[92]

11.100 The Office of Youth made the point that people do not know what is legal and what is not.[93] Professor Phillip Slee argued:

> there does need to be exactly that kind of education for the community around what constitutes criminal activity. When we worked with the police we found that young people in particular did not know that uploading images or taking images et cetera could constitute stalking or blackmail. So again we come back to that notion of strongly advocating for an educational approach, albeit keeping in mind that there is a legal component to it.[94]

11.101 The Australian Council for Computers in Education highlighted the need to consider the legal risks arising from using social networking sites as there is a concern about the level of understanding of the nature of the risks in areas of 'the law that give rise to possible legal liability for young people using [social networking sites]:

- Privacy disclosure and breach of confidence
- Intellectual property rights especially copyright infringement
- Defamation; and
- Criminal laws including harassment and offensive material.[95]

11.102 The Australian Psychological Society added that:

---

91 Mr Nick Abrahams and Ms Ju Young Lee, *Submission 66*, p. 1.

92 Association of Independent Schools of SA, *Submission 19*, p. 12.

93 Mrs Tiffany Downing, Director, Office of Youth South Australia, *Transcript of Evidence*, 3 February 2011, p. CS21.

94 Professor Phillip Slee, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, p. CS15.

95 Australian Council for Computers in Education, *Submission 128*, p. 2.

> while legal implications should not be the sole driver of cyber-safety measures targeted to children and young people, important components of cyber-safety include informing them about their 'digital footprint', including the likelihood that their activities are often very traceable, and facilitating them to take responsibility for the consequences of their actions, including that they may be held liable for inappropriate activity.[96]

11.103 Increasingly the New South Wales Director of Public Prosecutions is prosecuting offences involving young people using the internet.[97] Offences may fall both with state and commonwealth jurisdictions because of the use of telecommunications.[98] Family Voice Australia made the point that 'prosecutions should only happen in the very worst cases'.[99]

Legal risks

11.104 The National Children's and Youth Law Centre stated that in most cases bullying had occurred at schools as well as online and young people seek advice on the possibility of legal recourse.[100] The Centre also commented:

> Some examples of these questions are whether schools can regulate young people's online access, whether you can be banned from using a website, the consequence of acrimonious online conversations, using unsecured wireless networks, what action can be taken about racist comments online, illegal downloads of music and movies, whether there is any law about protecting children online and use of file sharing programs.[101]

11.105 It believes that there should be support for schools including:

> providing accurate information about rights, community education and support services, effective complaints procedures and accessible dispute resolution mechanisms. Legal remedies should be a measure of last resort in most cases (although the desirability of legal mechanisms when it comes to prosecuting child pornography offences is not in question). Children also need to be active participants in this process and must be consulted both

96 Australian Psychological Society, *Submission 90*, p. 17.

97 New South Wales Director of Public Prosecutions. *Submission 47*, p. 1.

98 New South Wales Director of Public Prosecutions. *Submission 47*, p. 1.

99 Mr Richard Egan, National Policy Officer, FamilyVoice Australia, *Transcript of Evidence*, 9 December 2010, p. CS55.

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

101 National Children's and Youth Law Centre, *Submission 138*, p. 8.

> in the design of education programs and their evaluation. This lends young people a sense of ownership, and enhances the effectiveness and relevance of emerging policies and programs amongst their fellow peers.[102]

National accredited training

11.106 Evidence to the Inquiry indicates that the police and the justice system in Australia are not sufficiently supporting or equipped to support some victims and parents/carers. For many people, complaining to local police about abuses in the online environment has not always been satisfactory. Only the worst cases of bullying and cyber-bullying seem to be investigated, let alone prosecuted. In practice, intervention orders against individuals are difficult to enforce. The increasing impact of the online environment means that without additional resources and education for police on the front line, this situation may worsen. The systematic education of frontline police in the range of cyber-safety issues will assist in increasing sensitivity of handling complaints about this difficult area.

11.107 To be effective, this education needs to begin during recruit training and to be reinforced through a range of courses throughout an officer's career. In keeping with the cooperative national approach required to deal with abuses in the online environment, the AFP is the appropriate body to devise suitable courses, in conjunction with the police forces of the other Australian jurisdictions.

11.108 One suggestion was the establishment of a National Accredited Bullying and Cyberbullying Training Program for the AFP and State Police:

> Provide the necessary resources to support Federal and State Police to minimise bullying and cyberbullying practices by providing Police Members with a National Accredited Bullying & Cyberbullying Training Program.[103]

102 National Children's and Youth Law Centre, *Submission 138*, p. 10.

103 Mr Stewart Healley, *Submission 136*, p. 23.

Recommendation 21

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

11.109 The training should also be extended to Magistrates' Courts, to:

> Provide the necessary resources to support Magistrate Court and DPP Staff to minimise bullying and cyberbullying practices by providing Judges and Prosecutors with a National Accredited Bullying & Cyberbullying Training Program.[104]

11.110 The Committee was told of case where, to protect her child, a mother had to take out restraining orders against a number of girls:

> At the initial hearing the magistrate who granted the interim orders stated something to the effect that he could not include Facebook and MySpace as he was not personally familiar with and did not understand those sites.[105]

Recommendation 22

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

Law enforcement

11.111 Professor Marilyn Campbell commented that while legislation can set a benchmark for societal norms, it does not follow that young people must be imprisoned if they offend and that:

104 Mr Stewart Healley, *Submission 136*, p. 23.

105 Name withheld, *Submission 130*.

> the police only uphold the law, and there is no law against being nasty and there is no law against bullying.[106]

11.112 Professor Elizabeth Handsley referred to the similarity with domestic violence law and the possibility of applying existing legislation:

> there is plenty of law that could be applied to that behaviour; it is just a matter of getting the enforcement mechanisms in place that pick it up and properly apply it to that behaviour. But there is always room for context-specific laws that make it very clear to law enforcers, 'No, you really need to take this into account and to take it seriously.'[107]

11.113 Bullying is usually seen as a behavioural matter and not a criminal offence and police are rarely involved.

11.114 However, the Community Law Centre suggests that 'the offence of cyber-assault be specifically incorporated into legislation and strengthened to adequately protect consumers including children throughout Australia.' It also point out noted that:

> New South Wales is the only jurisdiction that explicitly criminalises cyber-bullying by school children into its Crimes Act8. Section 60E of the *Crimes Act 1900* (NSW) makes it an offence where a person 'assaults, stalks, harasses or intimidates' any school staff or student while attending school. This wording, however, leaves bullying outside of school premises without the ambit of this section.[108]

11.115 It should be noted that:

> cyberbullying can constitute criminal conduct, especially when the behaviour is seriously threatening, harassing or intimidating. While there may be a natural tendency to seek to avoid the criminalisation of young people in this context, criminal sanctions are appropriate to more cases than are generally appreciated, while very few young people seem to appreciate their potential for attracting criminal liability. Media reports and other accounts, however, have recently highlighted that schools themselves, if not teachers and parents also, are increasingly inclined to resort to the criminal law; often out of fear, frustration or in the interests of

106 Associate Professor Marilyn Campbell, Australian University Cyberbullying Research Alliance, *Transcript of Evidence*, 3 February 2011, pp. CS13, 16.

107 Professor Elizabeth Handsley, President, Board Member and Chair of Executive Committee, Australian Council on Children and the Media, *Transcript of Evidence*, 3 February 2011, p. CS45.

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

> community safety. It is imperative to consider the issue of either criminalising or providing formative discipline for these behaviours.[109]

11.116 Mr Stewart Healley made the point that:

> Nevertheless, cyber bullying may easily be conceived in terms of well know criminal offences such as assault, threats, extortion, stalking, harassment, and indecent conduct. In addition, an increasing array of new offences, such as torture, voyeurism, cyber stalking, and telecommunications offences may be relevant. The New South Wales provisions and some of these other offences as they apply to cyber bullying are worth closer examination.[110]

11.117 Under common law, the responsibility of schools for cyber-bullying is not well understood.[111] The Australian University Cyberbullying Research Alliance submitted that:

> In the case of the perpetrator, depending on circumstances, such an action might be framed as action for the tort of 'assault', an intentional infliction of psychiatric harm, defamation or the embryonic tort protecting privacy. Unlike criminal law, age is no barrier to a civil liability to pay compensation for cyberbullying.[112]

11.118 The Alliance also emphasised practical considerations:

> The decision whether to bring an action against a child perpetrator is therefore more likely to involve more practical considerations such as whether he or she has sufficient financial resources to make him or her worth suing. Whatever the position in other countries, under Australian law parents are generally not legally liable for the acts of their children and thus it is usually schools which are involved in civil litigation.[113]

11.119 The following comments were made by respondents to various questions throughout the Committee's *Are you safe?* survey:

---

109 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 28.

110 Mr Stewart Healley, *Submission 136*, p. 91.

111 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 27.

112 Australian University Cyberbullying Research Alliance, *Submission 62*, p. 28.

113 Australian University Cyberbullying Research Alliance, *Submission 62*, pp. 28-29.

> Add a law that says every website needs to act on cyberbullying, whatever site they run (Male aged 15).
>
> Stronger laws regarding bullying practice online (Female aged 17).
>
> Providing the police would be good but it will not help to solve the problem. It could make the bullies more aggressive? (Female aged 16).
>
> With polocing and enforcing using teachers and parents to enforce thse are not a good idea, most of the time I have noticed that my generation does not care or respect most teachers and parent, they need to know there will be servere consquences but also you need to find a way to make then understand respect amoung others, at a young age and contunie to drill it in, also mabye teaching the discipline may help (Female aged 16).

11.120 The AFP made the point that although there are numerous crime prevention, education and awareness programs actively endeavouring to raise awareness of parents, carers, teachers and children, these are mostly targeted at mainstream audiences.[114] The AFP added that very few of these programs have been evaluated for their impact.[115]

Role of industry

11.121 The Australian Institute of Criminology refer to the greater potential of an effective partnership between the public and private sectors rather than attempting to use law enforcement on its own in dealing with online risks.[116]

11.122 The AFP advised that,

> Legal mechanisms for compelling [content service providers (CSP's)] to remove content are limited, and are unlikely to succeed due to the costly and lengthy process involved. Even where a legal remedy was successful, it would likely be detrimental to the AFP's future relationships with that CSP where assistance of an even more critical nature is required.[117]

---

114 Australian Federal Police, *Submission 64*, p. 2.

115 Australian Federal Police, *Submission 64*, p. 4.

116 Australian Institute of Criminology, *Submission 56*, p. 11, citing Choo K-KR 2009a, *Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences*, Research and public policy no. 103. Canberra: Australian Institute of Criminology.

117 Australian Federal Police, *Submission 64*, p. 19.

11.123 The Australian Institute of Criminology added that:

> The private sector must also play a role in crime prevention as most online environments are commercially owned and operated (e.g. social networking sites). Although there is an imperative for private sector organisations to respond to corporate and shareholder interests, these interests should not neglect the need to provide a safe and secure environment for users, particularly children and young people. Business interests, therefore, need to devote resources both to maximising profit as well as minimising opportunities for systems to be used for illegal activities.[118]

Concluding comments

11.124 Cyber-values stressed the need to deal with the underlying values instead of adopting defensive stances and excessive regulations:

> For most ethical problems, participants resorted to legal sanctions and technical precautions for solutions.[119]

11.125 All Australian jurisdictions have laws that can be used against crimes committed in the online environment. Inevitably, the enactment of laws follows criminal acts, and it is not clear that current statutes include a range of effective cyber-safety protection. A review of what has been enacted in the various jurisdictions would be a means of assessing what is effective, and where additional legislation is required. The AFP reflected,

> The Commonwealth legal and regulatory framework is under constant review. Law reform in this area presents a number of challenges due to the rapidly changing digital environment and the transnational and highly adaptable nature of online criminality.[120]

11.126 The Communications Law Centre commented that opportunities for criminal acts in the online environment will continue to increase, as it becomes further intertwined with the everyday lives of both adults and children/young people.[121]

---

118 Australian Institute of Criminology, *Submission 56*, p. 11.

119 Cyber-values, *Submission 8*, p. 2.

120 Australian Federal Police, *Submission 64*, p. 13.

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

11.127 That review could also address the provision of more adequate recourse for victims of cyber-safety crimes, particularly but not only cyber-bullying and identity theft. It could also be extended to include effective legal remedies and adequate compensation for the harm done to victims, especially young people.[122]

Recommendation 23

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

11.128 The Alannah and Madeline Foundation added that there should also be a nationally coordinated cyber-policy plan involving all jurisdictions to ensure that:

> People who have been the victims of cyber abuse [have] a dedicated body to which they can address concerns and complaints, and which has the expertise to remove offending material and prosecute offenders rapidly.[123]

11.129 The process of seeking information from international police forces and other agencies through mutual assistance treaties was designed at the beginning of the digital age, in 1987. It now rarely produces timely results for Australian investigators of online crime. The Australian Institute of Criminology commented:

> the mutual legal assistance treaties that are in existence present problems not only for child exploitation matters but for all transnational police investigations. There probably is a need to improve the speed of undertaking those inquiries, but conducting prosecutions and gathering evidence across jurisdictions is bound to be difficult.[124]

11.130 A review of the current operations of these treaties is under way:

> In January [2011], the government released a second exposure draft of some proposed legislative reforms to Australia's mutual assistance laws which will be designed to promote more

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

123 Alannah and Madeline Foundation, *Submission 22*, p. 13.

124 Dr Russell Smith, Principal Criminologist, Manager, Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS9.

> responsive and flexible measures to a degree; that is obviously at the Australian end. Mutual assistance is always a two-way street where there is another country involved as well. Another step that we are taking is that the Attorney-General, in the quintet of attorneys-general, with the US, Canada, New Zealand and the United Kingdom—there is a meeting in the middle of the year and, at that meeting, the attorneys propose to discuss cyber threats and how we might more effectively cooperate in dealing with them as well.[125]

11.131 The Australian Government has announced its intention to accede to the Council of Europe *Convention on Cybercrime 2001.*

11.132 In relation to an appropriate legal framework, the Alannah and Madeline Foundation highlighted:

- The need to legally define the rights and responsibilities of schools in responding to bullying and cyberbullying situations, and cyber-defamation;
- Legal remedies in themselves are not a solution to bullying, but are a necessary part of the solution; and
- The need to clarify the role of the criminal and civil law in relation to cyberbullying and bullying.[126]

11.133 The Foundation is of the view that a legal framework should be established to manage cyber-abuse that crosses state and political boundaries, and that:

> Federal, State, and Territory government convene a working group involving other stakeholders to consider an appropriate legislative response to cyberbullying and bullying in general in our schools.
>
> Because of the lack of boundaries for the abuse that occur online and with mobile phones, all Australians need to be confident that consistent rules and consequences will apply in all states and territories.[127]

11.134 The Department of Broadband, Communications and the Digital Economy questioned this approach:

---

125 Ms Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch, Attorney-General's Department, *Transcript of Evidence*, 24 March 2011, p. CS9.

126 Alannah and Madeline Foundation, *Submission 22*, p. 5.

127 Alannah and Madeline Foundation, *Submission 22*, p. 13.

> The real question that I think confronts us is whether a legislative framework would be any faster than a voluntary framework. We have found no evidence that the relevant websites, these large multinational websites, are reluctant to take this sort of material down. Their user policies are actually very broad in terms of the kinds of materials they can take down compared to, for example, what is covered in the Broadcasting Services Act. They cover a much wider range of material that they describe as inappropriate than is described in legislation. So the breadth of the policies is broader, and we have not seen any evidence of a reluctance on their part to take it down. The key is how you work through a large multinational organisation to move quickly, and it is not clear that legislation would make them move any more quickly than a voluntary arrangement.[128]

11.135 Further, ACMA commented that:

> ACMA and the Attorney-General's portfolio, especially through the Federal Police, have moved to work very closely together. So if a complaint comes in we do triage so it goes to the right place in government. Secondly, we are also focusing on the same issue that other countries have focused on, which is about having points of influence in American companies and educating them to understand that we have local sensitivities which may not at first blush be immediately apparent to them, because community standards do vary from country to country. I think Australia has a particularly good framework for setting out what is important to Australians. So they are the challenges in dealing with the types of problems we have been talking about that we have been working hard to meet.[129]

128 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS14.

129 Ms Andree Wright, Acting General Manager, Consumer, Content and Citizen Division, Australian Communications and Media Authority, *Transcript of Evidence*, 3 March 2011, p. CS15.