SUBMISSION No. 58

Australian Government

Attorney-General's Department

Attorney-General's Department

Submission to the Joint Select Committee on Cyber-Safety

February 2011

1 Introduction

The Internet is an essential tool for all Australians, including children. It is an integral part of our economic and social activities, and a vast resource of information, education and entertainment. The ability to effectively use online tools provides both a skill for life and the means to acquire new skills. While the Internet has created substantial benefits for children, it has also exposed them to a number of dangers, including exposure to illegal and prohibited content. Parents rightly expect the Australian Government to play its part in helping protect children online.

The Attorney-General's Department (the Department) plays a role in the Government's cyber-safety efforts. The Department is responsible for administering Commonwealth policy on criminal law and law enforcement (including cyber crime), cyber security, anti-discrimination, including issues such as cyber-racism, identity security, and classification.

Criminal Code offences

The Department is responsible for Parts 10.6 and 10.7 of the *Criminal Code Act 1995* (the Criminal Code), which contain comprehensive offences dealing with the misuse of telecommunications and cyber crime. **Appendix A** contains a summary of offences relevant to the Committee's consideration of cyber-safety issues.

Part 10.6 contains offences that criminalise the inappropriate use of telecommunications, including the Internet. These offences include: using a carriage service to menace, harass or cause offence; threats to kill or cause harm to a person; and using a carriage service for child pornography.

Part 10.7 contains offences that criminalise conduct which impairs the security, integrity and reliability of computer data and electronic communications. These offences include: unauthorised access, modification or impairment with intent to commit a serious offence; unauthorised impairment of electronic communication; and unauthorised access to, or modification of restricted data.

These offences were framed in technology neutral language to ensure that the offences will remain applicable as technology evolves. For example, the term 'computer' was not defined to ensure the computer offences will encompass new developments in technology, for example, mobile phones that allow access to the Internet. Conduct such as hacking into a person's Facebook account and altering it or using malicious software to steal personal information would generally be covered by the offences in Part 10.7 of the Criminal Code.

National response to cyber crime

At the Standing Committee of Attorneys-General (SCAG) meeting on 7 May 2010, Commonwealth, State and Territory Attorneys-General agreed to establish a National Cyber Crime Working Group (NCWG) to enable jurisdictions to work cooperatively to combat cyber crime.

The NCWG comprises members from State, Territory and Commonwealth law enforcement agencies and justice departments, the Australian Crime Commission, CrimTrac and the Australia New Zealand Police Advisory Agency.

The NCWG met on 28 July 2010 to discuss the issues identified by SCAG at its May meeting and identify other priority areas for enhancing capability. Since the July meeting, the NCWG has conducted a scoping study of existing domestic and international mechanisms for reporting online

crime and prepared a discussion paper on options to improve current reporting arrangements. These options include the creation of a centralised national online reporting facility.

The NCWG has also progressed work on measures to improve coordination and information-sharing in cyber crime investigations, ensure appropriate training for police and judicial officers on electronic evidence and enhance consistency in education and prevention strategies relating to cyber crime.

The NCWG held its second meeting on 10 February 2011. Recommendations arising from that meeting will be put to Ministers in early to mid 2011.

Education and awareness-raising

The Department has released a number of products to advise the public on protecting against online threats. Most recently, the Attorney-General and the Minister for Broadband, Communications and the Digital Economy jointly released the *Protecting Yourself Online – What Everyone Needs to Know* booklet as a part of National Cyber Security Awareness Week (6–11 June). The booklet provides a comprehensive collection of cyber security and safety information and advice on the basic steps Australians need to take to stay secure online.

2 The nature, prevalence, implications of and levels of risk associated with cyber-safety threats

Cyber-bullying

Cyber-bullying is bullying carried out using the Internet, interactive and digital technologies or mobile phones. According to research by Professor Donna Cross at Edith Cowan University, as many as 15 per cent of students aged between 10 to 14 years have been victims of cyber-bullying.[1]

There are currently offences under both Commonwealth and State and Territory legislation which allow for the investigation and prosecution of the types of harassing, threatening or intimidatory online conduct which could constitute cyber bullying and cyber stalking.

At a Commonwealth level, serious instances of cyber-bullying may constitute an offence under Commonwealth law. Under section 474.14 of the Criminal Code, 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. This offence carries a maximum penalty of three years imprisonment.

In relation to cyber-bullying by children, it is important to note that the Criminal Code sets the age of criminal responsibility for Commonwealth offence at 14 years. A child aged 10 years or more but under 14 years old can only be criminally responsible if he or she knows that his or her conduct is wrong. The onus is on the prosecution to establish awareness of wrongdoing beyond a reasonable doubt (section 7.2, Criminal Code).

[1] Turning up heat on web harassment, *Sydney Morning Heard*, 8 May 2009. http://www.smh.com.au/articles/2009/05/07/1241289315391.html.

Generally, criminal legislation at the State and territory level allows for the prosecution of harassing threatening and intimidatory behaviour through a combination of assault, threatening and stalking offences. In addition to legislation in their own jurisdictions, State and territory law enforcement agencies can rely on the offences found in the Criminal Code which directly address these forms of behaviour.

Cyber-stalking

Cyber-stalking refers to stalking or harassing behaviour carried out using the Internet, interactive and digital technologies or mobile phones. Stalking behaviours can include threats, cryptic messages and sexual innuendo that occur in a frequent and intrusive manner. The usual goal for stalking is to create a sense of fear in the recipient and the motivation is based on control and intimidation.

The key offences in the Criminal Code which relate to cyber-stalking are:

- Section 474.14 – *Using a telecommunications network with intention to commit a serious offence* – This offence is intended to be broad and cover the use of the Internet or another telecommunications network to commit serious offences, for example fraud or stalking. A serious offence is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment. This offence is punishable by the maximum penalty of the serious offence.

- Section 474.15 – *Using a carriage service to make a threat* – This offence is intended to cover threats to kill or cause serious harm that are made over the Internet. A threat to kill is punishable by a maximum penalty of 10 years imprisonment. A threat to cause serious harm is punishable by a maximum penalty of seven years imprisonment.

- Section 474.17 – *Using a carriage service to menace, harass or cause offence* – This offence is intended to cover online conduct that a reasonable person would find to be menacing, harassing or causing offence. This is a broad offence that covers a wide range of conduct. There is no definition in the Criminal Code for the terms 'menace' or 'harass'. This offence is punishable by a maximum penalty of three years imprisonment.

At present, all States and Territories have their own laws which deal with stalking behaviour. Victoria and Queensland have explicitly extended the definition of stalking to include the sending of electronic messages.[2]

Cyber-racism

The Internet is a powerful new means for people with racist ideas, who previously had limited reach through print media, to spread their views particularly in forums used by the general public. While research in regard to cyber-racism is still limited, it is clear that popular social networking sites provide a forum where racist messages and views can reach a wide audience.

The Commonwealth *Racial Discrimination Act 1975* (RDA) makes it unlawful for a person to discriminate against or vilify another person because of that person's race, colour, descent or national or ethnic origin. Section 18C of the RDA makes it unlawful for a person to do an act, otherwise than in private, if the act is reasonably likely, in all the circumstances, to offend, insult,

[2] See *Criminal Code (Stalking) Amendment Act 1999* (Qld) and *Crimes (Stalking) Act 2003* (Vic).

humiliate or intimidate another person or a group because of a person's race, colour, descent or national or ethnic origin. An aggrieved person can lodge a complaint under the RDA with the Australian Human Rights Commission (AHRC). The AHRC can investigate and seek to conciliate an outcome between the parties.

Racism on the Internet was considered in *Jones v Toben* [2002] FCA 1150. In that case, the Federal Court found that a website that denied the Holocaust and vilified Jewish people was unlawful under the RDA. In 2008-2009, 18 per cent of the racial hatred complaints received by the AHRC related to racist material, up from nine per cent in 2007-2008.

On 27 April 2010, the AHRC in association with the Internet Industry Association (IIA) convened a Cyber-Racism Summit to discuss strategies to address cyber-racism. A range of key stakeholders attended, including Government, social networking sites, academics and young people. One of the key themes that emerged was that any strategy to address cyber-racism needs to focus on young people as they are the biggest users of Internet tools.

An initial action following the Summit will be the publication of a summary of safety tools and options available to users of the most popular social media sites, which is currently being compiled by the IIA. This summary information will complement and reinforce the safety features popular social media sites have in place.

Online grooming

Online grooming refers to a range of behaviour that is designed to make it easier for an offender to procure a child for sexual activity. For example, the offender might build a relationship of trust with a child, and then seek to sexualise that relationship (for example, by encouraging romantic feelings or exposing the child to sexual concepts through pornography).

Responsibility for combating child sexual exploitation is shared between the Commonwealth, States and Territories. States and Territories are generally responsible for child sex-related offences occurring domestically (eg within each jurisdiction). Traditionally, the Commonwealth has enacted child sex-related offences occurring across or outside Australian jurisdictions (eg, child sex tourism offences and offences involving the use of the Internet).

In 1995, the Commonwealth first enacted offences targeting the use of a carriage service (eg, the Internet or mobile telephone) for sexual activity with children, including grooming and procuring. These offences were recently enhanced as a result of reforms to Commonwealth child sex-related offences, contained in the *Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010*.

The Act, which entered into force on 15 April 2010, has improved the operation of Commonwealth online grooming offences, including by increasing penalties. The online grooming offence regime 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) – maximum penalty: 15 years imprisonment

- 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) – maximum penalty: 12 years imprisonment

- 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 – maximum penalty: seven years imprisonment.

Exposure to illegal and inappropriate content

The Criminal Code creates offences in relation to online suicide material. Section 474.29A creates an offence for a person to use a carriage service to access, transmit, make available, publish or otherwise distribute material which directly or indirectly:

- 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.

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. This offence carries a maximum penalty of 1,000 penalty units.

Section 474.29B provides a preparatory offence to section 474.29A. Specifically, it creates an offence for a person to possess, produce, supply or obtain suicide related material with the intention that it be used in committing an offence against section 474.29A. This offence also carries a maximum penalty of 1,000 penalty units.

There are a number of reviews currently considering the classification of media content. On 21 December 2010, the Commonwealth Attorney-General and Minister for Home Affairs announced their intention to ask the Australian Law Reform Commission to conduct a review of classification in light of changes in technology, media convergence and the global availability of media content. The Commission is to provide its final report by 9 December 2011.

Identity theft

In the past decade, there has been increasing awareness of the dangers posed by identity crime. Recognition of the threats posed by identity crime has led to a number of measures directed at preventing online identity crime through systematic and whole of government improvements to the national identity management system. The centrepiece of this response is the National Identity Security Strategy (the Strategy), which was endorsed by the Council of Australian Governments in 2005. The 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 (POI) documents
- enhancing the security features on POI 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.

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

The costs to individuals and business from identity crime are significant, with the Australian Bureau of Statistics (ABS) estimating that personal frauds of various kinds cost nearly $1 billion a year, and that half a million Australians have experienced at least one form of identity fraud.[3] Preventing identity crime is also important to reduce the threat of terrorist and other serious criminal activity, which is often founded on the use of false or multiple identities.

The risk of identity theft to children and young people

There is a paucity of data relating to identity theft and children. The ABS survey only covered people aged 15 and over. Other surveys, such as the Office of the Privacy Commissioner (OPC) Survey, most recently conducted in 2007, covered people aged 18 and over.

The ABS Survey found that people aged 25-34 had the highest proportion of people reporting identity theft (4.3 per cent), against 2.1 per cent of people aged 15-24. The OPC Survey showed a similar trend. Only 2 per cent of respondents aged 18-24 had reported incidents of identity theft or fraud in the survey, as compared to 9 per cent for the total population sampled.

It should be noted that these surveys are subject to sampling errors and, when looking at a sub-group of respondents, such as a particular age category, the results must be treated with even greater caution. Results should be viewed as indicative, rather than as outcomes of reliable reporting mechanisms.

Children and young people have a greater tendency than older people to make their personal information freely available on social networking sites and even link such information to a biometric, such as a photograph. Hence, the greatest risk stems from their extensive use of social networking.

There is no immediate economic value to stealing a child's identity. However, once a child turns 18 years of age, their identity becomes valuable as it allows a person to apply for a proof of age card, drivers' licence, passport or credit card. So there is a risk, particularly for teenagers, that criminals will collect personal information and bide their time before using the stolen identity. Some children even publicise personal information about their parents, siblings and friends which also puts other people's information at risk of identity theft.

There have been reports of social networking accounts being compromised by hackers and then used for fraudulent purposes.[4] They have involved the accounts of young people travelling overseas. Hackers purported to be the account holder and wrote to family members, pretending they had been mugged and requesting emergency funds to be transferred overseas.

Children and teenagers can also fall victim to their peers. Online identities can be assumed and used as part of anti-social behaviour such as cyber-bullying. For example, children opening up email accounts in the name of another child to send malicious emails or children hacking into other children's social networking accounts and posting embarrassing or hurtful material.

---

[3] *Personal Fraud, 2007*, ABS Catalogue Number 4528.0.

[4] http://news.ninemsn.com.au/technology/721613/hackers-extorting-facebook-users-with-mugging-tale

In summary, online environments, especially social networking, make children vulnerable to identity crime, both from perpetrators with a 'criminal' intent, and from peers engaging in bullying behaviour.

The Department has released a number of products to advise consumers on protecting against identity theft, including protecting personal information stored online or locally.

Model identity fraud offences

In March 2008, the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General recommended the introduction of specific identity fraud offences and a certificate for victims to assist in re-establishing their credit worthiness. The model offences do not require that a crime, such as theft, fraud, forgery or deception be perpetrated but merely that there is an intention to commit or facilitate the commission of an indictable offence.

Parliament is currently considering the Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008 (the Bill) which would give effect to the model laws. The Bill was passed by the House of Representatives on 23 February 2009 and is currently under consideration by the Senate.

The Bill would insert three new identity crime offences into the Criminal Code:

- dealing in identification information with the intention of committing, or facilitating the commission of a Commonwealth indictable offence, punishable by up to five years imprisonment

- possession of identification information with the intention of committing, or facilitating the commission of, conduct that constitutes the dealing offence, punishable by up to three years imprisonment, and

- possession of equipment to create identification documentation with the intention of committing, or facilitating the commission of, conduct that constitutes the dealing offence, punishable by up to three years imprisonment.

The Bill also contains measures to assist victims of identity crime. The amendments would allow 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.

3 Convention on Cybercrime

The Council of Europe Convention on Cybercrime (2001) (the Convention) is the only multilateral treaty in force that specifically addresses cyber crime. The main objective of the Convention 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.

The Convention requires participating countries to create offences in relation to 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.

Australia announced its intention to accede to the Convention on 30 April 2010. However, further legislative amendments to Australian legislation are required to enable compliance with the Convention, including amendments 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
- require confidentiality in relation to the preservation of, access to and disclosure of stored communications and telecommunications data.

The Department is working closely with government to progress these and other required amendments.

4 Proposal for an Online Ombudsman

The Department notes that the Committee will consider the merits of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues.

The power of an Ombudsman generally lies in his or her ability to investigate complaints and then notify the relevant government agency or the public of the findings. The Department notes that many of the websites an Online Ombudsman would receive complaints about would have no, or only a minimal, presence in Australia. Consideration will need to be given to how an Australian Ombudsman could perform an effective oversight and investigation role in this context.

The Department also notes that there are a range of agencies that deal with complaints about the online environment including ACMA, the AFP, ACCC and the Privacy Commissioner. In assessing the merits of establishing an Online Ombudsman, it will be important to examine how the role of this new body can be clearly delineated from the roles of existing agencies to ensure there is no confusion about where to direct complaints or delays causing by adding another layer to the current system.

Attachment A

SUMMARY OF RELEVANT OFFENCES IN THE CRIMINAL CODE

Part 10.6

Part 10.6 of the *Criminal Code Act 1995* (Cth) contains offences which criminalise the misuse of telecommunications, such as the Internet. The offences relevant to the Committee's consideration of cyber-safety include:

- Section 474.14 – *Using a telecommunications network with intention to commit a serious offence* – This offence is intended to be broad and cover the use of the Internet or another telecommunications network to commit serious offences, for example fraud or stalking. A serious offence is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment. This offence is punishable by the maximum penalty of the serious offence.
- Section 474.15 – *Using a carriage service to make a threat* – This offence is intended to cover threats to kill or cause serious harm that are made over the Internet. A threat to kill is punishable by a maximum penalty of 10 years imprisonment. A threat to cause serious harm is punishable by a maximum penalty of seven years imprisonment.
- Section 474.17 – *Using a carriage service to menace, harass or cause offence* – This offence is intended to cover online conduct that a reasonable person would find to be menacing, harassing or causing offence. This is a broad offence that covers a wide range of conduct. There is no definition in the Criminal Code for the terms 'menace' or 'harass'. This offence is punishable by a maximum penalty of three years imprisonment.
- Sections 474.19 – *Using a carriage service for child pornography material*, Section 474.20 – *Possessing, controlling, producing, supplying or obtaining child pornography for use through a carriage service*, Section 474.22 – *Using a carriage service for child abuse material*, Section 474.23 – *Possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service* – These offences are intended to cover the use, access, distribution, production, supply and distribution of child pornography or child abuse material online. These offences are punishable by a maximum penalty of 10 years imprisonment.

Part 10.7

Part 10.7 of the Criminal Code contains offences which criminalise the misuse of computers. The penalties for these offences range from two to 10 years. A summary of the offences in part 10.7 is as follows:

- Section 477.1 – *Unauthorised access, modification or impairment with intent to commit a serious offence* – This offence is intended to cover unauthorised use of computer technology to commit serious crimes, such as fraud or terrorist offences. A serious offence is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment.
- Section 477.2 – *Unauthorised modification of data to cause impairment* – This offence is intended to cover the unauthorised modification of data on a computer that would impair access to, or the reliability, security or operation of the data. For example, a person who uses the Internet to infect a computer with malware. To fall within Commonwealth jurisdiction, the offence needs to have occurred over a carriage service or involve a

Commonwealth computer or data. This offence is punishable by a maximum penalty of 10 years imprisonment.

- Section 477.3 – *Unauthorised impairment of electronic communication* – This offence is intended to cover cyber-attacks such as denial of service attacks, where a server is inundated with a large volume of data, which is intended to impede or prevent its functioning. This offence is punishable by a maximum penalty of 10 years imprisonment.
- Section 478.1 – *Unauthorised access to, or modification of, restricted data* – This offence is intended to cover unauthorised access to or modification of data held on a computer which is restricted by an access control system. For example, hacking into password protected data. This offence is punishable by a maximum penalty of two years imprisonment.
- Section 478.2 – *Unauthorised impairment of data held on a computer disk* – This offence is intended to cover the unauthorised impairment of data held on a computer disk, credit card or other device used to store data by electronic means. For example, impairment of data by passing a magnet over a credit card. This offence is punishable by a maximum penalty of two years imprisonment.
- Section 478.3 – *Possession or control of data with intent to commit a computer offence* – This offence is intended to cover people who possess programs designed to hack into other people's computer systems or impair data or electronic communications. For example, possessing a program which will enable the offender to launch a denial of service attack against a Commonwealth Department's computer system. This offence is punishable by a maximum penalty of three years imprisonment.
- Section 478.4 – *Producing, supplying or obtaining data with intent to commit a computer offence* – This offence is intended to cover the production and/or supply of data to be used in a computer offence. This offence is punishable by a maximum penalty of three years imprisonment.