SUBMISSION No. 56

Australian Government
Australian Institute of Criminology

Telephone +61 2 6260 9205
Facsimile +61 2 6260 9278
GPO Box 2944
Canberra ACT 2601 Australia

Submission to the Joint Select Committee on Cyber-Safety

Dr Adam Tomison, Director of the Australian Institute of Criminology

Dr Kim-Kwang Raymond Choo, Senior Research Analyst

Dr Russell G Smith, Principal Criminologist and Program Manager

Background

In May 2010, the Joint Select Committee on Cyber-Safety chaired by Senator Dana Wortley launched a new inquiry into the safety of children and young people on the Internet. The Australian Institute of Criminology (AIC) welcomes the opportunity to contribute to the current inquiry.

The AIC has worked closely with the Australian Government Attorney-General's Department (AGD) and a number of key AGD portfolio agencies including the Australian Federal Police (AFP), to undertake research in technology-enabled crime issues. Recent projects undertaken by the AIC in this area include:

- In September 2003, the Australian Institute of Criminology was engaged by the then newly-established Australian High Tech Crime Centre to conduct research into a range of technology-enabled crime issues. This research investigated technology-enabled crime in the context of an evolving international and domestic legal and law enforcement framework, and sought to identify the crime risks which will arise out of the environment in which Australians use information and communications technologies (ICT) in the future. As part of this research, a number of publications were released including a comprehensive review of risks entitled "Future Directions in Technology-enabled Crime: 2007-09" (Choo, Smith & McCusker 2007) and the resource materials on technology-enabled crime (Urbas & Choo 2008).

- In July 2007, the AIC undertook a survey of small, medium and large businesses from a range of industry sectors and from all Australian states and territories during February – April 2008 regarding the prevalence and nature of computer security incidents they had experienced, the areas in which business systems are vulnerable to such incidents and the cost, types and effectiveness of approaches Australian businesses use to prevent them. The study was funded under the Proceeds of Crime Act 2002, which is administered by the Australian Government Attorney-General's Department.

- In November 2007, the Australian Government Attorney-General's Department commissioned the AIC to search for, locate and report on the existing international academic and policy-relevant literature concerning the use of social networking sites for grooming children for sexual purposes, the extent and nature of the problem, and effective ways in which to address it. This research produced a report entitled "Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences" (Choo 2009a) and an article entitled "Responding to online child sexual grooming: an industry perspective" (Choo 2009b). This research was also presented at a number of international conferences and in the media (Australia and Singapore).

- More recently in 2009, the AIC sponsored the 8th Asia-Pacific Regional Conference on Child Abuse and Neglect (APCCAN09) of the International Society for Prevention of Child Abuse and Neglect; the Program included a number of papers on online safety and online sex offending. The Director of the AIC chaired the Conference.

The material in this document is provided by the AIC in response to the Joint Select Committee on Cyber-Safety's Inquiry into Cyber-Safety.

Submission details

1. Introduction

Coyle and Vaughn (2008: 13) explained that '[s]ocial networks and the need to communicate are universal human conditions … [and] communication technologies [generally] help to increase and strengthen social ties'.

Undeniably, ICT including the new media channels (e.g. social networking sites and blogs) have become an important element in our day-to-day activities, and are increasingly popular with children and young people in Australia and overseas. For example, in the "Media and Communications in Australian Families 2007" study commissioned by the Australian Communications and Media Authority, a representative sample of 751 Australian family households with children aged between 8 and 17 were surveyed to gauge media use in the home, how young people divide their leisure time and how parents view their children's use of media and communications technologies. The study found that in relation to the families surveyed, 42% of young people reportedly posted their own material online and 72% of young people aged between 14 and 17 years reported having their own profile on a social networking site (ACMA 2007).

Weaver and Morrison (2008: 97) explained that '[t]he social-networking trend is causing a major shift in the Internet's function and design. While we previously thought of the Internet as an information repository, the advent of social networks is turning it into a tool for connecting people. The mass adoption of social-networking websites of all shapes and sizes points to a larger movement, an evolution in human social interaction'.

The increasingly popularity of social networking sites with children and adults worldwide could also be explained by the fact that:

> social network sites provide simple, inexpensive ways to organize members, arrange meetings, spread information, and gauge opinion. As more systems emerge, there will be greater capacity for groups to organize and participate in collective action, a hallmark of civil society. (Ellison, Lampe and Steinfield 2009: 8).

A more recent online survey commissioned by ACMA (2009) involving 819 respondents (comprising children aged between eight and 17 years and their parents) reported similar observation. The study found that

- 90 percent of respondents aged between 12 and 17 years old reported the use of social networking sites;
- 97 percent of respondents aged between 16 and 17 years reportedly using at least one social networking site; and
- 91 percent and 74 percent of respondents aged between 12 and 17 years old, and 8 and 11 years old reportedly rated the internet as an important aspect of their daily life respectively.

It is concerning however, that 17 percent and 24 percent of respondents aged between 12 and 17 years old, and 8 and 11 years old respectively reported that one of their main reasons for using social networking sites was to make new friends (ACMA 2009). The internet and social networking sites can be and have been abused by cybercriminals and child sex predators to reach out to children and young people, as explained by Choo (2009a).

2. Online risks

Criminologists have argued that crime is most likely to occur with the concurrence of (1) opportunities for crimes to occur (2) the presence of suitably motivated offenders, and (3) the absence of capable guardians and other deterrents to crime. ICT advancement has created an ideal criminogenic environment as there are abundant opportunities, highly motivated offenders, and not a great deal of coordinated and effective regulation. Muir (2005) questioned whether ICT advances have outpaced our understanding of their social impact, particularly involving their negative aspects.

ICT and the new media channels such as social networking sties enable offenders who are motivated by personal sexual gratification to target children and young people individually or collectively. Children and young people are particularly vulnerable to exploitation via ICT and the new media channels because these mediums are attractive to them. Children and young people often use these mediums unsupervised and increasingly have access to portable devices with the capacity for data storage, digital photography and communications such as third generation mobile phones. The types of offences that are relevant to online child exploitation include accessing, sending or uploading child exploitation material; grooming and procuring of children and young people over the internet; possession and publication of child exploitation materials; photographing of filming children and young people for sexual gratification; and the sexual assault of children and young people.

Online child exploitation

Wilson and Jones (2008) noted that the internet facilitates access to child exploitation materials that were once difficult and risky to locate. It is also unlikely that child sexual offenders will shy away from using new technologies to facilitate the process of grooming children for sexual abuse. According to a recent strategic overview published by the Child Exploitation and Online Protection,

> [t]he application of offline grooming techniques is made far easier in such environments, as offenders are able to build a range of contacts and express shared interests and opinions with children who are increasingly used to having the world as their audience in online forums. Equally, as more and more social sites incorporate instant messaging – a medium which facilitates the establishment of private relationships – an increase in reports of grooming in these environments is anticipated (CEOP 2008: 7).

Durkin (1997 cited in Middleton et al. 2006: 590) further identified four ways in which child sexual offenders can exploit the internet:

- trafficking child pornography
- locating children for the purpose of sexual abuse
- engaging in inappropriate sexual communications with children, and
- communicating with other like-minded individuals (i.e. child sexual offenders).

Sexual offenders can also use the internet to locate child-sex tourism operators, to make direct contact with child prostitutes and to mail-order children over the internet (i.e. trafficking in children).

As with all official crime statistics, data compiled by law enforcement, prosecution agencies, the courts and corrections are not indicative of the actual incidence of victimisation. In the case of online child exploitation, major police operations, such as

Operation Ore, have led to a substantial increase in prosecutions in the United Kingdom (from 549 in 2001 to 2,234 in 2003), but even these prosecutions represent only a fraction of offences actually perpetrated against children. It has been argued that even this number has placed an almost intolerable burden on law enforcement and judicial agencies (Harrison 2006).

Victims' reluctance to report sexual abuse is well known and occurs due to a range of factors. These include the intensely personal impact that sexual crimes have on victims (Talbot, Gilligan, Carter & Matso 2002) and the fact that even if incidents are reported officially, not all may result in arrest and prosecution (Wolak, Finkelhor & Mitchell 2005).

The following statistics provide an indication of the continually increasing number of cases that have come to the attention of police in Australia, and the United Kingdom. It is, however, important to note that an increase in the number of online child exploitation cases/arrests may be a result of tighter enforcement rather than an increase in the number of child sex offenders.

Australia

Until 2007, there have been over 130 completed prosecutions for online procuring, grooming and exposure offences in Australia (Griffith & Roth 2007). The number of police investigations into online child exploitation has increased considerably in recent years. Statistics compiled by the Commonwealth Director of Public Prosecutions indicated that in the financial year 2008-2009, there were

- two Summary (Charges) and 18 Indictable (Charges) under Section 474.26 Criminal Code 1995 (Cth) – Using a carriage service to procure persons under 16 years of age' and
- five Summary (Charges) and 15 Indictable (Charges) under Section 474.27 Criminal Code 1995 (Cth) – Using a carriage service to "groom" persons under 16 years of age (CDPP 2010).

More than 150 people were reportedly charged in the financial year 2008-2009 with online child sex exploitation offences (AFP 2010, Millar 2010), and the Commonwealth Director of Public Prosecutions also reported prosecuting an increasing number of offences involving the online exploitation of children in the financial year 2008-09 (CDPP 2010).

United Kingdom

According to statistics compiled by the UK Home Office (2010), there were 315 online child grooming offences recorded in England and Wales in the financial year 2008-09 – an increase of 16 percent from the previous financial year. UK's Child Exploitation and Online Protection Centre further highlighted that online child 'grooming is still the number one offence reported to CEOP, although whereas before this was done primarily via instant messaging, a fast-growing trend is exploiting children through vast, integrated social networking sites' (CEOP 2009).

Sexting

Undeniably, ICT have created a new space in which children and young people can both learn and play. It is a place of both opportunity and risk where they can develop but where they may also become the victims of crime or engage in illegal behaviour themselves. The illegal behaviour that a young person may engage in includes taking or sending explicit images or videos of oneself or others before forwarding the images or videos to others. For example, a study in the United States commissioned by the National Campaign to Prevent Teen and Unplanned Pregnancy found that

- 20% of respondents aged between 13 and 19 years old and 33% of respondents aged between 20 and 26 years old have reportedly electronically sent, or posted online, nude or semi-nude pictures or video of themselves, and
- 15% of respondents aged between 13 and 19 years old who have reportedly sent or posted nude or semi-nude images of themselves claimed they have done so to someone they only knew online (National Campaign to Prevent Teen and Unplanned Pregnancy 2008).

In a recent incident, four boys and one girl from the rural Victorian town of Colac were allegedly 'charged with making child pornography over the filming of a sexual encounter that took place in a school gym' (Whinnett 2010).

Cyberbullying

In recent years, a new form of bullying, including harassment targeting children and young users, has emerged which makes use of ICT and new media channels such as blogs, email, text messaging, chatrooms, mobile phones, mobile phone cameras and social networking sites. Cyberbullying can also include online fights, denigration, impersonation, trickery, and cyberstalking. Reeckman and Cannard (2009) argued that '[t]here are notable differences between cyberbullying and traditional and face-to-face bullying … [as c]yberbullies can remain anonymous'. Thomas also highlighted similar concerns.

> The anonymity provided by the internet introduces a new element: The victim may have no way to identify the bully. Neither parents nor school officials may know how to intervene to stop the harassment. Children may be reluctant to report incidents, for fear their computer privileges will be curtailed (Thomas 2006: 1015).

Australia

- More than a fifth of respondents (aged between 15 and 20 years) in the 2008 youth poll initiated by Senator Natasha Stott Despoja in 1992 reportedly experienced being ‘upset or felt threatened by someone they came into contact with online (Despoja 2008: 13).

- Of the 91 student respondents enrolled in the Youth Unit at Northern Melbourne Institute of TAFE (NMIT), 63% reported experiences of being cyberbullied although only 9% reported being cyberbullied by another NMIT student (Reeckman & Cannard 2009). A significant percent (58%) of the respondents admitted to be a cyberbully.

United States

- The study commissioned by the National Crime Prevention Council (2007) reported similar concerns. Conducted between 2 to 15 February 2006, approximately 46 percent of a nationally representative sample of 824 middle and high school students aged 13 through 17 in the United States reported that they had experienced some form of cyberbullying in the last year.
- In the study by Williams and Guerra (2007), 3,339 youths in Grades 5, 8 and 11 in 78 school sites in Colorado were first surveyed in late 2005, and 2,293 respondents in the original sample participated in a follow-up survey in 65 school sites in 2006. The study found that 9.4 percent of the respondents experienced internet bullying.

The anonymous nature of the internet also allows offender to masquerade as the victim and post fabricated and malicious information online with the intention of stalking, harassing or embarrassing the victim. In a recent case, for example, an individual allegedly ‘engaged in a course of conduct consisting of malicious postings to MySpace, Facebook, Craig’s List and other Internet social sites in which he caused the personal identity information of [the victim] – including her home address – to be publicly displayed. At the time, the indictment says, [the defendant] had been served with a restraining order forbidding contact with [the victim] … [the defendant also] allegedly posed as [the victim] and distributed Web site invitations to visit [the victim’s] residence for sexual gratification’ (US DoJ 2008).

Unlike traditional face-to-face bullying, victims of cyberbullying may find it harder to escape as explained by a young respondent – a student aged between 12 and 20 years in the city of Gothenburg, Sweden – in the study by Slonje and Smith:

> One participant reflected on the impact cyberbullying outside school may have: “I believe that cyberbullying most often can be worse for the victim. Partly because the bullies spend so much energy on the bullying, but also because the bullying takes place outside school, in other words when the victim is at home. Home is usually a sanctuary for most people. But the bullies take this sanctuary away from the victims by cyberbullying them.” (Slonje & Smith 2008: 151).

In the Australian Covert Bullying Prevalence Study (ACBPS) conducted by Edith Cowan University, released by the then Deputy Prime Minister The Hon Julia Gillard

MP in June 2009, a total of 20,832 Australian students aged 8 to 14 years from over 200 schools and 456 school staff were interviewed.

- Sub-study 1: Synthesis of published theoretical and empirical evidence;
- Sub-study 2: Qualitative data (2007) collected from 84 students aged 8 to 13 years;
- Sub-study 3: Quantitative CHPRC data (from existing data sources 2002-2006) collected from 13 330 students aged 8 to 14 years; and
- Sub-study 4: Cross-sectional quantitative national data (2007) collected from 7 418 students aged 8 to 14 years and 456 school staff (Cross, Shaw, Hearn, Epstein, Monks, Lester & Thomas 2009).

The ACBPS found that

- 27% of Year 4 to Year 9 (Australian) student respondents reported being bullied every few weeks or more often overtly, covertly or both during the last term at school;
- 61% of students reported being bullied in any way had also experienced covert bullying (either on its own or in conjunction with overt bullying). Of students who had reportedly experienced covert bullying, 24% had been physically hurt, and 13% had been sent nasty messages on the internet. 53% of student respondents who indicated that they had bullied others had engaged in covert bullying (either on its own or in conjunction with overt bullying);
- 16% of student respondents reported being bullied covertly every few weeks or more often in the term the survey was conducted. Year 5, 6 and 8 student respondents were most likely to report being bullied covertly (18-20%) and those in Year 9 least likely (12%). This form of bullying was experienced slightly more often by girls (18%) compared with boys (15%) and in Government schools (17%) more often than non-Government schools (14%);

Despite the high number of reported incidences of bullying experienced by student respondents in the ACBPS, the study indicated that '[t]he vast majority of Year 4 through Year 9 students had not [reported] experience[ing] cyber bullying, with only 7-10% of students reporting they were bullied by means of technology over the school term' (Cross, Shaw, Hearn, Epstein, Monks, Lester & Thomas 2009: xxiii). This extensive study also found that '[s]lightly higher rates of cyber bullying were found among secondary students and students from non-Government schools [and c]yber bullying was not observed by or reported to as many staff members as other forms of bullying, but was not rare (20%)' (Cross, Shaw, Hearn, Epstein, Monks, Lester & Thomas 2009: xxiii).

Cyberstalking

The wealth of personal information and pictures online (e.g. on popular social networking sites) could potentially be used by individuals and sexual predators to identify, locate, contact, stalk and harass their victims. In a recent study, researchers from Virginia Commonwealth University examined documented cyberstalking cases reported in newspapers between 1999 and 2006 to understand more about victimisation patterns. Of the 61 reported cases of cyberstalking, the researchers found that more than half of the victims and offenders (60 percent) do not have prior relationships (Moriarty & Freiberger 2008). This is, perhaps, due to the ease of offenders locating their victims online. Whitty (2008: 1843-4), for example, had 'argued that the online environment could produce a greater number of stalkers and harasses than offline … [as] people can often be more easily located online. Slonje and Smith (2008: 148) agreed and indicated that 'the opportunity for cyberbullying may increase with age as older pupils more often will have mobile phones or access to the internet'.

The study by Cox Communications (2007) highlighted that people with a public profile are more likely to be bullied and harassed online, and to receive personal messages via email, instant messaging, chat or text messages from strangers when compared with respondents without a public profile. Smith (2007: 2) also reported that '[t]hose who have posted photos of themselves and created profiles on social networking sites are more likely to have been contacted online by people they do not know' and 'girls are significantly more likely than boys to be contacted by someone they do not know when other factors are held constant'.

However, 58 percent of the respondents in the Cox Communications (2007) study did not think that posting personal information and photos on public networking sites was an unsafe practice, 47 percent were not worried about other people using their personal online information in ways they did not want them to, and 49 percent were unconcerned that the posting of personal information online might negatively affect their future.

In the 2006 US-based Youth Internet Safety Survey (YISS-2), the 1,500 youths aged between 10 and 17 years who were interviewed reported frequent exposure to unwanted sexual material, sexual solicitations and harassment online (Wolak, Mitchell & Finkelhor 2006). Some four percent of all young respondents to the survey indicated that people they met online requested nude or sexually explicit photographs of them (Wolak, Mitchell & Finkelhor 2006), and respondents aged between 14 and 17 years were reportedly more likely to receive sexual solicitations online than other age groups (Wolak, Mitchell & Finkelhor 2006).

In the Growing Up with Media survey, 1,588 youths aged between 10 and 15 years were surveyed between August and September 2006 (Ybarra, Espelage & Mitchell 2007). The respondents were required to be able to read English and to have used the internet at least once in the previous six months prior to the survey. The study found the following results:

- Internet harassment or unwanted sexual solicitation
    - 35 percent reported being the victim of either internet harassment or unwanted sexual solicitation.
    - 21 percent reported perpetrating either internet harassment or unwanted sexual solicitation.
- Internet harassment only
    - 34 percent of all youth reported being the victim of internet harassment at least once in the previous year while eight percent reported being targeted monthly or more often.
    - 21 percent reported perpetrating internet harassment of others at least once in the past year and four percent reported doing so monthly or more often.

Although only a minority of the respondents in the Growing Up with Media survey were frequently involved in internet harassment or sexual solicitation as victims or perpetrators, the various associated psychosocial problems (e.g. elevated rates of substance use, involvement in offline victimisation and commission of sexual aggression) highlighted the need for early intervention and prevention programs for this group of young people.

Cyberstalking behaviours include:

- Sending repeated unwanted messages using email and SMS or posting messages on blogs, profiles on social networking sites, etc.
- Ordering goods and services on the behalf of victims, which could potentially result in legal, reputation and financial losses to the victims
- Publicising private information about the victim
- Spreading false information
- Gathering information about a victim online
- Encouraging other individuals to harass the victim
- Unauthorised access into the victim’s computer(s) or internet accounts (e.g. email and social networking site accounts) (Mullen, Pathé & Purcell 2009).

McEwan, Mullen and MacKenzie (2007) highlighted some of the difficulties in drafting anti-stalking legislation. For example, not all of the above mentioned behaviours are criminal. For example, mining for information about a victim online using publicly available information (e.g. profiles on social networking sites and online resumes with addresses and other contact details) is not illegal, nor is posting of messages of a non-threatening nature. However when these “innocuous” ‘activities are repeated over an extended period of time in an unwelcome manner these seemingly inoffensive acts develop into a course of conduct with menacing overtones for the target’, argued McEwan, Mullen and MacKenzie (2007: 208).

3. Responses

The AIC would like to highlight a number of key points that may further inform the Joint Committee’s Inquiry into the safety of children and young people on the Internet.

Public-private partnership

The potential for responding to online risks lies in an effective partnership between the public and private sectors. A legislative approach is useful to keep children safe in the online environment, but it is unlikely that law enforcement alone can cause a noticeable reduction in the online child-grooming statistics, making non-legislative responses crucial in improving internet safety for children (Choo 2009a). The role of public policing agencies is only one, albeit important, part of the overall response to technology-enabled crime (Choo 2009b). 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.

Non-legislative responses include major social networking sites working proactively with law enforcement agencies to protect children and young people against sexual offenders online, and the development of software to locate and identify perpetrators and the distributors of child abuse materials (e.g. the establishment of the Technology Group Against Child Pornography that seeks to evaluate specific and emerging technologies used by sexual offenders in their child exploitation activities in 2006). Popular social networking sites such as Facebook and MySpace should also consider

- offering privacy-friendly default settings such as allowing users to specify who are able to access their profile instead of the default free-for-all settings;
- collaborating with law enforcement and other stakeholders (e.g. not-for-profit groups and schools) to provide training and assistance to help school kids navigate online safety issues; and
- taking a proactive approach in policing their online environment (e.g. including abuse reporting button on social networking sites).

Cyber security awareness raising and educational activities

Technology-enabled crime will continue to evolve into new forms, while continuing to exploit social engineering (as human actors are likely to remain one of the weakest links in attempts to secure systems and networks) and the trusting nature of children and young people. User awareness and education/training are distinct activities, and both are critical in mitigating technology-enabled crime.

Children and young people are generally more technologically savvy and at ease with the use of web 2.0 (e.g. social networking sites) than their parents, teachers and other individuals tasked with taking care of them. The virtual/digital generations are increasingly communicating in ways unfamiliar to adults in virtual venues only dimly grasped by them. It is not surprising that adults are not up-to-date with recent advances in ICT used by the virtual/digital generations and, therefore, also have difficulty in coping with or responding to online risks faced by their children. However, some countries have sought to address this educational need including Australia (e.g. the $3 million national pilot project aimed at addressing cyber bullying in Australian schools announced by the then Deputy Prime Minister The Hon Julia Gillard MP and Minister for Youth, Kate Ellis (Gillard & Ellis 2009)).

Besides focusing preventive strategies on children, parents should also be included in the educational programs. For example, parents should ensure that children and young people are subject, to some degree, to family rules that limit the frequency and their connection time, and be familiar with the communication technologies (e.g. instant messaging programs and social networking sites) to reduce their child's risk behaviour in the longer term. The issue of adult awareness is crucial when it comes to effective action by parents and schools against cyberbullying. Both parents and teachers should be aware of the various types of online risks (including online child grooming) and of what actions can be taken. The ThinkUKnow Australia website (http://www.thinkuknow.org.au/site/index.asp) – a joint effort by the UK Child Exploitation and Online Protection Centre, the Australian Federal Police, Microsoft Australia and the Australian Communications and Media Authority – is one of the recent additions to a list of educational programs designed to educate both parents and children about online dangers. On the website, there are simple-to-follow useful programs for teachers, parents or guardians that explain the different ways in which children are using the internet, give practical advice on how to protect children and provide useful first-warning signs in how the behaviour of young people may change if they are being targeted by offenders.

The internet is a shared community and coordinated efforts are needed by parents, schools, communities, organisations and governments to ensure that a safe online environment is available for children. Funding for educational outreach programs such as promoting safe use of the internet among children (e.g. advising children about the risks associated with meeting online friends) in various media, informing the public of the risks linked to the use of online technologies and conducting educational road shows tailored to the needs of children, parents, teachers and other individuals tasked with taking care of children should be encouraged.

There is also a need for further research to analyse best practices on awareness raising and educational activities from countries such as New Zealand, the United States, the United Kingdom, South Korea, Canada, Japan and other OECD member nations to effectively respond to online risks faced by children and young people. Findings of the research could then be used to support the Australian Government in evaluating the effectiveness of cyber security education and awareness raising programs, and provide the evidence base in implementation of sound strategies.

Need for further research (Online child exploitation)

There is relatively little research on how children and young people or parents cope with or respond to online risks, with efforts devoted to the incidence more than the consequences, coping strategies or long-term effects of exposure to risk; and content risks (e.g. sexually harmful content) and contact risks (e.g. sexually harmful behaviour including online child grooming) (Choo 2009a). Prior research into the causal relationship between possession and use of child exploitation materials, grooming and procuring children for sexual conduct, and actual sexual contact offending has largely been conducted prior to the widespread adoption and use of ICT, in the pre-Internet age. This earlier research has found no firm evidence of a causal link between possession and viewing of child exploitation material and the commission of sexual assault offences involving children. In a leading study prepared for the Department of Justice Canada, Rettinger (2000) found that ‘child and/or adult pornography is a feature of the lives of many pedophiles and other sex offenders, just as it is a feature in the lives of some persons who do not commit sexual offences. Alternatively, some sex offenders do not use pornography of any kind’. Rettinger concluded that ‘there appears to be no strong and consistent evidence that sex offenders are more avid consumers of pornography than other males. A simple, direct causal link between pornography and sexual offending is not supported by the literature.’

Rettinger’s study highlighted some of the limitations in the prior literature:

- Prior research has focused on so-called child pornography, often without precision in its definition. Current usage of the concept of child exploitation material has a different scope and focus than child pornography generally.

- Prior studies have concentrated on the use of child pornography by offenders who committed contact sex offences against children. This ignores those offenders who use child pornography but do not go on to commit offences with children.

- There has been a lack of rigour in some studies with respect to the definition of child pornography, often emphasising commercial pornography when much child pornography is not made available commercially.

- Prior research has often employed qualitative interview methods and there is no way of ensuring that respondents are truthful. Offenders in the criminal justice system may have an interest in downplaying the role of pornography as it may label them as persistent offenders.

Despite this, a number of studies have indicated an association between the use of child exploitation material and contact offending. Law enforcement officials often report this association anecdotally. Perhaps the most well-known study that does suggest a link between the use of child exploitation material and contact offences was the report by the United States Postal Inspection Service which found that some 35 percent of those arrested for possessing child pornography were child molesters (Lanning 1997). A criticism of this study is that the results may be skewed by the way in which the Postal Inspection Service targets its investigations and the sample is restricted to those seeking access to child pornography by mail order.

A study by Marshall (1988) reported that 53 percent of a sample of child sex offenders used child pornography in preparing for offending. Carter et al. (1987) reported that child molesters used child pornographic material prior to and during their offences. By way of contrast, they also reported that pornography was sometimes used to relieve the impulse to commit offences. The possible catharctic effect of the use of child pornography must thus be considered as a limiting factor in relation to contact offending.

An Australian study by Smallbone and Wortley (2001) examined the use of child pornography by child sexual assault offenders. This was conducted for the Queensland Crime Commission and involved 182 respondents. This sample was drawn from the male prison population of persons serving sentences for sexual offences against children. It was found that most respondents (86.4 percent) reported they used adult pornography and ten percent reported having used child pornography. However, most of the study sample of incarcerated males had not used the internet (86 percent) and it cannot be said to be indicative of the offending patterns of those who use the internet to access child pornography.

These three studies all explore the use of pornography by those committing contact offences, it does not investigate the use of pornography by those who use pornography but do not commit contact offences (as noted by Rettinger 2000).

As Taylor and Quayle (2003) have observed, much of the research into the use of child exploitation material pre-dates the internet, which has made child exploitation material freely available (Taylor 1999). This gap in research concerning the impact of the internet is important because of the special characteristics of technology-enabled crime. Among these characteristics are the general intelligence and social status of offenders, the compulsive or addictive nature of some offender engagement, the heightened role of fantasy for the offender, and the level of networking among communities of offenders.

Further research is needed in order to understand the causal relationship between the uses of child exploitation material obtained online and actual contact offending. In particular, it is important to understand how different types of material are used during the grooming process, and how these might lead to the commission of sexual offences against children.

Need for further research (Cyber security research)

It is important that government policies do not lag behind new technology trends, causing unnecessary restrictions on the use of new technology, or conversely, by an absence of regulation, to enable the proliferation of new forms of online exploitation and harm. The speed of change and developments in ICT has, and does, require therefore the regular review of policies to ensure their relevance and their ability to capture significant new ICT trends. Clearly, regular assessment and briefings with the ICT sector and regulatory bodies are necessary to ensure that developments in ICT are well understood and can be used to refine policy strategies.

The challenge for the public and private sectors is to design technologies that are robust, in the sense that their legitimate use is minimally constrained, but their illegitimate use prevented or discouraged. This of course will not always be possible. There is a continuing need to identify and prioritise current and emerging risk areas, develop and validate effective technical measures and mitigation controls; and fund technical research to find ways to mitigate existing and new online risks.

The Australian Government has invested significantly in law enforcement responses, education, science, and R&D. It is to be hoped that there will be further investment to enable Australian security researchers to play a more significant role in designing state of the art security tools that can be deployed in the online environment, and help to position Australia as an international leader in cyber security.

References

Australian Communications and Media Authority (ACMA) 2007. *Media and communications in Australian families 2007*. http://www.acma.gov.au/WEB/STANDARD/pc=PC_310893

Australian Communications and Media Authority (ACMA) 2009. *Click and connect: Young Australians' use of online social media (02: Quantitative research report)*. http://www.acma.gov.au/webwr/aba/about/recruitment/click_and_connect-02_quantitative_report.pdf

Australian Federal Police (AFP) 2010. *Annual report 2008 - 2009*. http://www.afp.gov.au/media-centre/publications/~/media/afp/pdf/a/afp-annual-report-2008-2009.ashx

Carter DL & Prentky RA & Knight RA & Vanderveer PL & Boucher RJ 1987. Use of pornography in the criminal and developmental histories of sexual offenders. *Journal of interpersonal violence* 2: 196-211

Child Exploitation and Online Protection (CEOP) 2008. *Strategic overview 2007-2008*. http://www.ceop.gov.uk/downloads/documents/CEOPStrategicOverview2008.pdf

Child Exploitation and Online Protection Centre (CEOP) 2009. Behind every statistic, a young victim. *Press release* 20 May. http://www.ceop.gov.uk/mediacentre/pressreleases/2009/ceop_20052009.asp

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. http://www.aic.gov.au/publications/current series/rpp/100-120/rpp103.aspx

Choo K-KR 2009b. *Responding to online child sexual grooming: An industry perspective*. Trends & issues in crime and criminal justice no. 379. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current series/tandi/361-380/tandi379.aspx

Choo K-K R, Smith RG & McCusker R 2007. *Future directions in technology-enabled crime: 2007-09*. Research and public policy series no. 78, Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx

Commonwealth Director of Public Prosecutions (CDPP) 2010. *Annual report 2008 - 2009*. http://www.cdpp.gov.au/Publications/AnnualReports/CDPP-Annual-Report-2008-2009.pdf

Cox Communications 2007. *Teen internet safety survey, wave II*. http://www.cox.com/TakeCharge/includes/docs/survey_results_2007.ppt

Coyle CL & Vaughn H 2008. Social networking: Communication revolution or evolution?. *Bell Labs technical journal* 13(2): 13–18

Cross D, Shaw T, Hearn L, Epstein M, Monks H, Lester L & Thomas L 2009. *Australian covert bullying prevalence study (ACBPS)*. Perth, WA: Child Health Promotion Research Centre, Edith Cowan University

Despoja NS 2008. *Youth Poll 2008*. http://www.natashastottdespoja.com/cms_resources/Youth%20Poll%20May%202008.pdf

Ellison NB & Lampe C & Steinfield C 2009. Social network sites and society: current trends and future possibilities. *ACM interactions* January + February issue: 6–9

Gillard J & Ellis E 2009. $3 million for national pilot to increase cyber-safety in schools. *Media release* 2 August. http://www.deewr.gov.au/Ministers/Gillard/Media/Releases/Pages/Article_090803_074909.aspx

Griffith G & Roth L 2007. Protecting children from online sexual predators. *NSW Parliamentary Library briefing paper* no. 10/07. Sydney: NSW Parliamentary Library. http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/3043E49AB3F4ABF9CA2573530006F989/$File/Dealing%20with%20Online%20PredatorsFINAL&INDEX.pdf

Harrison C 2006. Cyberspace and child abuse images: a feminist perspective. *Affilia: journal of women and social work* 21(4): 365–379

Lanning L V 1997. The sex offender – "A profile." In Agenda for action: A conference on the sexual exploitation of children, 21-23, Ontario Police College. Nov 2-7, 1997. Conference Final Report. Toronto: Solicitor General of Canada

Marshall W L 1988. The use of sexually explicit stimuli by rapists, child molesters, and nonoffenders. *Journal of sex research*. 25: 267-88

McEwan TE and Mullen PE and MacKenzie R 2007. Anti-stalking legislation in practice: Are we meeting community needs? *Psychiatry, psychology and law* 14(2):207–217

Middleton D et al. 2006. An investigation into the applicability of the Ward and Siegert pathways model of child sexual abuse with internet offenders. *Psychology, crime and law* 12(6): 589–603

Millar P 2010. Internet risk to children on rise. *The age* 21 May. http://www.theage.com.au/technology/technology-news/internet-risk-to-children-on-rise-20100520-vowh.html

Moriarty LJ & Freiberger K 2008. Cyberstalking: Utilizing newspaper accounts to establish victimization patterns. *Victims and offenders* 3(2–3): 131–141

Muir D 2005. *Violence against children in cyberspace*. Bangkok: ECPAT International

Mullen PE, Pathé M & Purcell R 2009. *Stalkers and their victims (2nd ed)*. Cambridge: Cambridge University Press

National Campaign to Prevent Teen and Unplanned Pregnancy 2008. *Sex and tech: results from a survey of teens and young adults*. http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf

National Crime Prevention Council 2007. *Teens and cyberbullying*. http://vocuspr.vocus.com/VocusPR30/Temp/Sites/2623/57d586957e1d404ca0f0d5f6d0b18996/Cyberbullying-Exec%20Summary-FINAL.doc

Reeckman B & Cannard L 2009. Cyberbullying: a TAFE perspective. *Youth studies Australia* 28(2): 41 – 49

Rettinger L J 2000. *The relationship between child pornography and the commission of sexual offences against children: A review of the literature*. Ottawa: Department of Justice Canada http://www.justice.gc.ca/eng/pi/rs/rep-rap/2000/rr00_5.pdf

Slonje R & Smith PK 2008. Cyberbullying: Another main type of bullying?. *Scandinavian journal of psychology* 49(2): 147–154

Smallbone S & Wortley R 2001.Child sexual abuse: Offender characteristics and modus operandi. *Trends & Issues in crime and criminal justice* no 193. Canberra: Australian Institute of Criminology http://www.aic.gov.au/documents/1/D/7/%7B1D7F5F5E-2B6A-44CA-B2CB-9B330AE888A8%7Dti193.pdf

Smith B 2007. Law 'lags behind' cyber bullying. *The age* 17 May. http://www.theage.com.au/news/national/law-lags-behind-cyber-bullying/2007/05/16/1178995236283.html

Talbot T, Gilligan L, Carter M & Matson S 2002. *An overview of sex offender management*. Silver Spring, MD: United States Center for Sex Offender Management

Taylor M 1999. The nature and dimensions of child pornography on the Internet Combating child pornography on the Internet conference, Vienna. www.asem.org/Documents/aaconfvienna/pa_taylor.html

Taylor M & Quayle E 2003. *Child pornography: an internet crime*. Hove: Brunner-Routledge

Thomas T 2001. Supervising child sex offenders in the community: some observations on law and practice in England and Wales, the Republic of Ireland and Sweden. *European journal of crime, criminal law and criminal justice* 9(1): 69–90

UK Home Office 2010. *Crime in England and Wales 2008/09*. http://www.homeoffice.gov.uk/rds/pdfs09/hosb1109vol1.pdf

United States Department of Justice (US DoJ) 2008. KC man indicted for cyberstalking. *Media release* 9 May. http://kansascity.fbi.gov/dojpressrel/pressrel08/cyberstalking050908.htm

Urbas G & Choo K-KR 2008. *Resource materials on technology-enabled crime*. Technical and background paper no. 28. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current series/tbp/21-40/tbp028.aspx

Weaver AC & Morrison BB 2008. Social networking. *IEEE computer* 41(2): 97–100

Whinnett E 2010. Colac students to face child porn charges after sex in gym filmed on mobile phone. *News.com.au* 18 April. http://www.news.com.au/technology/colac-students-to-face-child-porn-charges-after-sex-in-gym-filmed-on-mobile-phone/story-e6frfro0-1225855009565

Whitty MT 2008. Liberating or debilitating? An examination of romantic relationships, sexual relationships and friendships on the Net. *Computers in human behavior* 24(5): 1837–1850

Wilson D & Jones T 2008. In my own world: A case study of a paedophile's thinking and doing and his use of the internet. *The Howard journal of criminal justice* 47(2): 107–120

Wolak J, Finkelhor D & Mitchell K 2005. *Child-pornography possessors arrested in internet-related crimes: findings from the National Juvenile Online Victimization Study*. Alexandria, VA: National Center for Missing and Exploited Children

Wolak J, Mitchell K & Finkelhor D 2006. *Online victimization of youth: five years later*. Alexandria, VA: National Center for Missing and Exploited Children.

Ybarra ML, Espelage DL & Mitchell KJ 2007. The co-occurrence of internet harassment and unwanted sexual solicitation victimization and perpetration: associations with psychosocial indicators. *Journal of adolescent health* 41(6) Supplement 1: S31–S41