Trends & issues in crime and criminal justice

No. 379 July 2009

Australian Government
Australian Institute of Criminology

Responding to online child sexual grooming: an industry perspective

Kim-Kwang Raymond Choo

Foreword | *As the internet and other forms of information and communications technology advances, opportunities for child sexual offenders and other financially-motivated cybercriminals to sexually exploit children will increase. Official statistics here and overseas indicate the number of investigations and prosecutions remain small but are increasing rapidly. This paper discusses non-legislative measures to address the issue of online child exploitation, particularly child grooming. Using knowledge of offending patterns and encouraging effective coordination and collaboration by government and private-sector entities enables law enforcement to develop strategies to address the problem. Social-networking sites are currently working with law enforcement agencies to protect children through the removal of known offenders from their websites. The financial services industry is assisting to eliminate offenders' access to financial-payment systems. These types of joint and transnational initiatives reduce opportunities for, and the detection of, online child exploitations. Although it is well recognised that educational preventative strategies are required to raise awareness amongst young people and children, it is less clear what would be effective in encouraging them to report suspicious or explicit contact or material to parents and authorities.*

Judy Putt
General Manager, Research

Recent advances in information and communications technologies (ICT) have enabled adults with an inappropriate sexual interest in children to establish contact with them, to develop relationships and to groom potential victims for sexual abuse (Krone 2005). Of particular relevance to this discussion is the potential for individuals to make contact with children for sexual gratification or to groom them for subsequent meetings during which sexual activity may be undertaken. The dangers of online child exploitation have received widespread attention. Online child (sexual) grooming offences have been introduced in a range of countries, including Australia, although there are jurisdictions that have yet to introduce legislation to criminalise online child exploitation including online child grooming.

While a legislative approach is useful to keep children safe in the online environment, 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. This paper reviews and discusses various non-legislative measures, such as initiatives by those that operate social-networking sites and the financial services industry, to deal with the issue of online child exploitation, particularly online child grooming.

Online child (sexual) grooming

Child grooming, a premeditated behaviour intended to secure the trust and cooperation of children prior to engaging in sexual conduct, is a process that commences with sexual predators choosing a location or target area likely to be attractive to children (AIC 2008). A process of grooming then commences during which offenders take a particular interest in their child victim to make them feel special with the intention of gaining their trust. As trust is developed between the child victim and the offender, offenders then seek to desensitise child victims to sexual conduct by introducing a sexual element into the relationship.

All this is able to be achieved with ease in the online environment. Large numbers of children now use the internet. In one US study, 55 percent of surveyed young people aged between 12 and 17 years were found to have used online social-networking sites (Lenhart & Madden 2007). Sexual offenders are also using the internet to locate children for criminal purposes, including the creation of pornography, sex tourism, making contact with child prostitutes and establishing contacts for subsequent sexual assault.

Online sexual solicitations by adults targeting children are of great concern. The anonymous nature of the internet allows offenders to masquerade as children in cyberspace to gain the confidence and trust of their victims over a period of time before introducing a sexual element into the online conversation and eventually arranging a physical meeting. The lack of visual cues in cyberspace that may assist child victims in making judgments about the suitability, trustworthiness and sincerity of others with whom they communicate also facilitates the grooming process for offenders.

Personal information online

Part of the grooming process involves eliciting personal information from children. This can be for purposes of sexual gratification itself, use in evading detection, or use in other illegal activities, such as cases involving fraud and deception. In online child grooming cases, offenders have been known to use the internet to gather private information on their child victims to further their criminal pursuit with little risk of interdiction. Search engines are an invaluable tool that can be abused to locate publicly available information concerning children and their activities. Private information about a target child can also be obtained by engaging the victim in conversation in public domain sites such as Internet Relay Chat (IRC) rooms and online gaming forum sites. Another effective way of obtaining personal information and pictures of children is to browse personal profiles set up on-site.

Recent technological advances also enable offenders to disguise their identities and prevent the source of their communications from being discovered by law enforcement. The use of cryptography, steganography and anonymising protocols make the task of tracking communications difficult for police and regulators alike.

The extent of online child grooming

The extent to which social-networking sites and IRC rooms are used for child grooming is considerable. A recent cybercrime survey in the United Kingdom estimated that 850,000 cases of unwanted online sexual approaches were made in IRC rooms during 2006 and that 238 offences of meeting a child following sexual grooming were recorded (Fafinski 2007). In the US Youth Internet Safety Survey conducted in 2006, the 1,500 young people 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). In the Growing Up With Media survey, 35 percent of the 1,588 young people aged between 10 and 15 years who were surveyed reported being the victim of either internet harassment or unwanted sexual solicitation (Ybarra, Espelage & Mitchell 2007).

Official crime statistics report increasing numbers of cases of online sexual abuse being recorded by police and coming before the courts, with a number involving grooming carried out in social-networking sites. In Australia, Griffith and Roth (2007) reported that there have been over 130 completed prosecutions for online procuring, grooming and exposure offences to date.

In the United Kingdom, it appears that the number of police investigations into online grooming has increased considerably in recent years, with 322 offences recorded in 2006–07 (Nicholas, Kershaw & Walker 2007). The Child Exploitation and Online Protection Centre in the United Kingdom receives an average of 10 reports a month concerning children between the ages of eight and 11 years, the majority of which relate to online grooming (UK CEOP 2007).

In the United States, the number of annual reports of online child exploitation (including online child grooming) made to the National Center for Missing and Exploited Children through its CyberTipline increased from 4,560 in 1998 to 76,584 by the end of 2006 (NCMEC 2007b). In 2006, there were 6,384 reports of 'online enticement of children for sexual acts'. The statistics relating to the category of online enticement of children for sexual acts show a substantial increase in the 707 reports made in 1998. This increase is due partly to the fact that there is now a mandatory obligation on internet service providers (ISPs) to report child-abuse materials on their systems to the National Center for Missing and Exploited Children. A call has been made for this reporting obligation to be extended to include mobile phone carriers, social-networking websites and web-hosting companies (United States House of Representatives Committee on Energy and Commerce, Republicans 2007: 5).

Non-legislative responses

Fighting online child exploitation is clearly a multidimensional challenge that requires effective coordination and collaboration on the part of a wide range of government and private-sector entities. This was recently emphasised at a hearing of the US Commission on Security and Cooperation in Europe on 27 September 2007, also known as the Helsinki Commission (Specht 2006). The Helsinki Commission noted that tracking child-abuse materials peddlers around the globe requires better international cooperation.

The difficulties faced by Australian law enforcement agencies investigating online child exploitation cases are compounded when the suspect is located abroad or when the sites are hosted overseas. As most online environments are commercially owned and operated, there is an imperative for organisations to respond to corporate and shareholder interests. Such interests should not, however, neglect the need to provide a safe and secure environment for users, particularly children. Business interests, therefore, need to devote resources both to maximising profit as well as minimising opportunities for systems to be used for illegal activities.

> Technology convergence will continue as a business driven requirement, with rapid changes and developments, requiring of stakeholders an equally fast response and collaboration in providing new safety options (European Commission Information Society and Media Directorate-General 2007: 36).

This paper reviews and discusses various non-legislative measures such as initiatives by those that operate social-networking sites and the financial services industry to deal with the issue of online child exploitation.

Initiatives by social-networking sites

Various industry bodies and corporations have recognised their responsibilities to ensure that the online environment is both safe and secure for users. Social-networking sites such as MySpace and Facebook have been proactive in working with law enforcement agencies to protect children against sexual offenders online.

MySpace, for example, works with local police and investigators regarding user activity and interfaces with law enforcement agencies at local, state and federal levels. MySpace personnel have met with law enforcement officials from around the world to find out how MySpace can enhance its cooperation with law enforcement and increase user security. MySpace has created streamlined procedures for law enforcement agencies and officials to obtain critical data that can be used to aid in investigations. It published a law enforcement guide to inform law enforcement agencies of these procedures and outline how police officers can work with MySpace regarding subpoenas and requests for information. This guide has been broadly distributed to agencies around the United States and in other countries. In addition, MySpace created a one-page guide for easy reference for officers. It runs an around-the-clock hotline to receive and respond to law enforcement queries in both emergency and non-emergency cases. The MySpace safety team interfaces directly with law enforcement and helps agencies discover how MySpace can be helpful in their investigations (Nigam 2007).

In some countries, legislation requires the operators of social-networking sites to remove offenders from sites. In the United States, for example, s. 7 of the *Stop the Online Exploitation of Our Children Act 2006* requires site operators to remove offenders from social-networking sites in certain circumstances. Collaboration between MySpace and the state of Florida has reportedly resulted in the deletion of about 2,000 locally known sex offenders from MySpace (Kierkegaard 2008). More recently, MySpace reportedly provided the Connecticut Attorney General with the names of 90,000 registered sex offenders who have been identified and blocked from the social-networking site over the past two years (Schonfeld 2009).

Role of financial services industry

As child-abuse materials often involve payment (although this may not always be the case), one effective strategy used to identify offenders is to monitor online payments made to those who provide illegal content to users for a fee, and/or to eliminate offenders' access to financial-payment systems. It is also possible to deregister companies that facilitate the production, purchase and sale of child exploitation materials online. US representative, Ed Whitfield, Chairman of the House Energy and Commerce Subcommittee on Oversight and Investigations, observed that:

> [l]ike most Americans, I was shocked to learn that commercial child pornography over the Internet is a multi-billion dollar industry. Because child pornography sites often use credit cards and other electronic tools to process payments from pedophiles, banks and credit card companies are uniquely positioned to cut off the flow of money to these sites and shut this illicit trade down (Whitfield 2006: unpaginated).

In March 2006, the US-based Financial Coalition Against Child Pornography was launched by US Senator Richard Shelby, Chairman of the Senate Banking, Housing, and Urban Affairs Committee to eradicate commercial child-abuse materials over the internet by 2008 (Shelby 2006).

The Prevention Working Group of the Financial Coalition Against Child Pornography (2007: 1), comprising major financial processors and internet service companies, identifies best practice associated with stopping the distribution and sale of child-abuse materials over the internet and assists 'other Coalition members in evaluating their respective procedures for detecting commercial child [abusers] and preventing commercial child [abusers] from obtaining access to services offered by Financial Coalition members'.

Financial institutions have recognised their responsibility to not knowingly contributing to illegal acts such as allowing their customers to pay for child-abuse materials. The Association of Banks in Singapore, for example, announced in January 2007 that:

> its nine merchant acquiring and credit card issuing member banks (ABN AMRO Bank NV, Bank of China Limited, Citibank Singapore Limited, DBS Bank Ltd, The Hongkong and Shanghai Banking Corporation Limited, Maybank, OCBC Bank, Standard Chartered Bank and United Overseas Bank Limited) have banded together to work with the major payment card providers in Singapore (including American Express, JCB, MasterCard and Visa) to help combat child pornography on the Internet (ABS 2007: unpaginated).

Under another joint initiative, Microsoft and the International Centre for Missing and Exploited Children have linked with over 30 financial institutions worldwide, including credit card companies, to develop a system that will monitor and report online commercial transactions involving crimes against children. Microsoft is also a partner in the Global Campaign Against Child Pornography, which facilitates and coordinates the efforts of international law enforcement agencies, individuals and organisations to fight online child exploitation by creating an international child-abuse materials monitoring and oversight system and developing and promoting systems for identifying the victims of child abuse. Such joint public–private initiatives build public awareness of the problem of online child exploitation and discourage other organisations from placing advertisements on websites that promote or host child-abuse materials.

Financial institutions can also be involved in the development of robust authentication technologies (eg age-related verification technologies) to restrict children from accessing adult sites or sites that host materials deemed inappropriate for children.

Online reporting and monitoring systems

Online reporting and monitoring systems are important tools in containing online child exploitation. On the Virtual Global Taskforce website (http://www.virtualglobaltaskforce.com/), for example, visitors are able to easily report child-abuse exploitation matters to law enforcement agencies by clicking on the 'Report Abuse' button.

The use of reporting hotlines provides individuals with an alternative to reporting to law enforcement agencies, as many people are reluctant to report illegal content directly to the police. Instead, they may prefer to report illegal activities to civilian hotlines. Hotlines are therefore an important intermediary, passing reports of illegal content on to the appropriate bodies for action.

The International Association of Internet Hotlines, founded in 1999, is substantially funded by the Safer Internet Plus Programme of the European Commission. The Association coordinates a global network of 30 member hotlines in 27 countries. These hotlines monitor activities on the internet and allow members of the general public to report illegal internet content such as child-abuse materials.

Once reports are made to hotlines, they are confidentially reviewed to determine their location on the internet and whether the content is likely to be illegal under local legislation. Relevant cases are then able to be referred to law enforcement agencies or ISPs for further action. James E Finch, Assistant Director of the Cyber Division of the FBI, has observed that probes of child-abuse websites almost always span multiple jurisdictions and usually extend beyond the borders of the United States (Specht 2006). As the referral website may originate in a country other than that in which the hotline is situated, the International Association of Internet Hotlines network facilitates international cooperation, exchange of information and expertise among hotlines in different countries.

In the case of Ireland, for example, in 2006 no report received by the Hotline referred to child-abuse materials located in Ireland. All cases proved to be hosted or distributed form outside the jurisdiction (Internet Service Providers Association of Ireland 2007).

Referrals are forwarded to collaborating hotlines where the offensive content is being hosted. Due to the sensitive nature of passing potentially illegal material to other hotlines around the world, it is paramount that this cooperation is based on transparency and the ability to be able to trust each partner. For example, the Canada-based Cypertip.ca hotline reports that:

> on average, the U.S. National Center for Missing and Exploited Children's cyber tip line receives 700 to 1,100 reports per week. The cyber tip line reviews 75,000 to 100,000 images/videos a week, forwarded from U.S. law enforcement (Province of Manitoba nd: 1).

A number of difficulties arise when referrals are made between countries due to the differences that exist in national legislation relating to online child exploitation (eg age of consent and lack of legislation to criminalise online child exploitation). For example, physical sexual contact involving a minor aged 17 years might be illegal in one country but legal in others. Without consistency in legislation, it is difficult to arrange extradition and to carry out enforcement activities across borders.

However, despite these differences, there have been a number of successful arrests made as a result of online reports lodged with hotlines. Despite these successes, there is no room for complacency. There is, as suggested in a recent report by the European Commission Information Society and Media Directorate-General (2007), a need to review the hotline model in view of the emerging technologies and the increasing number of reports being received. Issues include reviewing whether and how the hotlines can adjust to different and much higher volumes of reports, whether full use is being made of data collected by the hotlines and finally, determining whether or not it is possible for hotline networks such as the International Association of Internet Hotlines to facilitate the creation of a single blacklist of addresses of known illegal websites so that international ISPs and mobile providers can block access to them.

Investigative tools

The involvement of the ICT industry in the development of computer forensic packages that can be used for online child-exploitation investigations is becoming increasingly important as the use of ICT increases and evolves.

Law enforcement, security researchers and organisations could all contribute to a safer online environment for the young by developing tools to locate and identify perpetrators and distributors of child-abuse materials. One such example is the establishment of the Technology Coalition Against Child Pornography in 2006, which seeks to evaluate specific and emerging technologies used by sexual offenders in their child-exploitation activities.

Other examples include LexisNexis Risk and Information Analytics Group's Advanced Investigative Solution, which was launched in June 2007. The Advanced Investigative Solution is designed to help law enforcement agencies locate and monitor non-compliant sexual predators. It seeks to leverage critical information while linking analysis, mapping and alerts needed to rapidly identify and locate sexual predators. The solution, integrating both the company's Advanced Sex Offender Search technology and Enterprise Data Fusion System, enables law enforcement to identify and locate registered sexual offenders and non-compliant sexual offenders who fail to register their most current address as required by law. The company also recently announced a joint initiative with Sentinel, a company specialising in online verification, to enable the detection and identification of sexual predators on social-networking sites such as MySpace.

The Child Exploitation Tracking System, developed by Microsoft and housed in the Canada-based National Child Exploitation Coordination Centre, has reportedly been adopted by various international law enforcement agencies.

In Australia, the collaboration between computer science researchers from the

University of South Australia's Enterprise Security Management Laboratory and law enforcement officers from South Australia Police's Electronic Crime Section has resulted in the development of several investigative tools designed to assist SA Police in their online child-exploitation investigations. For example, the Zero Skills Analysis Program is said to 'improve the identification of electronic evidence of crimes relating to terrorist activity, child-abuse materials, counterfeiting and identity fraud, by allowing police officers without specialist IT training to conduct analysis in the field' (UniSA 2006: unpaginated). The Communication Analysis Tool is designed to capture electronic communications to a computer, flagging emails or other data that relate to cyberstalking (UniSA 2006). This tool can also be used in investigating online child grooming cases.

The Australian Federal Police (AFP) is also an active partner in the recently established Internet Commerce Security Laboratory—a joint venture between the University of Ballarat, Westpac Banking Corporation, IBM Australia and the Victorian Government—to develop technologies to combat technology-enabled crime including online child exploitation (Quinn 2008).

Despite the controversy surrounding the use of surveillance tools—such as keylogging tools, spyware and Trojan programs—by law enforcement agencies, they can be useful in the investigation of online child exploitation matters. One of the many popular venues used by child sexual offenders during their grooming process is IRC rooms. Surveillance software that allows the collection and analysis of data from IRC rooms can be useful to both parents and investigators. The eavesdropping tool developed by Camtepe, Krishnamoorthy and Yener (2004) is one such example. The tool reportedly collects data from any selected channel in the IRC room by logging all messages in the room without human intervention. The data collected are then analysed to locate hidden communities and communication patterns within the room.

Educational programs

Children, child sexual offenders and criminals involved in online commercial child exploitation are generally more technologically savvy and at ease with the use of web 2.0 than their parents, teachers and other individuals tasked with taking care of them. Children and 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. Some countries have sought to address this educational need.

Livingstone and Haddon (2007) also highlighted the importance of the role that parents play in mediating children's internet use, which is lacking in a number of countries. To counter this problem, the Safety, Awareness, Facts and Tools website (http://www.saftonline.org/), provides step-by-step instructions for non-computer literate parents and guardians on how to use various web applications that children may be using (eg MSN Messenger and Bebo). This includes instructions on how to establish a personal profile, share videos, add friends and share photographs. School administrative staff, parents and guardians can also download materials on internet-safety legislation, how to implement an acceptable-use policy in the school, how to install local filtering and monitoring systems and how to locate tips for online safety.

Children also need to be educated with respect to the consequences of their online activities such as making and sending pornographic or otherwise harmful images of themselves over the internet or mobile phones, posting intimate pictures or personal information on social-networking sites, blogs and other internet websites and going out on blind dates with 'friends' whom they have only met or known online. Other risky online behaviours, such as participating in chats where the content is sexually loaded or causes discomfort, should be discouraged.

The issue of adult awareness is crucial when it comes to effective action by parents and schools against online child exploitation. Both parents and teachers should be aware of the various types of online risks and of what actions can be taken. It is also important for parents to recognise that children may be reluctant or hesitant to inform their teachers, parents or guardians and probably adults in general, about potentially dangerous activities they encounter online out of a fear of having limits placed on their use of the internet or mobile phones.

Educational outreach programs should, arguably, include educating children about the need to inform their teachers, parents or guardians should they be harassed or threatened online; and parents about taking a proactive approach in advising their child about online risks without having to resort to threatening to limit the use of the internet or mobile phones.

An important part of ensuring the vigilance of both children and parents will be to teach them how they can help prevent such crimes. Example initiatives include the NetSafe website (http://www.netsafe.org.nz/index.php) and the 'ThinkUKnow Australia' website (http://www.thinkuknow.org.au/site/index.asp). The latter is a joint partnership between AFP, Microsoft Australia and the Australian Communications and Media Authority designed to help teachers, carers and parents educate children about safety and encourage them to think before they act online.

Conclusion

As the internet and other forms of ICT continue to advance, the opportunities for child sexual offenders and other financially-motivated cybercriminals to sexually exploit children will increase. A multidimensional response to combat online child grooming is likely to offer the greatest benefits. This

Dr Kim-Kwang Raymond Choo is a research analyst with the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Judy Putt, General Manager, Research, Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

ISSN 0817-8542 (Print)
1836-2206 (Online)

GPO Box 2944
Canberra ACT 2601, Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government

Project no. 147

should focus on effective coordination and collaborative activities among governments, law enforcement agencies, professionals such as teachers and health workers, and other private organisations.

Partnerships between public-sector law enforcement and regulators, and private-sector agencies, will continue to be a guiding principle of online child-exploitation crime policing in the future. For the public sector, partnerships will result in increased reporting of child-exploitation matters to police, more timely sharing of information, sharing equipment for processing digital evidence, better preservation of evidence, avoidance of duplicated effort, reducing costs and bidirectional training of investigators.

References

All URLs were correct at 4 June 2009

Association of Banks in Singapore (ABS) 2007. Singapore banks join global battle against child pornography. *Media release* 17 January. http://www.abs.org.sg/cms/images/archives/press/17%20Jan%2007_Final%20Media%20Release%20on%20Singapore%20Banks%27%20Battle%20Against%20Child%20Pornography.pdf

Australian Institute of Criminology (AIC) 2008. *Online child grooming laws*. High tech crime brief no. 17. Canberra: AIC. http://www.aic.gov.au/publications/htcb/htcb017.html

Camtepe SA, Krishnamoorthy MS & Yener B 2004. A tool for internet chatroom surveillance, in Hsinchun C et al (eds), Proceedings of the IEEE international conference on intelligence and security informatics, Tucson, Arizona, 10–11 June. *Lecture notes in computer science* 3073: 252–265

European Commission Information Society and Media Directorate-General 2007. *Safer internet and online technologies for children: summary of the results of the online public consultation and 20–21 June 2007 Safer Internet Forum Report*. Brussels: European Commission Information Society and Media Directorate-General

Fafinski S 2007. *UK cybercrime report*. https://www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf

Financial Coalition Against Child Pornography 2007. *Internet merchant acquisition and monitoring best practices for the prevention and detection of commercial child pornography*. http://www.occ.treas.gov/ftp/release/2007-81a.pdf

Griffith S 2007. Keep kids e-safe: a community effort in Sugar Land, Texas. *The police chief* 74(4). http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1158&issue_id=42007

Griffith G & Roth L 2007. Protecting children from online sexual predators. *NSW parliamentary library briefing paper* no. 10/07. Sydney: NSW Parliamentary Library

Kierkegaard S 2008. Online child protection: cybering, online grooming and ageplay. *Computer law and security report* 24(1): 41–45

Krone T 2005. Queensland police stings in online chat rooms. *Trends & issues in crime and criminal justice* no. 301. http://www.aic.gov.au/publications/tandi2/tandi301.html

Lenhart A & Madden M 2007. *Social networking websites and teens: an overview*. Washington DC: Pew Internet and American Life Project

Livingstone S & Haddon L 2007. *What do we know about children's use of online technologies?* http://www.lse.ac.uk/collections/EUKidsOnline/Reports/ReportD1.1FullversionCover.pdf

Internet Service Providers Association of Ireland 2007. *4th report of the ISPAI www.hotline.ie service*. http://www.hotline.ie/report2006/index.html

National Center for Missing and Exploited Children (NCMEC) 2007. *CyberTipline annual report totals*. http://www.cybertipline.com/en_US/documents/CyberTiplineReportTotals.pdf

Nicholas S, Kershaw C & Walker A 2007. *Crime in England and Wales 2006/07*. London: Home Office

Nigam H 2007. Safety on MySpace. *The police chief* 74(3). http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1140&issue_id=32007

Province of Manitoba nd. *Child pornography legislation*. http://www.gov.mb.ca/asset_library/en/newslinks/ChildPornographyLegislation.JS.doc

Quinn A 2008. Leading the charge on technology-led policing. *Platypus magazine* 100: 9–11

Schonfeld E 2009. Thousands of MySpace sex offender refugees found on Facebook. *Techcrunch* 3 February

Specht M 2006. More global effort needed to fight sex crimes against children. *USINFO current issues* 28 September

Shelby RC 2006. Shelby leads fight against child pornography. *Media release* 15 March

United Kingdom Child Exploitation and Online Protection (UK CEOP) 2007. Most wanted special edition. *E-bulletin issue* 13 November

United States House of Representatives Committee on Energy and Commerce, Republicans 2007. *Sexual exploitation of children over the internet: a staff report prepared for the use of the Committee on Energy and Commerce*. Washington, DC: House of Representatives. http://republicans.energycommerce.house.gov/108/ News/01032007_Report.pdf

University of South Australia (UniSA) 2006. SAPOL and UniSA join forces to combat crime. *Media release* 7 April. http://www.unisa.edu.au/news/2006/070406.asp

Whitfield E 2006. Bank, credit card company efforts to combat child porn examined. *Media release* 21 September. http://whitfield.house.gov/news/press.aspx?id=153

Wolak J, Mitchell K & Finkelhor D 2006. *Online victimization of youth: five years later*. http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=2530

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