Australian Government
Australian Institute of Criminology

# Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences

Kim-Kwang Raymond Choo

AIC Reports
Research and Public Policy Series 103

# Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences

*Kim-Kwang Raymond Choo*

**AIC** Reports
Research and
Public Policy Series
103

**www.aic.gov.au**

ISSN 1836-2060 (Print)
1836-2079 (Online)
ISBN 978 1 921185 86 1 (Print)
978 1 921532 33 7 (Online)



Project no. 147

Published by the Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Tel: (02) 6260 9200
Fax: (02) 6260 9299
Email: front.desk@aic.gov.au
Website: http://www.aic.gov.au

Please note: minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

**Disclaimer**: This research report does not necessarily reflect the policy position of the Australian Government.

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **http://www.aic.gov.au**

# Foreword

Advances in technology have provided individuals with unparalleled opportunities to communicate efficiently and in real time. At the same time, the community has been exposed to a wide range of criminal activities, one of which involves the online exploitation of children. The potential for individuals with an inappropriate sexual interest in children to establish online contact with them and groom them for sexual abuse represents a very real threat to the safety of children in the technological age.

The grooming of children for sexual abuse is a premeditated behaviour that commences with sexual offenders choosing a location or target area likely to be attractive to children. Social networking sites, in particular, have become an important element in the child grooming process. These technologies, popular with the digital/virtual generation, allow offenders to make contact with children and even masquerade as children in cyberspace to secure their trust and cooperation. As trust is developed, offenders seek to desensitise child victims to sexual conduct by introducing a sexual element into the relationship.

Social networking sites… have become an important element in the child grooming process.

In November 2007, the Australian Institute of Criminology (AIC) was commissioned by the Attorney-General's Department to search for, locate and report on the existing 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 report brings together a number of aspects of the research that the AIC undertook in 2008. It reviews recently published academic and policy-relevant research on the misuse of online social networking sites and other forms of communications technologies by sexual predators to groom children for sexual conduct. Information is also provided on the extent and nature of the problem including some available statistical information.

The report begins by defining 'online child grooming' and identifying ways in which emerging technological changes may be exploited to facilitate and commit online child grooming. The implications of these developments are then assessed in terms of their impact on policing, policymaking and legislation. Suggestions are also made for responding effectively to these developments – a task that will entail a whole-of-government approach and a closer working relationship among government, those involved in developing

new digital technologies and creating the infrastructure in which they operate, and the end users (including parents, children and educators).

Awareness and understanding of the threats of online child exploitation will continue to be a vital component of the fight against online child grooming both in Australia and overseas. The report concludes by highlighting the need for a comprehensive research effort where a better understanding of online child exploitation, particularly online child grooming issues, is needed. Specific research is needed to develop insight into the online child grooming offending cycle and to explore the behaviour of online groomers who target children. The research effort will inform policy and policing strategies aimed at curbing the continuing evolution of online child exploitation.

**Judy Putt**
**General Manager, Research**
**Australian Institute of Criminology**

# Contents

# Figures



# Tables

# Acknowledgements

This report is based on research funded by the Criminal Justice Division of the Australian Government Attorney-General's Department. The author would like to thank Dr Russell G Smith, Dr Judy Putt and Diana Nelson at the AIC as well as staff of the Criminal Justice Division of the Attorney-General's Department for comments on earlier drafts of the report. Thanks are also extended to the staff of the JV Barry Library at the AIC for their assistance in sourcing some of the relevant literature.

# Executive summary

## Introduction

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. Of particular concern are so-called 'social networking' technologies in which participants can post information and then receive responses at a later time (such as email, newsgroups, usenet, bulletin boards and blogs), or instant messaging services in which communications can be carried out in real time between individuals (such as internal relay chat (IRC) rooms and voice over internet protocol (VoIP)). Broadband services now also enable still and moving images to be shared as archived material or in real time using video streaming of files.

Research has indicated that social networking internet sites are being used extensively by children and that some communications are of an improper and illegal nature, in which personal information is gathered to facilitate financial fraud as well as for use in establishing relationships with children for purposes of sexual gratification.

The 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. The research began on 5 November 2007 and took approximately 10 weeks.

### *Terminology and definitions*

This report uses the definitions set out in ss 474.26 and 474.27 of the *Criminal Code Act 1995* (Cth) to define 'online child grooming' for the purposes of the discussion. The stated ages of 18 for offenders and 16 for children constitute the primary age-limited scope of the discussion, rather than the age restrictions included in the definition of 'paedophile' contained in the American Psychiatric Association's *Diagnostic and statistical manual of mental disorders* (1994).

In relation to the nature of 'communications' sent from offenders to children, the discussion focuses primarily on internet-based social networking sites, although some consideration is given to other forms of electronic communications, especially those involving mobile and wireless technologies.

### *Limitations*

The report canvasses international material published in English since January 2000, located by searching various academic databases. It reviews recently published academic and policy-relevant research on the misuse of online social networking internet sites by sexual predators to groom children for sexual conduct. The research focuses on any evidence of the extent and nature of the criminal threat and the measures being undertaken by Australia and other countries to deal with this problem. Information is provided on the extent and nature of the problem including any statistics that are available, and background information on how academics, industry and policymakers in Australia and other countries view effective ways in which to address it.

# The nature of online grooming

## *The psychopathology of child sex offenders*

Individuals who have sexual fantasies involving children or erotic attractions towards children have been present in society throughout history. Surveys have found that almost two-thirds (62%) of the general male population report sexual fantasies about young girls, while surveys of university students have found that almost one-quarter (21%) acknowledge being sexually attracted to children on occasions (Briere & Runtz 1989 cited in Gee, Devilly & Ward 2004). Surveys of clinical psychiatric patients have found that up to one-third of offenders with mental disorders report having either deviant fantasies involving children or deviant sexual activities (Langevin, Lang & Curnoe 1998).

Pathological sexual 'interest' in children has been explained using various theoretical models, one of which argues that offenders seek relationships with children due to a fear of relationships with adults, as relationships with children are deemed less threatening by perpetrators (the social skills deficit model of Emmers-Sommer & Allen 1999 cited in Olson et al. 2007).

## *The nature of online grooming*

Children have been found to be vulnerable to adult sexual predators because their development of social skills is not yet complete, making them less likely to pick up relevant cues such as inappropriate remarks that predators may make during conversations. Children with low self-esteem, lack of confidence and naivety are more at risk and more likely to be targeted by offenders. Sexually curious adolescents who are often easily aroused are also more willing to take risks than less curious children, thus making them a target for predators.

## *The child grooming process*

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. 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.

## *The attractions of new technologies for children*

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 the young people surveyed aged between 12 and 17 years were found to have used online social networking sites (Lenhart & Madden 2007). Another study estimated that 70 percent of all teenagers in the United States currently visit social networking sites on a monthly basis and, by 2011, 84 percent of online teens in the United States will use social networking each month (eMarketer 2007).

Social networking through blogging, instant messaging, IRC rooms and short message services all enable children to communicate with friends quickly, effectively and ostensibly with confidentiality. Other communications technologies such as email, VoIP and mobile phones can also be used in the grooming process. Acronyms and other non-linguistic signs (so-called 'emoticons') are often used to accelerate the writing process, and many of these are used to represent sexual content.

## *The attractions of new technologies for sexual predators*

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. 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. Another emerging risk relating to online child exploitation is 'rape' crimes that take place in online gaming or virtual worlds. These forms of virtual crimes can potentially cause real psychological, social and financial harms to their victims, particularly children.

### *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 chat 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 sites such as MySpace, Facebook and Friendster.

In a recent Teen Internet Safety Survey conducted in the United States of children aged between 13 and 17 years with internet access, 71 percent indicated that they had established an online profile and 47 percent had an internet profile that was public and viewable by anyone (Cox Communications 2007). In the Media and Communications in Australian Families 2007 study of 751 Australian families, it was found that approximately 70 percent of girls aged between 14 and 17 years, and 50 percent of boys, had a personal profile on MySpace or other similar sites, and approximately one in eight respondents aged between 14 and 17 years reported posting their videos online (ACMA 2007a).

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 grooming

### *Victimisation survey data*

The extent to which social networking sites 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 chat rooms during 2006 and that 238 offences of meeting a child following sexual grooming were recorded. 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). In the Survey of Children's Use of the Internet, which was carried out between December 2005 and January 2006, 19 percent of the 848 students aged between nine and 16 years in 21 Irish schools indicated that they had been harassed, upset, bothered, threatened or embarrassed by someone when chatting online, while seven percent reportedly met someone in real life after knowing them on the internet and 24 percent of these indicated that the person who had introduced themselves as a child on the internet turned out to be an adult (Webwise 2006).

### *Official crime statistics*

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

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 2007a).

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 pornography 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.

### *Case studies*

To provide an indication of how child grooming occurs and the penalties that have been imposed on convicted offenders, a series of nine case studies is provided. These have been taken from authorised law reports or official websites of relevant government agencies. On the basis of these cases, it appears that offenders use various types of technologies to facilitate their grooming activities, and often carry out their conduct over months before they arrange a physical meeting. A number of the cases involved undercover police pretending to be children to obtain evidence against offenders, a procedure that has created difficulties during court proceedings in some jurisdictions. Offenders have also raised the so-called 'fantasy defence', claiming that their actions were an expression of fantasy and not indicative of real intentions (Smith, Grabosky & Urbas 2004). Such a defence has been successful in some cases in the United States, thus creating an additional difficulty for prosecutors.

## Victim profiles

A number of studies have sought to determine the demographic characteristics of the victims of sexual abuse, including the victims of internet-related exploitation such as online grooming. Research has also sought to establish the harmful consequences of exploitation and abuse, many of which endure throughout adulthood.

Victims of both offline, conventional sexual abuse and online sexual abuse come from all walks of life in terms of social class, geographic area of residence, and ethnic and cultural background.

In terms of age and sex, most sexual assault victims are pubertal girls, most often aged between 13 and 17 years. Preschool children of both sexes have also been victims of abuse. Victims of online sexual exploitation are more likely to be female than the victims of other internet-related problems.

There is clear evidence in the academic literature that sexual abuse during childhood creates long-term problems for those who have been victimised. Many exhibit serious mental health problems as well as behavioural disorders and addictions. This occurs not only with children who experience offline sexual abuse, but also online exploitation.

Prior research has found conflicting evidence of the relationship between sexual victimisation in childhood and subsequent sexual offending in adulthood. There is no research that specifically examines whether victims of online grooming are more or less likely to become perpetrators themselves, than is the case with other victims of sexual exploitation.

Some research has found that the impact of grooming on child victims is exacerbated if pornography is involved as this can make incidents more enduring in the minds of victims. Davidson (2007), for example, explained that children are re-victimised each time their image is accessed, with images on the internet forming a permanent record of abuse.

## Offender profiles

Offenders are a heterogeneous group and as noted in a 2006 US hearing investigating the sexual exploitation of children over the internet, several sexual offenders 'were true pillars in their respective communities, including … lawyers and teachers' (Whitfield n.d.: unpaginated). Individuals arrested in several recent online child exploitation cases in Australia, for example, have included former police officers, teachers and a former prosecutor.

Offenders are often known acquaintances or family members of the children whom they abuse and may have known their victims in real life prior to using the internet and other communications technologies to further their grooming activities. One study found that in 85 to 95 percent of child sexual abuse cases, the perpetrator was someone the child knew and depended on.

In relation to the age of offenders, prior research shows that sexual offences against children can be committed by both adults and juveniles. A relatively high proportion of online sexual offenders are juveniles and this proportion appears to be increasing.

In terms of recidivism, a significant percentage of sexual offenders do not have prior criminal histories involving offences against minors, or even non-sexual offences. However, many juvenile sexual offenders do continue their sexual offending into adulthood.

Prior research has shown that crimes relating to pornography of all types were likely to involve lone offenders, typically adult males, rather than offenders acting in concert. Persons committing sexual offences against children tend to be inadequate in their social functioning and diverse in their psychopathology, often involving neurotic and compulsive behaviours. Apart from individual personality characteristics, child sexual offenders carry out a range of patterns of offending, often involving multiple etiological pathways to child sexual abuse.

A number of studies have demonstrated that offenders convicted of sex crimes against children are at heightened risk of being stigmatised and ostracised by other inmates during periods of incarceration and are at increased risk of sexual and other violent victimisation while in prison. This raises the need for specialised forms of treatment for such offenders, which not only prevent them from being harmed while in custody, but also can lead to reduced rates of recidivism on release.

Supervision and rehabilitation of sexual offenders, particularly child sexual offenders, is a difficult and demanding process that requires appropriate education, training and a degree of devolved autonomy.

## Legislative responses

To keep children safe in the online environment, international conventions such as the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse have been introduced to deal with child exploitation offences. Countries such as Australia, Canada, the United States and the United Kingdom have also introduced online child grooming offences.

Most jurisdictions within Australia now have legislation in place that criminalises online child grooming for the purposes of sexual contact. In jurisdictions with no specific online child grooming legislation, Commonwealth legislation can, in certain circumstances, be used to prosecute offenders. The fact that an adult pretends to be a child to establish contact with the victim is not an impediment to prosecution as child grooming can be viewed as an act preliminary to commission of a sexual offence. This is clarified in some legislation.

Legislation that seeks to regulate the behaviour of sexual offenders on release from custody, such as sex offender registration and community notification, has also been introduced in several countries such as the United States.

Several countries have introduced internet filtering regimes that seek to restrict internet users from accessing online social networking sites and websites that host potentially objectionable materials such as child exploitation and racial vilification materials.

Several countries such as Syria, Malaysia and China have introduced internet filtering regimes to restrict

their internet users from accessing online social networking sites and websites that host potentially objectionable materials. The extent of internet filtering varies among countries and regions. However, internet filtering is not limited to Asian and Middle Eastern countries. In the United States, for example, the Children's Internet Protection Act (CIPA) was enacted as part of the Consolidated Appropriations Act of 2001 by Congress in December 2000 and mandates the installation of internet-filtering software to block access to materials that are obscene, child pornography or harmful to minors at schools and libraries receiving federal funds for internet access. Shortly after the CIPA was enacted, a number of non-governmental organisations (NGOs) filed a lawsuit challenging the Act. The challenge was upheld initially, but on 23 July 2003, the Supreme Court of the United States upheld the provisions of the CIPA.

In Australia, the Restricted Access System Declaration 2007 came into effect on 20 January 2008, and places obligations on all content service providers to check that individuals accessing restricted content provided in Australia are at least 15 years of age for MA15+ content or 18 years of age for R18+ content. These restrictions apply only to content hosted either in Australia or provided from Australia.

It is not an easy task for regulators to restrict access to all potentially objectionable materials online, as the range of such content to be filtered out, blocked or banned is extensive. There is a need for the continued development of software to trace, analyse and block websites hosting or disseminating online child exploitation and other potentially objectionable materials.

It is important to note the different statutory definitions of age that are relevant for child exploitation offences in various countries. Ages of consent to sexual activity and ages used to delimit the scope of child pornography offences differ from country to country.

In addition to these jurisdictional differences regarding statutory ages, there are jurisdictions that have yet to introduce legislation to criminalise online child exploitation. A recent report by the International Centre for Missing and Exploited Children found that 95 countries did not have legislation that criminalises child pornography, while 27 countries did not provide for computer-facilitated child exploitation offences at all. The lack of online child grooming legislation in some countries could impede police investigations and prosecutions, as it may be impossible to extradite an offender identified in child grooming matters from countries with no online child grooming offences.

There is a need for concerted law enforcement and international legislation to combat online child exploitation. Countries such as Australia, Singapore, the United Kingdom and the United States have a relatively comprehensive legislative framework in place to deal with online child grooming but, until the process of harmonisation of laws and sanctions is more advanced, disparities within and among countries will continue to create risks.

## Non-legislative responses

Fighting 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. Various industry bodies and corporations have recognised their responsibilities to ensure that the online environment is both safe and secure for users.

### *Initiatives by social networking sites*

Social networking sites such as MySpace have been proactive in working with law enforcement agencies to protect children against sexual offenders online. Terms of use on social networking sites prohibit users from abusing the sites for activities such as harassment of other users and dissemination of objectionable materials. Users who violate these terms may have their accounts deactivated and in situations of a criminal nature, may be reported to appropriate law enforcement agencies.

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.

## *Role of financial services industry*

Because child pornography invariably involves payment, 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.

An example of such an initiative is the US-based Financial Coalition Against Child Exploitation. Under this arrangement, 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. Such initiatives build public awareness of the problem of online child exploitation and can assist in discouraging other organisations from placing advertisements on websites that promote or host child exploitation materials. Financial institutions can also be involved in the development of robust authentication 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. 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 onto the appropriate bodies for action.

Networks of reporting hotlines operate internationally, within Europe and in countries such as the United Kingdom, the United States and Canada. Once reports are made to hotlines, they are confidentially reviewed to determine the 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. On average, the National Center for Missing & Exploited Children's CyberTipline in the United States receives 700 to 1,100 reports per week and reviews 75,000 to 100,000 images/videos a week, which are forwarded to law enforcement agencies.

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. 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. Despite these differences, there have been a number of successful arrests made as a result of online reports lodged with hotlines.

Suggestions have been made regarding the 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 determining whether it is possible for hotline networks 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 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 pornography. One such example is the

establishment in 2006 of the Technology Coalition Against Child Pornography, which seeks to evaluate specific and emerging technologies used by sexual offenders in their child exploitation activities.

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 South Australia Police in their online child exploitation investigations. One such tool is the Communications Analysis Tool. Although it is designed to capture electronic communications to a computer – flagging emails or other data that relate to cyberstalking – the tool can also be used to investigate online child grooming cases.

## *Social network analytical tools*

Any individual can create multiple online identities or have multiple avatars (virtual representations of themselves) and be a member of more than one social networking site at any one time. Social network analytical tools such as mapping tools can be extremely useful for law enforcement investigators when establishing virtual relationships and connections between sexual offenders and their potential victims, understanding these relationships and connections, and analysing their implications in online social networking sites. Such techniques can also be used to facilitate the extraction of the hidden relationships among child sexual offenders in the social networking sites through user interactions.

The future will see the need for investigative and social network analytical tools designed for law enforcement to be validated and accredited by international standard bodies to ensure that the results obtained using such tools can be used in judicial proceedings. Governments might also need to consider whether it is necessary to either introduce new legislation, or to amend existing legislation, so that evidence garnered through the use of surveillance tools such as keylogger, spyware and Trojan programs is admissible.

## *Internet filtering*

The increasing amount of potentially objectionable material online underscores the need for internet filtering and parental control technologies.

Content classification and filtering systems, developed to control access to undesirable content online, include rating systems designed to confer values on content based on certain criteria. Filtering systems are designed to enforce certain predetermined filtering policies and to evaluate, according to those policies, whether a user can or cannot access specified material.

One of the oldest and more commonly used internet filtering techniques is based on proprietary uniform resource locator (URL) collections. Each URL is associated with a specific content category. When a webpage is requested, the classifier checks its address in the database in search of its category. With the definition of the category, the filter can block or release access to the site, according to the policy of internet use configured by the organisation, individual or ISP.

Internet filtering software can be broadly categorised into server-side filtering systems and client-side (or user-side) filtering systems. In server-side filtering systems, the filtering or content-rating software is installed on the servers of internet content providers or ISPs. In client-side filtering systems, the responsibility for blocking potentially objectionable materials is shifted away from internet content providers or ISPs to individuals as the software is installed on personal computers.

## *Rating systems*

Effective regulation of internet and gaming content through the use of rating systems requires coordination at regional, national and international level. The Pan-European Game Information age rating system is one such system. It uses a voluntary self-regulated framework to promote the safe use of video games. The Pan-European Game Information, established in 2003, is designed to help European parents make informed decisions when buying interactive games and to ensure that minors are not exposed to games that are unsuitable for their particular age group.

Although technologies such as content classification and filtering systems on their own cannot solve problems of online child exploitation, regulators and the general public can benefit from deploying these technologies to restrict or deny children and young people access to known sites containing potentially objectionable materials, online social networking sites, IRC rooms or games that promote sexual behaviour or contain sexual references.

## *Reforms*

There is, arguably, a need for continued support from both the public and private sectors to develop and enhance existing technological tools such as internet filtering and content-rating software for use in tracing, analysing and blocking websites hosting potentially objectionable materials. For example, the design of client-side internet filtering and content-rating software should be user-friendly and easy to use by the average individual.

Programs to inform and educate the general public, particularly parents and school staff, of the choice of technological tools available should also be in place. There is a need to develop robust age identification and verification systems that can restrict or deny access to children and young people to known sites containing potentially objectionable or adult material.

## *International task forces*

As policing child sexual exploitation continues to cross many jurisdictions, establishing international collaboration among international law enforcement agencies will assist in identifying perpetrators, leading to charges and success in prosecutions. The use of police task forces is likely to provide an effective means of sharing intelligence among law enforcement agencies in multiple jurisdictions. The Virtual Global Taskforce is one example of how law enforcement agencies from various countries work together to fight online child exploitation.

The multidisciplinary Internet Taskforce for Child Protection on the Internet established in March 2001 is another example of public–private partnership that brings together government, law enforcement, children's agencies and the internet industry in the fight against online child exploitation.

In the United States, the Innocent Images International Task Force, which became operational in June 2004, comprises law enforcement officers from Europol and 17 countries including Australia. In Australia, the Australian Federal Police's Online Child Sex Exploitation Team performs an investigative and coordination role within Australia for multijurisdictional and international online child sex exploitation matters.

## *Specialist units*

Specialist behavioural units are another invaluable resource for law enforcement. In the United States, the Behavioural Analysis Unit provides the Federal Bureau of Investigation (FBI) with behavioural-based investigative and operational support by applying case experience, research and training to complex and time-sensitive crimes, typically involving acts or threats of violence, which include crimes against children. Other behavioural analysis units are the Child Exploitation and Online Protection Centre in the United Kingdom and the National Center for Missing & Exploited Children Child Victim Identification Program in the United States.

## *Training in computer forensics*

With increased digitisation of information, the future will see an increased likelihood of digital content being a source of a dispute or forming part of underlying evidence to support or refute a dispute in judicial proceedings. Better-educated criminals are likely to explore alternatives to hiding data over the internet. These include storing data on password-protected file-sharing websites, email accounts and less reputable content providers hosted in countries with lax cybercrime legislation. Criminals are also likely to leverage the use of anti-forensic tools and information-hiding tools, including steganography, to further impede collection of evidence.

In online child exploitation cases, evidence is likely to be stored on hundreds or thousands of computers and various ISPs and IRC room servers located in various jurisdictions. This requires computer forensic investigators and incident handlers to have in-depth knowledge of computer forensic principles, guidelines, procedures, tools and techniques, as well as anti-forensic tools and techniques.

Increasingly, forensic analysis of computers for law enforcement purposes is being undertaken by well-organised groups of computer forensic examiners working in government facilities or private sector workplaces such as consulting practices.

Only specially trained and authorised computer forensic examiners should process and examine electronic evidence, as evidence not retrieved by a computer forensic expert may result in the reliability of the evidence itself being called into question and potentially being ruled inadmissible in court. To ensure that the results of computer forensic examinations can be used in judicial proceedings, accreditation of individual examiners and validation of computer forensic analysis tools are desirable.

### *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 (e.g. social networking sites) than their parents, teachers and other individuals tasked with taking care of them. This serves as a reminder to parents that even by closely monitoring what their children are doing online may not be sufficient to prevent some kinds of exploitation from occurring, especially if parents have limited ICT skills.

Research has found that parents often do not have, or do not know if they have, software on their computers to monitor where their child goes online and with whom they interact. Many parents are also unable to correctly decipher the meanings of several common internet acronyms.

Children also need to be educated about 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 chat rooms 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.

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 educating parents about taking a proactive approach in advising their child about online risks without resorting to threatening limiting the use of the internet or mobile phones.

## 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. The use of social networking sites is, and will continue to remain, popular with the digital and virtual generations. Children and young people will continue to communicate in ways unfamiliar to adults such as through the use of acronyms and non-linguistic signs in virtual venues. This makes the task of regulation all the more difficult for technologically limited guardians of the internet.

Serious concerns have been expressed about the ways in which new technologies might be exploited for online child grooming and this report provides some indications of the ways in which emerging technological changes may be exploited to facilitate and commit online child grooming. Key risk areas include:

- the use of anonymising protocols, password authentication techniques, encryption techniques and steganographic techniques
- trafficking child pornography, particularly movie files and real-time images that are facilitated through the use of broadband services
- using search engines to locate children for the purpose of sexual abuse online
- risks relating to virtual 'rape' of minors perpetrated in online games or virtual worlds
- obtaining personal information regarding children online by sexual offenders and fraudsters alike.

It can reasonably be anticipated that online child grooming prosecutions involving multiple

jurisdictions will continue to arise in the years ahead along with an increasing demand for new strategies in terms of how law enforcement agencies investigate, prosecute and prevent online multijurisdictional child grooming crimes.

A multidimensional response to combat online child grooming is likely to offer the greatest benefits. This 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.

It has been suggested that international law enforcement agencies and academia should consider sharing practices and research information, and establishing an information repository for research purposes. This would enable law enforcement agencies and researchers to have better data on child grooming to analyse trends and characteristics.

Further studies are necessary to develop insights into the online child grooming offending cycle and to investigate whether victims of online child grooming will eventually progress to become perpetrators of online child grooming in their adulthood. Further research is also needed to explore the behaviour of online groomers who target children, and the link/boundary between non-contact online sexual abuse of children and internet offenders' propensity for contact abuse. Research is also needed to investigate the behaviour and motivations of those using extreme sexual pornographic images depicting adults.

# Introduction

Digital technologies and the internet have provided a means of enabling people of all ages to communicate efficiently using a range of electronic procedures. These include conventional communication channels such as email, newsgroups, usenet, bulletin boards and blogs in which information is posted or sent and responses are received at a later time. More recent services allow communication to take place in real time with instantaneous responses. These include instant messaging services, IRC and VoIP services such as Skype. In addition, wireless communications including mobile phones and other wireless networked devices can be used to engage in real-time communication. Where such technologies are used for social, as opposed to business, communication, the activities are collectively known as 'social networking' and the internet sites through which they are undertaken are known as 'social networking sites'.

According to Muir (2005), advances in ICT have outpaced our understanding of their social impact, particularly involving their negative aspects. One particular area of risk concerns the exploitation of children by adults and their grooming for sexual activity. Understanding the way in which children use the internet and how sexual predators seek to communicate with children online provides an important means of preventing adults from grooming children and preventing illegal sexual abuse from taking place. This study seeks to inform policymakers about the misuse of internet-enabled social networking sites such as Bebo (http://www.bebo.com/), Facebook (http://www.facebook.com/), Friendster (http://www.friendster.com/) and MySpace (http://www.myspace.com/) for online grooming of children for sexual purposes.

Recent research by Gartner has indicated that the global active membership of Facebook, one of the more popular social networking sites, is expected to reach 200 million by the end of 2008 (Valdes 2007). Although social networking can be used for legitimate forms of communication, opportunities also exist for those with criminal intent to infringe legal and regulatory controls. Some of the primary risks include:

- using social networking sites as vehicles to direct unsuspecting users to phishing sites or to distribute malware (malicious code). For example, one recent incident involved the installation of Zango Cash Toolbar in video clips hosted on several MySpace users' profile pages (Websense Security Labs 2006)
- using social networking sites as vehicles for the distribution of politically motivated propaganda or other offensive content such as racial vilification material and insensitive statements about particular ethnic groups. Examples include material posted on internet sites by terrorist groups or other ideologically or politically motivated organisations

- obtaining personal information from social networking sites to facilitate other crimes such as identity theft and context-aware phishing. Such information can be used to identify or profile a particular user and thus increase the yield of future phishing attacks (Choo & Smith 2008).

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. Networking can also be a means of seeking out children for use in creating child abuse materials. The recent Teen Internet Safety Survey, Wave II by Cox Communications, suggested that a significant number of 13 to 16-year-old users of social networking sites had divulged personal information such as email addresses, dates of birth and phone numbers to complete strangers (Cox Communications 2007). This, potentially, increases other risks of exploitation.

Using desk-based research principally involving online resources and academic databases, this report:

- reviews recently published academic and policy-relevant research on the misuse of the internet by sexual predators to groom children for sexual conduct, focusing on any evidence on the extent and nature of the criminal threat and the measures being undertaken by Australia and other countries to deal with this problem. The emphasis of this review is on the misuse of social networking sites (e.g. Bebo, MySpace, Facebook and Friendster) and other uses of the internet for online grooming of children
- provides information on the extent and nature of the problem, including any statistical information that is available, and background information on how academics, industry and policymakers in Australia and other countries view effective ways in which to address it. This report avoids overlap with research already undertaken by the Attorney-General's Department.

The research began on 5 November 2007 and took approximately 10 weeks to complete.

# Terminology and definitions

There is a lack of consistency in the terminology used to describe online child grooming in the literature concerning online child exploitation. A number of terms are used – including 'online enticement of children' (NCMEC n.d.), 'internet luring of children' (s 172.1 of the Criminal Code, Canada), 'sexual grooming' (Singapore Ministry of Home Affairs 2007a) and 'internet seduction of children' (Quayle & Taylor 2003) – to describe online child grooming. Each has slightly different connotations.

O'Connell (2003) defined 'sexual grooming' as:

> [a] course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes (O'Connell 2003 cited in Craven, Brown & Gilchrist 2006: 288).

Howitt (1995) defined 'grooming' as:

> the steps taken by paedophiles to 'entrap' their victims and is in some ways analogous to adult courtship (Howitt 1995 cited in Craven, Brown & Gilchrist 2006: 288).

Both of these definitions use the term 'paedophile' to describe perpetrators and people accused of initiating sexual activity with children (Craven, Brown & Gilchrist 2006). As noted by Green (2002) and Kingston et al. (2007), to fall within the diagnosis of paedophilia in the current *Diagnostic and statistical manual of mental disorders* each of the following three criteria must be satisfied:

- the individual must have over a period of at least six months, experienced recurrent intense sexually arousing fantasies, sexual urges or behaviours involving sexual activity with a child or children (generally aged 13 years or younger)
- the individual must have acted on these sexual urges, or the sexual urges or fantasies cause marked distress or interpersonal difficulty
- the individual must be of at least 16 years of age and at least five years older than the child or children in the first criterion.

The use of the term 'paedophile' in the definition of child grooming places an important limitation on the scope of the phenomenon. For example, an individual responsible for initiating sexual activity with a child may do so with the intention of procuring the child to engage in, or submit to, sexual activity with another person. The individual may also be a situational offender who does not have an ingrained sexual interest in children. O'Donohue, Regev and Hagstrom (2000: 96) also noted that '[s]ome individuals who sexually abuse children may not have a sexual interest in children … and some individuals with a sexual interest in children may not actually abuse a child, simply because they have never acted on these interests or urges'. A recent report prepared for the use of the Committee on Energy and Commerce in the United States also suggested that not all offenders convicted of charges relating to the possession of child exploitation materials or child grooming committed sexual contact offences against children (United States House of Representatives Committee on Energy and Commerce, Republicans 2007). For example, in one case, an individual from Pompano Beach, Florida, allegedly:

> contacted a minor child on the internet site Myspace.com in November 2006 and through internet communications convinced the minor to leave her home in Tazewell County, Virginia and travel to Bluefield, West Virginia, for the purpose of engaging in prostitution. Subsequently, in early December 2006, Larson transported the minor to Miami, Florida and continued to direct her to engage in prostitution until Larson was apprehended by agents of the Federal Bureau of Investigation and the Miami Minor Vice Task Force in Miami, Florida on December 27, 2006 (US DoJ 2008a: unpaginated).

The offender reportedly pleaded guilty to one count of conspiracy to transport a minor in interstate commerce for the purpose of prostitution and one count of conspiracy to commit sexual exploitation of a child, and was sentenced to 188 months imprisonment in January 2008. The offender is required to register as a sex offender and to serve a term of eight years supervised release after his release from prison (US DoJ 2008a).

The third criterion relating to the *Diagnostic and statistical manual of mental disorders* definition of paedophilia provides a further limitation on the concept of child grooming if the term 'paedophile' is to form part of it. The individual charged with initiating sexual activity with a child must be at least five years older than the child in question and the accused must be at least 16 years of age. Such a definition is more restrictive than that currently provided for in both Commonwealth and NSW legislation. The *Crimes Act 1900* (NSW) (as amended by Crimes Amendment [Sexual Procurement or Grooming of Children] Bill 2007 on 28 November 2007) and the *Criminal Code Act 1995* (Cth), for example, define an adult person to mean a person who is of or over the age of 18 years and a child to mean a person who is under the age of 16 years. In addition, a 'child victim' in this case can be a person who pretends to be a child in a covert sting operation.

Two sections of the *Criminal Code Act 1995* (Cth) deal with procuring and grooming children online. These specify the offender as being a person who is at least 18 years of age and the child in question under 16 years of age. The relevant provisions are as follows.

474.26 Using a carriage service to procure persons under 16 years of age

(1) A person (the *sender*) commits an offence if:

- (a) the sender uses a carriage service to transmit a communication to another person (the *recipient*); and
- (b) the sender does this with the intention of procuring the recipient to engage in, or submit to, sexual activity with the sender; and
- (c) the recipient is someone who is, or who the sender believes to be, under 16 years of age; and
- (d) the sender is at least 18 years of age.

Penalty: Imprisonment for 15 years.

(2) A person (the *sender*) commits an offence if:

- (a) the sender uses a carriage service to transmit a communication to another person (the *recipient*); and
- (b) the sender does this with the intention of procuring the recipient to engage in, or submit to, sexual activity with another person; and

(c) the recipient is someone who is, or who the sender believes to be, under 16 years of age; and

(d) the other person referred to in paragraph (b) is someone who is, or who the sender believes to be, at least 18 years of age.

Penalty: Imprisonment for 15 years.

(3) A person (the *sender*) commits an offence if:

(a) the sender uses a carriage service to transmit a communication to another person (the *recipient*); and

(b) the sender does this with the intention of procuring the recipient to engage in, or submit to, sexual activity with another person; and

(c) the recipient is someone who is, or who the sender believes to be, under 16 years of age; and

(d) the other person referred to in paragraph (b) is someone who is, or who the sender believes to be, under 18 years of age; and

(e) the sender intends that the sexual activity referred to in paragraph (b) will take place in the presence of:

(i) the sender; or

(ii) another person who is, or who the sender believes to be, at least 18 years of age.

Penalty: Imprisonment for 15 years.

474.27 Using a carriage service to 'groom' persons under 16 years of age

(1) A person (the *sender*) commits an offence if:

(a) the sender uses a carriage service to transmit a communication to another person (the *recipient*); and

(b) the communication includes material that is indecent; and

(c) the sender does this with the intention of making it easier to procure the recipient to engage in, or submit to, sexual activity with the sender; and

(d) the recipient is someone who is, or who the sender believes to be, under 16 years of age; and

(e) the sender is at least 18 years of age.

Penalty: Imprisonment for 12 years.

(2) A person (the *sender*) commits an offence if:

(a) the sender uses a carriage service to transmit a communication to another person (the *recipient*); and

(b) the communication includes material that is indecent; and

(c) the sender does this with the intention of making it easier to procure the recipient to engage in, or submit to, sexual activity with another person; and

(d) the recipient is someone who is, or who the sender believes to be, under 16 years of age; and

(e) the other person referred to in paragraph (c) is someone who is, or who the sender believes to be, at least 18 years of age.

Penalty: Imprisonment for 12 years.

(3) A person (the *sender*) commits an offence if:

(a) the sender uses a carriage service to transmit a communication to another person (the *recipient*); and

(b) the communication includes material that is indecent; and

(c) the sender does this with the intention of making it easier to procure the recipient to engage in, or submit to, sexual activity with another person; and

(d) the recipient is someone who is, or who the sender believes to be, under 16 years of age; and

(e) the other person referred to in paragraph (c) is someone who is, or who the sender believes to be, under 18 years of age; and

(f) the sender intends that the sexual activity referred to in paragraph (c) will take place in the presence of:

(i) the sender; or

(ii) another person who is, or who the sender believes to be, at least 18 years of age.

Penalty: Imprisonment for 15 years.

This report will use these Criminal Code provisions to define 'online child grooming'. The relevant ages of 18 for the offender and 16 for the child will constitute the primary age-limited scope of the discussion, rather than adopting the age restrictions included in the definition of paedophile in the *Diagnostic and statistical manual of mental disorders*.

In relation to the nature of communications sent from an offender to a child, this report will focus primarily on internet-based, social networking sites, although some consideration will be given to other forms of electronic communications, especially those involving mobile and wireless technologies.

## Limitations

This report canvasses international material published in English since January 2000. The material was located by searching various academic databases (e.g. ACM Digital Library, Expanded Academic ASAP, InformaWorld, LexisNexis, Sage e-journal collections, ScienceDirect and SpringerLink) and Google™ Scholar using the keywords 'child luring', 'child enticement', 'child grooming', 'child sexual abuse', 'sexual perpetrator', 'content filtering' and 'internet filtering'.

While some of the research cited is academically robust in its methodology, it is important to note the small sample sizes involved in a number of the clinical studies. Although this is often appropriate for in-depth qualitative case studies that are published in the medical and psychiatric literature, the conclusions sometimes cannot be widely generalised to other populations. In addition, a number of studies were conducted online and involved self-selected samples that again limit the generalisability of the results, which occasionally involve less than reliable findings. Where particular questions of reliability or validity of findings arise, these will be identified in the text.

Finally, it should be noted that the problem of online grooming of children in social networking sites is relatively new. As a result, the research literature is in its infancy and longitudinal studies of prevalence have yet to be undertaken. However, this report does seek to draw together the current relevant research that is available to document the nature and extent of the problem in the English-speaking world.

# The nature of online grooming

## The psychopathology of child sex offenders

Individuals who have sexual fantasies involving children or erotic attractions towards children have been present in society throughout history. In a study by Langevin, Lang and Curnoe (1998), for example, a sample of 201 male patients was chosen from offenders seeking psychiatric assessment at the Forensic Service of the Clarke Institute of Psychiatry in Toronto, Ontario. Although the majority of the sexual offenders in the study reported having non-deviant sexual fantasies involving physically mature females, one-third reported having either deviant fantasies involving children or deviant sexual activities (Langevin, Lang & Curnoe 1998: 320). Deviant sexual fantasies in the study, marked by a significant departure from the behavioural norms of society, include fantasies involving exhibiting, peeping, non-consenting sexual rubbing, non-consenting sexual touching with the hands, rape and sadomasochism. The study suggested that:

- among the 'heterosexual paedophiles' group in the study, 84.7 percent of the respondents reported having sexual fantasies involving females aged 15 years or younger
- among the 'homosexual paedophiles' group in the study, 36.4 percent of the respondents reported having sexual fantasies involving females aged 15 years or younger.

A review of previously published academic studies by Gee, Devilly and Ward (2004) also highlighted similar levels of prevalence. This review and other studies also appear to suggest that in the online environment gender is a risk factor, 'with seemingly more girls than boys appearing to be harmed through cyberspace interactions (although boys are increasingly featured in pornographic images circulating online)' (Muir 2005: 9).

> [L]arge numbers of university students (21%) acknowledge being sexually attracted to children on occasions (Briere & Runtz 1989), that 61.7% of the general male population reported sexual fantasies about a young girl, whereas fewer reported fantasies about raping a woman (33%), being humiliated (11.7%), bestiality (5.3%), or sexual activity with a young boy (3.2%, Crepault & Couture, 1980). High numbers of surveyed participants also admitted to recent sexual thoughts about having sex with girls under the age of 15 (17%) or under 12 (5%), voyeuristic fantasies (54%), and exhibitionistic thoughts (7%; Templeman & Stinnett 1991) …
> (Gee, Devilly & Ward 2004: 317).

Pathological sexual interest in children has been explained using a number of theoretical models. The social skills deficit model (Emmers-Sommer & Allen 1999 cited in Olson et al. 2007), for example, argued that offenders 'seek relationships with

children due to a fear of relationships with adults, because relationships with children are deemed less threatening by the perpetrator' (Olson et al. 2007: 237).

> [T]here is some evidence that many of [the offenders] are adept at building a facade of trustworthiness. Children can be especially susceptible to this facade. Even though the adults may have suspicions and reservations, children are likely to find the adult perpetrator trustworthy and fun, causing adult caregivers of the child to silence their own suspicions (Olson et al. 2007: 237).

Vulnerability arises because of the incomplete development of children's social skills. Children are still learning how to communicate effectively (Lamb & Brown 2006) and hence are less likely to be as socially skilled as adults (Olson et al. 2007):

> … agreeing with every negative thing the teen has to say about a parent such as 'Your parents are unreasonable, not allowing a computer in your room' or 'Why shouldn't you be able to stay out until 2:00 in the morning? After all, you are 13. That's practically a woman'. These comments from an adult should be sending up red flags for our teens. Unfortunately, teens have a difficult time recognizing the nice person they have met online as a predator. In their minds, the two do not match (Kerlikowske 2007: unpaginated).

Children are less likely to pick up cues such as inappropriate remarks than adults. Hence, they become an easier target for sexual predators. It has been suggested that offenders typically target children with the following characteristics:

- low self-esteem or a lack of confidence – children exhibiting these characteristics may be easier to emotionally or physically isolate
- emotionally insecure, needy or unsupported – particularly those who are troubled or searching for parental substitutes
- naive nature – children are more willing to engage with strangers in a conversation online and may not know how to recognise and disengage from 'dangerous' situations
- adolescence – teenagers being sexually aware and, perhaps, curious about sex (Berliner 2002; Olson et al. 2007; Walsh 2005).

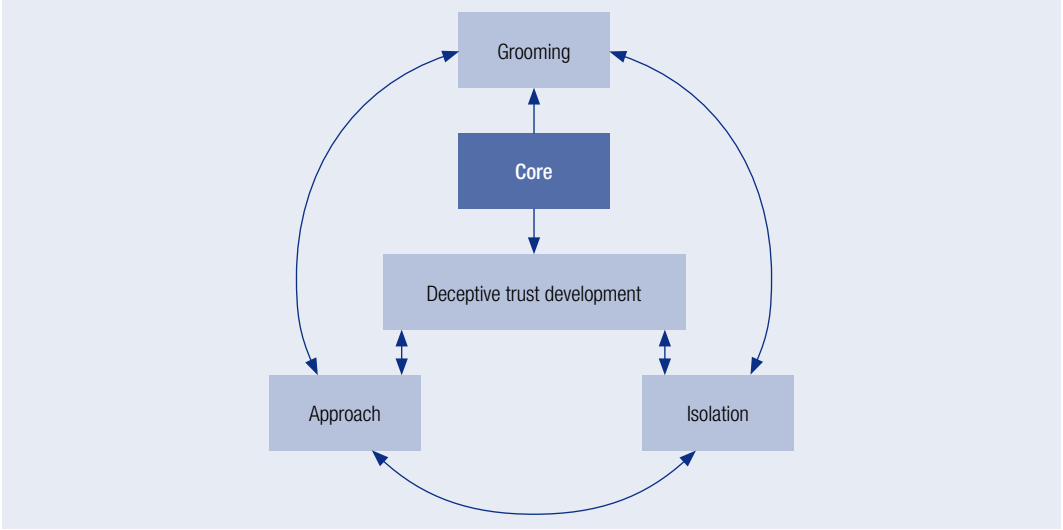
Sexual offenders have been known to target child victims with the above personality and emotional traits by providing them with love and affection that the child victims may not have received from their parents or peers. Sexually curious adolescents who are likely to be easily aroused are often more willing to take risks than less curious children. Research has also suggested that children and young people in their adolescence tend to make use of mass media including the internet 'to learn about two important aspects of identity development – sex and gender' (Subrahmanyam, Smahel & Greenfield 2006: 396). As a result, this particular group may be at a higher risk of being targeted by child sexual offenders than those less willing to use the internet. A sexual element is likely to be introduced into the relationship between the sexual offender and target child victim once trust had been cultivated and bonds formed.

## The child grooming process

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 that is likely to be attractive to children. In the physical world, this could be venues frequented by children such as schools, shopping malls, playgrounds and parks (Lang & Frenzel 1988). A process of grooming then commences during which offenders take a particular interest in their child victim and make the victim feel special with the intention of forming a bond to gain the trust of the child. According to Olson et al. (2007), the development of trust is the core component of the grooming process as the likelihood of sexual encounters in the physical world is contingent on the offender's ability to cultivate trust (Figure 1).

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 (see Lanning 2002). As noted by Terry and Tallon (2004: 22), a 'methodical and deliberate tactic of engaging a victim in sex involves a process of initially introducing the victim to the idea of sex and then gradually engaging [the child] in sexual activity'. Offenders can, for example,

**Figure 1** Child grooming process




Note: Olson et al. (2007: 243) defined approach as 'the initial physical contact or verbal lead-ins that occur prior to the actual sex act'

Source: Adapted from Olson et al. (2007)

share intimate personal details of their sex life with the child 'confidante' with the intention of making it easier to procure the recipient to engage in sexual activity with the offender or another person. Showing the child pornography is another effective means of grooming as '[p]ornography sexualizes rape, battery, sexual harassment, prostitution, and child sexual abuse; it thereby celebrates, promotes, authorizes, and legitimizes them' (Palczewski 2001: 7).

> [Child grooming] is a term describing how a child sex abuser uses various techniques, including showing porn to children, to lower their defenses and to get them to accept the sexual acts as 'normal' rather than 'abnormal' or 'abuse' (Schell et al. 2007: 52).

## The attractions of new technologies for children

ICT such as social networking sites have become an important element in the child grooming process, as these technologies are particularly popular with the digital generation. The digital generation, also known as 'Generation Virtual' and 'Gen-V', comprises people from various 'demographic age groups who make social connections online – through virtual worlds, in video games, as bloggers, in social networks or through posting and reading user-generated content at e-commerce sites like Amazon.com' (Havenstein 2007a: unpaginated). Recent research by Gartner found that since the launch of Facebook in February 2004, it is reportedly 'one of the top six most-trafficked Web sites, with 50 billion page views per month' (Valdes 2007: 5). In another study carried out in the United States by Pew Internet and American Life Project, 55 percent of the 935 respondents (US youths aged between 12 and 17 years) were found to have used online social networking sites (Lenhart & Madden 2007).

The attractions of the internet and social networking sites for children are explained clearly:

> More and more teens' social lives revolve around the Internet and making lifelong friends with people they might never meet in the real world. In this environment, it is easier to pretend to be something one is not. Truth is not necessary because no one will know. Every day, teens are entering a social cyberworld with false identities. The phenomenon of reinvention is more interesting. Teens lie about themselves online, but for some reason they are willing to believe what complete strangers say about themselves … Teenagers who are not popular in the real world can find a kind of substitute popularity online by adding more friends to their social

> networking site. Who needs real-life friends when they have so many people online willing to chat and tell them how cool they are? Children are having 10-minute conversations with strangers online and suddenly they have a new best friend. Teens are substituting virtual social lives with friends who often have no faces or verifiable identities for social lives in the physical world. Kids are making friends with people they meet in gaming rooms and virtual-world sites. Some become so obsessed with and absorbed in the game or virtual world that they lose the drive to achieve in the real world (Kerlikowske 2007: unpaginated).

Social networking sites are popular with children owing to the ease with which new virtual friends can be made simply by clicking on an 'add friend' request. If the other person accepts the request, a new friend is added to the list. This allows children to:

> quickly immerse their created 'virtual presence' among the created virtual presences of their entire social group and can immediately and conveniently get in contact with one or all. Regardless of the physical or temporal location of a person, then, users can intangibly surround themselves with the online representations of friends and acquaintances – allowing them to instantaneously feel close to any or all of them (Hindujaa & Patchin forthcoming: 3).

A recent study by eMarketer, an internet market research company, also highlighted the increasing popularity of online social networking sites with both adults and children. The study predicted that advertising spending on online social networks worldwide will nearly double, to US$2.2b in 2008 from US$1.2b in 2007, fuelled by an expanding online social networking population (Walsh 2007). The same study estimated that 70 percent of all teenagers in the United States currently visit social network sites on a monthly basis and by 2011, 84 percent of online teens in the United States will use social networking each month (eMarketer 2007).

Blogs are another emerging form of modern-day communications (Rosenbloom 2004; Vogelstein et al. 2005) that allow internet users (also known as 'bloggers') to disseminate and share information and ideas. Their increasing popularity of bloggers (including children) posting content (e.g. daily activities and thoughts) online is, perhaps, as Huffaker (2004 cited in Hindujaa & Patchin forthcoming) argued due to the following characteristics:

- user friendliness – ease in using with little technical expertise or internet skills required
- worldwide reach – anyone with internet access can read and leave comments or feedback
- virtual community – link to other blogs (including those of strangers) and thus forming some sorts of virtual communities.

Other popular communications technologies used to exchange written messages in real time, with various levels of informality, include instant messaging programs (e.g. MSN Messenger, Yahoo! Messenger and ICQ), IRC rooms and short message service (SMS; mobile-to-mobile text messages). The popularity of such technologies with young people is now demonstrable:

> If you are 8, 9, 10 or even 11 years old, you have probably never known the world without the internet or mobile phones … 41% of children aged 8–11 regularly use the internet, 32% of children aged 8–11 regularly use a mobile phone, 56% of children aged 8–11 play computer games, 7% of 10 year olds have their own web cam (UK CEOP 2007a: 3).

A recent study in the state of Virginia entailed an online survey of 1,277 students aged between nine and 17 years, an online survey of 1,039 parents, and telephone interviews conducted with 250 school district leaders throughout the state (these were people who made decisions on internet policy). It was found that:

- 96 percent of students aged between nine and 17 years with online access have reportedly used social networking technologies, such as chatting, text messaging, blogging and visiting online communities such as Bebo, Facebook and MySpace, and services designed specifically for younger children such as Webkins and the chat sections of Nick.com
- 81 percent of students aged between nine and 17 years reportedly visited a social networking site within the past three months and 71 percent reportedly used social networking tools on a weekly basis (Grunwald Associates LLC 2007).

In another study by Garnacho and Garmendia (2007), six focus groups were conducted with young people who were regular internet users in various cities of Spain. Each group comprised four males and four females as follows:

- two groups of 12 and 13-year-olds in Barcelona and Madrid
- two groups of 14 and 15-year-olds in Bilbao and Valencia
- two groups of 16 and 17-year-olds in A Coruña and Seville.

The study found that:

> adolescents spend the greater part of their time on Internet using Messenger, because it enables them to talk with their friends instantaneously and rapidly, as email seems less immediate to them. Besides, it allows them to keep in constant contact with their friends: 'If you're by yourself, you turn on Messenger' (boy, aged 17, A Coruña). Perhaps this is similar to the use they make of the mobile telephone, with the difference that Messenger doesn't require 'having credit'. However, they use Messenger for conversations that are more informal and entertaining; for more serious conversations they prefer the telephone. Obviously, when they are outside the home they are obliged to use SMS. 'When I'm at home I use Internet … but if I'm out or somewhere that doesn't have a computer … by mobile phone' (boy, aged 13, Madrid). Besides, with Messenger they exchange photos, music, they play, etc. (Garnacho & Garmendia 2007: 6).

Acronyms, a series of letters or numbers that represent a word or phrase, are 'now part of every teen's vernacular when communicating with friends in chat rooms or instant messaging' (Denis 2007: unpaginated). Table 1 provides a list of sexually oriented internet acronyms commonly used by children and young people.

**Table 1** List of commonly used sexually-oriented internet acronyms

| Acronym | Definition |
|---|---|
| 8 | Oral sex |
| 143 | I love you |
| 459 | I love you |
| 1174 | Nude club |
| 420 | Marijuana |
| ADR or addy | Address |
| ASL | Age/sex/location |
| CD9 | Code 9 (parents are around) |
| DUM | Do you masturbate? |
| DUSL | Do you scream loud? |
| GNOC | Get naked on cam (webcam) |
| GYPO | Get your pants off |
| IWSN | I want sex now |
| KFY | Kiss for you |
| KPC | Keeping parents clueless |
| LMIRL | Let's meet in real life |
| MOOS | Member(s) of the opposite sex |
| MOSS or MOTSS | Member(s) of the same sex |
| MorF | Male or female |
| MOS | Mum over shoulder |
| NIFOC | Nude in front of computer |
| P911 | Parent alert |
| PAL | Parents are listening |
| PAW | Parents are watching |
| PIR | Parent in room |
| POS | Parent over shoulder |
| PRON | Porn |
| RU/18 | Are you over 18? |
| RUH | Are you horny? |
| SorG | Straight or gay? |
| TDTM | Talk dirty to me |
| WYCM | Will you call me? |

Source: Adapted from http://www.netlingo.com/top50teens.cfm

In a typical online conversation involving children, such acronyms and other non-linguistic signs (so-called 'emoticons') are often used to accelerate the writing process. Box 1 is an example of a conversation in an IRC room between two parties going by the nicknames 'Sk8tr' and 'Ynggrl':

**Box 1** An example of an online conversation in an IRC room

**Sk8tr:** hey

**Ynggrl:** sup [*translation: 'What's up?'*]

**Sk8tr:** asl [*translation: 'Age, sex and location?'*]

**Ynggrl:** 15f [*translation: '15, female'*]

**Sk8tr:** wut r u doing 2nite [*translation: 'What are you doing tonight?'*]

**Ynggrl:** n2m [*translation: 'Not too much'*]

**Sk8tr:** wuf [*translation: 'Where are you from?'*]

**Ynggrl:** paw [*translation: 'Parents are watching'*]

Source: Adapted from Denis (2007)

The use of acronyms was noted in a recent case involving an individual arrested and charged in Queensland with using the internet to procure a child under 16 for a sex act. The individual used the pseudonym 'Max Smith' and was alleged to have initiated contact with an undercover police officer posing as 13-year-old 'Erin Sinclair' in an IRC room in December 2005 (AAP 2007b). 'Max Smith', who was subsequently acquitted of the online child grooming charge, claimed that he believed that 'Erin Sinclair' was an adult and not a 13-year-old girl because 'Erin Sinclair' used words not commonly used by teenagers such as 'veging' and 'spaz' during the online conversation.

## The attractions of new technologies for sexual predators

Criminologists have argued that crime is most likely to occur when there are opportunities for crimes to happen, the presence of suitably motivated offenders, and the absence of capable guardians or other deterrents to crime. Developments in ICT have created an ideal criminogenic environment as there are abundant opportunities, highly motivated offenders, and not a great deal of coordinated and effective regulation. McNulty (2007), explains this as follows.

> In the past, criminals who created or collected child pornography or who tried to entice children for sexual purposes were restricted by their own awareness of their deviancy. The grotesque nature of child sexual abuse and the corresponding fear of detection kept many sexual offenders from associating in the physical world with similarly minded criminals. Cyberspace, however, allows for a previously unavailable degree of anonymity. As a result, sexual offenders have flocked to online communities to share images of child sexual abuse and to discuss their barbaric behaviour (McNulty 2007: unpaginated).

ICT allow both children and adults more avenues in which to establish positive interpersonal relationships, but these technologies have also facilitated the commission of conventional crime by enabling offenders to locate potential victims with ease and to share information concerning the vulnerabilities of victims with other offenders around the globe. It is unlikely that child sexual offenders will shy away from using new technologies to facilitate the process of grooming children for sexual abuse (Choo, Smith & McCusker 2007; Kierkegaard 2008).

> Given what is known about the perpetrators of child sexual abuse, it is not surprising that they are exploiting the characteristics of cyberspace – its vastness, anonymity, illusion, lack of effective control, and potential mass and international market. Cyberspace offers unparalleled opportunities for the deceit and secrecy on which child sexual abuse relies and unprecedented access to vulnerable children and adults in their own homes (Harrison 2006: 368).

Durkin 1997 (cited in Middleton et al. 2006) 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
- 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.

The anonymous nature of the internet allows offenders to masquerade as children in cyberspace (e.g. IRC rooms and social networking sites) to gain the confidence and trust of their victims over a period of time (from minutes to months) before introducing a sexual element into the online conversation. Sometimes the transition from innocent to sexualised discussions can be rapid:

> Within four minutes of introducing himself in a local Internet relay chatroom meant for teenagers, Aauarius asked to feel my breasts. Even after knowing that I was a 13-year-old schoolgirl, he asked for my height, weight, waist measurement and size of my 'top' (Tan 2007: unpaginated).

In the study by Quayle and Taylor (2003), based on data obtained from the COPINE project at the Department of Applied Psychology, University College Cork, one of their 23 male subjects who had been convicted of downloading child pornography as part of his offending behaviour, admitted to impersonation, both as a child and an adult, to facilitate contact with other children in IRC rooms:

> Assuming a child's persona (sustained over a number of months) allowed the respondent to easily win the trust of others he supposed to be children and to engage in 'cybersex' with them … However, self-representing as an adult male allowed him to chat to underage males, to engage in sexual activity with them both online and via the telephone, and to arrange physical meetings with them (Quayle & Taylor 2003: 102).

The lack of visual cues in cyberspace, which may assist child victims in making judgments about the suitability, trustworthiness and sincerity of others with whom they communicate (Wells & Mitchell 2007), also facilitates the grooming process. This is especially the case with virtual game sites.

> The avatar–person relationship is not a one-to-one ratio – some individuals maintain multiple avatar 'personae' … One recent development is the arrival of automated avatars ('bots'), although these are common in many gaming environments. Approaching a 'bot' in a corporate setting, or initiating a conversation, results in alerts being transmitted through to the corporate contact center so that a real person can take over control of the avatar (Prentice 2007: 3).

The offenders can engage child victims in the same conversation while assuming different identities online (via avatars) as illustrated in the following case:

> Southwark Crown Court heard how Paul Rogers, 37, had pretended to be a 14-year-old girl named Sarah who used the e-mail address 'skoolchic_sez' to groom a girl he was told was 12 … In a later exchange, he offered to pay the youngster 100 pounds to strip him, dress him in female underwear and spank him – but only if the 12-year-old was in underwear herself. During the same conversation, 'Sarah' introduced her cousin who was also Rogers (UK man jailed for child grooming 2007: unpaginated).

Instead of visiting venues in the physical world, offenders now seek out their victims by visiting IRC rooms from the leisure of their home or internet cafes. Ropelato (2007), for example, it is estimated that 89 percent of sexual solicitations of youth are made in IRC rooms. The recent UK cybercrime survey commissioned by online criminology firm, 1871 Ltd, also reported an estimated:

> ... 850,000 cases of unwanted online sexual approaches, primarily messages of a sexual nature within Internet chat rooms, during 2006. During the same period 238 offences of meeting a child following sexual grooming were recorded (Fafinski 2007: 14).

Once a child victim is identified, the offender can invite the child into a private area of the IRC to engage in private conversations. For example, in a study by Sibley and Heath (2004), the following IRC channels were logged in various phase of the study:

- *Phase 1: Taxonomy creation*
  (7 IRC channels on the Austnet IRC network logged for 96-hour, which yielded a corpus of 691,180 words posted by a total of 6,867 unique users)

  #30&40's

  #frankston

  #sydney

  #adelaide_singles

  #Teen

  #asianmelb

  #canberra

- *Phase 2: Initial validation sample*
  (Five IRC channels on the Austnet IRC network logged for 96 hours, which yielded a corpus of 824,016 words posted by a total of 9,880 unique users.)

  #chatzone

  #Melbourne

  #Brisbane

  #Perth

  #teens
- *Phase 3: Confirmatory validation sample*
  (Five IRC channels on the Galaxynet IRC network logged for 48 hours, which yielded a corpus of 382,705 words posted by a total of 4,905 unique users.)

  #teen

  #teens

  #sex

  #cybersex

  #singapore20+

  (Seven IRC channels on the Austnet IRC network logged for 96 hours, which yielded a corpus of 411,372 words posted by a total of 4,400 unique users.)

  #Chatzone

  #Teen

  #Perth

  #teens

  #Melbourne

  #Brisbane

  #sex

The study found that of the 82 most commonly used phrases for private interaction requests on IRC:

- three percent were phrases targeting females such as 'any females' and 'any ladies'
- one percent were phrases targeting males such as 'any hot guys' and 'any sexy guys'
- six percent were communication request phrases such as 'Wanna chat?'
- one percent were phrases used to identify oneself such as '12 f' (translating to 12, female)
- one percent were phrases requesting others to contact the person who posted the message such as 'msg me now' (Sibley & Heath 2004).

Other communications technologies such as instant messaging, email, VoIP and mobile phones can also be used in the grooming process. During the grooming process, offenders can expose the child victim to sexually harmful content, such as pornography and sexual speech, or provide verbal encouragement to sexually harmful behaviour to desensitise the child victim and persuade them to have a sexual relationship. For example, in the case involving Lee Anthony Costi (the appellant), Costi allegedly told his victim:

> that he was 20 years old. She told him that she was aged 12. The Complainant's computer was linked to a webcam, and at the Appellant's request she showed him her breasts and her vagina and masturbated for him (*R v Costi* [2006] EWCA Crim 3152).

In another case, Gerald Alan Harris, was arrested on charges of:

> distribution of child pornography over the Internet, attempting to send obscene materials to a child under the age of sixteen, attempting to entice a minor to engage in sexual activity, and travelling in interstate commerce for the purpose of engaging in sexual acts with an individual whom he believed to be a twelve-year-old girl (US DoJ 2007a).

Often, the grooming process will continue for months before the offender arranges a physical meeting:

> From January through July 2007, Hinkley engaged in Internet conversations with 'Cassie' an individual Hinkley believed to be an eleven-year-old girl, and 'Sheryl', whom Hinkley believed to be 'Cassie's' mother. In fact, both 'Cassie' and 'Sheryl' were an undercover officer with the Cañon City Police Department in Cañon City, Colorado. During these conversations, Hinkley explicitly and graphically described to both 'Cassie' and 'Sheryl' the sexual activities he planned to engage in with them when the three met in person (US DoJ 2007b: unpaginated).

Undeniably, ICT have created a new space in which children 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 (AIC 2005). 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.

Professor Patricia Greenfield, director of the University of California's Children's Digital Media Center, noted that 'with today's all-pervasive sexualized media environment … [b]y late childhood, it has become very difficult to avoid highly sexualized material that is intended for an adult audience' (UCLA 2005).

Technologies have also made the task of contacting strangers and children online easier. In the Pew Internet and American Life Project Teens and Parents Survey conducted between 23 October and 19 November 2006, of the 886 teenagers aged between 12 and 17 years who reported using the internet, almost one-third had been contacted by strangers online and some seven percent felt scared or uncomfortable as a result. Much higher proportions of those who had created a social networking site profile or posted photos online had been contacted by strangers and made to feel scared or uncomfortable (Table 2).

**Table 2** Strangers contacting children online (percentage)

| | Contacted by strangers | Contacted by a stranger who made them feel scared or uncomfortable |
|---|---|---|
| All online teens (n=886) | 32 | 7 |
| **Sex** | | |
| Online boys | 24 | 4 |
| Online girls | 39 | 11 |
| **Online activities** | | |
| Have created a social networking site profile | 44 | 9 |
| Have not created a social networking site profile | 16 | 5 |
| Have posted photos online | 49 | 10 |
| Have not posted photos online | 16 | 4 |

Note: n=935 teens aged between 12 and 17 years

Source: Adapted from Smith (2007)

Child sexual offenders have also been known to use the internet to search for child exploitation materials and to distribute these materials across national and international boundaries for desensitising targeted child victims. Paedophiles often frequent selected internet sites to communicate with other like-minded individuals and/or to share images of children electronically.

> A recent FBI intelligence briefing describes how different symbols are used to indicate gender preference – 'boylove' or 'girllove' – or membership of a pedophile organisation … One website that openly displays the BoyLover and ChildLover logos was also central to a trial earlier this year, when an alleged Australian paedophile was described as using it to contact his alleged victim (Box 2007: unpaginated).

The internet has greatly facilitated the sharing of information and strategies for grooming children for sexual purposes, and in so doing, reinforcing adult–child sex philosophies of offenders.

> One of the perpetrators, David Hines, who received a criminal sentence, described how easy it was to obtain images of child pornography on the Internet – within twenty-four hours of first going on-line he had found material. He met other paedophiles. As with cyberstalking cases, this group of people thought they were protected by the anonymity of the Internet, so they traded sexually explicit images of children and talked about them. As a shy, introverted person, again similar to those who perpetrate cyberstalking crimes, he had found an instant set of friends. The problem was not just the trading of images, but also the way that paedophiles had an easy way to contact each other and to reinforce their beliefs that sex with children was not wrong, to promote the ghastly idea that somehow these children were 'in relationships' with adults. Paedophiles also shared information about how to 'groom' children for abuse (Adam 2002: 13–14).

A recent study reported that 'teen sex' and 'teen porn' ranked among the top 20 keywords used in pornographic-related internet searches during 2006 (Table 3).

The types of offences that are relevant to online child exploitation include producing, possessing and

**Table 3** Top 20 internet pornographic-related search requests by keyword, 2006

| 2006 top adult search requests | | | | | Demographics – sex and age in years (percentage) | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Search term | 2006 search requests (millions) | 2006 % change | 2005 % change | Web pages containing keyword (millions) | Male | Female | <18 | 18–24 | 25–34 | 35–49 | 50+ |
| Sex | 76 | 7 | 40 | 414.00 | 50 | 50 | 20 | 20 | 20 | 20 | 20 |
| Adult dating | 30 | 622 | 80 | 1.40 | 36 | 64 | 20 | 20 | 21 | 20 | 19 |
| Adult DVD | 14 | 53 | 21 | 1.82 | 58 | 42 | 20 | 19 | 23 | 21 | 17 |
| Porn | 24 | –3 | 29 | 88.80 | 96 | 4 | 23 | 14 | 10 | 36 | 17 |
| Sex toys | 16 | 4 | 1 | 2.65 | 58 | 42 | 20 | 16 | 19 | 19 | 26 |
| Teen sex | 14 | 36 | 25 | 2.10 | 44 | 56 | 22 | 19 | 19 | 22 | 18 |
| Free sex | 13 | 0 | 20 | 2.42 | 44 | 56 | 22 | 19 | 19 | 22 | 18 |
| Adult sex | 13 | 301 | 51 | 1.58 | 36 | 64 | 19 | 21 | 21 | 20 | 19 |
| Sex ad | 13 | 382 | 40 | 0.28 | 50 | 50 | 20 | 20 | 19 | 20 | 21 |
| Group sex | 13 | 88 | 33 | 2.07 | 50 | 50 | 20 | 20 | 20 | 20 | 20 |
| Free porn | 13 | –10 | 54 | 2.74 | 97 | 3 | 22 | 14 | 10 | 35 | 19 |
| XXX | 12 | 25 | 14 | 181.00 | 50 | 50 | 20 | 20 | 20 | 20 | 20 |
| Sex chat | 12 | 97 | 36 | 2.21 | 50 | 50 | 20 | 20 | 20 | 20 | 20 |
| Anal sex | 10 | 76 | 21 | 2.95 | 67 | 33 | 19 | 19 | 16 | 28 | 19 |
| Cyber sex | 9 | –20 | 3 | 1.24 | 41 | 59 | 23 | 25 | 14 | 30 | 8 |
| XXX videos | 7 | 71 | 40 | 1.44 | 64 | 37 | 17 | 19 | 26 | 27 | 11 |
| Playboy | 7 | –6 | 24 | 43.20 | 86 | 14 | 10 | 33 | 25 | 25 | 7 |
| Teen porn | 6 | 7 | 38 | 1.97 | 82 | 18 | 23 | 17 | 14 | 28 | 18 |
| Nude | 5 | –26 | 14 | 71.30 | 77 | 23 | 33 | 14 | 10 | 17 | 26 |
| Sexy | 4 | 21 | 33 | 198.00 | 50 | 50 | 20 | 20 | 20 | 20 | 20 |

Note: The statistics are compiled from the following sources: Australian Broadcasting Corporation, Associated Press, AsiaMedia, AVN, BBC, CATW, US Census, Central Intelligence Agency, *China daily*, Chosen.com, Comscore Media Metrix, Crimes Against Children, Eros, Forbes, Frankfurt Stock Exchange, Free Speech Coalition, Google, Harris Interactive, Hitwise, Hoover's, Japan Inc., *Japan review*, Juniper Research, Kagan Research, ICMEC, Jan LaRue, *Miami herald*, MSN, Nielsen/NetRatings, *New York times*, Nordic Institute, PhysOrg.com, PornStudies, *Pravda*, *Sarmatian review*, SEC filings, Secure Computing Corp., *Sydney morning herald*, TopTenREVIEWS, Trellian, WICAT, Yahoo! and XBIZ

Source: Adapted from Ropelato (2007)

disseminating child pornography, grooming children for the purposes of sexual contact and displaying live images of child sexual abuse.

> New information and communication technologies allow multiple images to be produced from one digital recording of abuse and the transfer of images from other media; the number of images involved gives little indication of the number of children who are abused or the timescale over which the abuse has occurred … and there has been an increase in sexual exploitation of children (Harrison 2006: 368).

Another emerging risk relating to online child exploitation is 'rape' crimes that take place in online gaming or virtual worlds. There are even websites on public domains that reportedly host games for players to 'earn points and upgrade to higher-level game scenarios by attacking sexy female cartoon characters' (Lim 2007a: unpaginated).

> Dr Ang Yong Guan, a [Singapore-based] psychiatrist, was speechless when The New Paper showed him one of the websites on his computer screen. The 'victim' of this brutal rape game is a young Japanese girl drawn in the anime style. She is shown blindfolded and tied to a chair. 'This is very serious, very sad,' said the 52-year-old psychiatrist who is chairman of the Action Group for Mental Illness. 'This is worse than pornography. These rape games are promoting a criminal activity and glorifying it. The young ones may not understand that they are inflicting pain onto "the other party". These children will grow up with warped values. That's

> frightening.' The whole value system of a child will be affected. It can affect their emotional growth. When they are not psychologically and emotionally ready and they are exposed to such materials, some of them can be overwhelmed and start to fantasise deeply (Lim 2007b: unpaginated).

These forms of virtual crimes can potentially cause real psychological, social and financial harms to their victims, particularly children. Brenner (2001), for example, argued that crimes in virtual worlds are as real as crimes in our own world although perpetrators of virtual rape crimes are unlikely to be prosecuted under extant rape statutes.

## 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. Meloy (1998) highlighted that the internet can be used:

> to gather private information on the target to further a pursuit; and (2) to communicate (in real time or not) with the target to implicitly or explicitly threaten or induce fear (Meloy 1998 cited in Adam 2002: 136).

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, an invaluable tool to provide individuals with immediate access to an enormous range of information, can also be abused to locate publicly available information of children on the internet by using keywords such as 'site:myspace.com', 'female' and '13 years old'.

Private information about a target child can also be obtained by engaging the victim in conversation in public domain sites such as IRC rooms and online gaming forum sites.

> The students witnessed an eye-opening video in which a 34-year-old law enforcement agent, posing as a 13-year-old girl with blonde hair and blue eyes, [entered] a chat room. Within 15 minutes, the fictitious girl received a sexual proposition from another participant in the chat room. The agent, a member of the Cyber Crime Unit, also demonstrated that it took a mere 20 minutes to gather information about another chat room visitor who used the screen name Teresa01. The agent learned Teresa01's home address, phone number, parent's names, and school name. The agent also obtained pictures of Teresa01. The agent's demonstration in the video had a rare effect on the middle school students: they were speechless at the presentation's conclusion (Griffith 2007: unpaginated).

Another effective way of obtaining personal information and pictures of children is to browse personal profiles online.

> On MySpace, teens build profiles that explain everything about them, from where they go to school and what time to their sexual preferences and fantasies. 'An adult predator couldn't ask for a better profile', he [internet parenting expert John Carosella] said. 'MySpace is a public place where adults hang out. People aren't who they say they are. It's a recipe for what your kids like and a roadmap on how to find them. It's dangerous' (Coen 2006: 13).

In the study by Pew Internet and American Life Project, for example, 55 percent of the 935 respondents (US youths aged between 12 and 17 years) reported having personal online profiles. Personal profiles of individuals can be posted on social networking sites such as Facebook, Friendster and MySpace, blogs, some online gaming sites and personal homepages. These profiles can be either public (i.e. can be viewed by anyone) or private (i.e. restricted to only friends or members of a designated group).

> Olivia visited a chat room where she was talking to friends about her favourite band. A guy she hadn't met before read her profile and said hi. They started chatting, and Olivia got on really well with him – he seemed to agree with everything she thought and said which was cool. After some time, he asked her for her Instant Message address so they could chat more privately. Olivia accepted him onto her contact list and after a few weeks of chatting

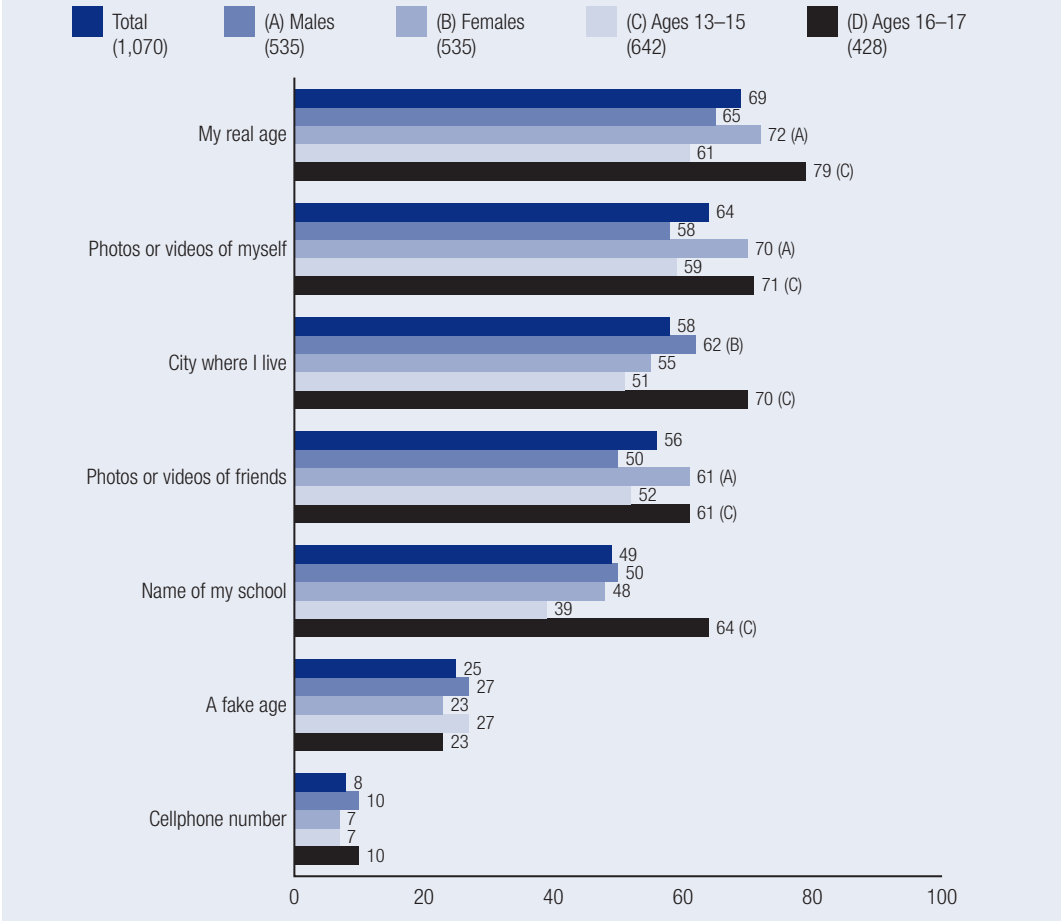
through IM [instant messaging] every day she felt she knew him pretty well. He sent a photo of himself to her and she thought he looked really nice, so when he asked her to send him a sexy photo of herself – she felt apprehensive, but sent one anyway. He told her that she looked great and suggested meeting up (http://www.virtualglobaltaskforce.com/case_studies.html).

In the recent Teen Internet Safety Survey, Wave II study, out of the 1,070 respondents aged between 13 and 17 years residing in the United States and with internet access, 71 percent of the respondents indicated that they had established an online profile and 47 percent had an internet profile that was public and viewable by anyone (Cox Communications 2007). Types of information posted online by the respondents are shown in Figure 2.

Although one in 10 respondents in the study posted their mobile phone numbers online and only one-quarter reportedly posted a fake age online (Figure 2), more than half the respondents reportedly posted information online about their real age and city in which they reside, and posted pictures or videos of themselves and their friends.

In the Media and Communications in Australian Families 2007 study commissioned by the Australian Communications and Media Authority (ACMA), 751 Australian families with children aged between eight

**Figure 2** Types of information posted online by children aged between 13 and 17 years (percentage)




Source: Adapted from Cox Communications (2007)

and 17 years were surveyed nationwide from 20 March to 12 May 2007. A total of 1,003 children aged between eight and 17 years in these families completed time-use diaries that indicated their online activities. The study found that:

- approximately 70 percent of girls aged between 14 and 17 years, and 50 percent of boys of the same age group had a personal profile on MySpace or other similar online sites
- approximately one in eight respondents aged between 14 and 17 years reportedly posted videos online (ACMA 2007a).

The wealth of personal information and pictures online could potentially be used by sexual predators to identify, contact or stalk their child victims. Personal information mined or obtained from online social networking sites can also be sold to interested parties for financial reward. A group of individuals carried out a coordinated attempt to mine personal information contained on Facebook. This led to litigation by the host of Facebook.

> Facebook is suing seventeen people and a Canadian Internet porn company for allegedly trying to mine the popular social networking site for its users' personal details. Facebook alleges that in June servers controlled by the defendants used automated scripts to make more than 200,000 requests for personal information stored on Facebook's site. The allegations are contained in an amended lawsuit filed earlier this month in U.S. District Court in San Jose, California … Experts have warned people against publishing too much personal information on social networking sites for fear it could be collected and then abused by fraudsters (Kirk 2007: unpaginated).

Statistics provided by Ropelato (2007), which are compiled from various sources, also indicate the willingness of young people to give out their email and residential addresses. The survey found that almost one-third of the young people aged between seven and 17 years who responded were willing to disclose their home address, while 14 percent were willing to disclose their email address online (Table 4).

**Table 4** Children internet pornography statistics

| | |
|---|---|
| Average age of first internet exposure to pornography | 11 years |
| 15 to 17-year-olds having multiple hard-core exposures | 80% |
| 8 to 16-year-olds having viewed pornography online | 90% |
| 7 to 17-year-olds who would freely give out home address | 29% |
| 7 to 17-year-olds who would freely give out email address | 14% |
| Children's character names linked to thousands of pornography links | 26 |

Note: The statistics are compiled from the following sources: Australian Broadcasting Corporation, Associated Press, AsiaMedia, AVN, BBC, CATW, US Census, Central Intelligence Agency, *China daily*, Chosen.com, Comscore Media Metrix, Crimes Against Children, Eros, Forbes, Frankfurt Stock Exchange, Free Speech Coalition, Google, Harris Interactive, Hitwise, Hoover's, Japan Inc., *Japan review*, Juniper Research, Kagan Research, ICMEC, Jan LaRue, *Miami herald*, MSN, Nielsen/NetRatings, *New York times*, Nordic Institute, PhysOrg.com, PornStudies, *Pravda*, *Sarmatian review*, SEC filings, Secure Computing Corp., *Sydney morning herald*, TopTenREVIEWS, Trellian, WICAT, Yahoo! and XBIZ

Source: Adapted from Ropelato (2007)

Another recent study by Sophos, an IT security company, showed the ease with which personal information could be gathered online:

> A fabricated Facebook profile [is created] before sending out 'friend requests' to individuals chosen at random from across the globe. To conduct the experiment, Sophos set up a profile page for 'Freddi Staur' (an anagram of 'ID Fraudster'), a small green plastic frog who divulged minimal personal information about himself. Sophos then sent out 200 friend requests to observe how many people would respond, and how much personal information could be gleaned from the respondents (Sophos 2007: unpaginated).

The results of the Facebook ID Probe study showed that:

- 87 of the 200 Facebook users contacted responded to Freddi, with 82 leaking personal information (41% of those approached)
- 72 percent of respondents divulged one or more email addresses
- 84 percent of respondents listed their full date of birth

- 87 percent of respondents provided details about their education or workplace
- 78 percent of respondents listed their current address or location
- 23 percent of respondents listed their current phone number
- 26 percent of respondents provided their instant messaging screen name.

Ease in obtaining personal information about children online facilitates offenders in targeting children for child exploitation offences (including child grooming).

> The anonymity, availability of extremely sensitive personal information and ease of contacting people make social networking sites a useful tool for online child predators. While many of the sites have age restrictions, it is possible for minors to misrepresent their age. To hide their IP addresses and locations, they piggyback on Wi-Fi connections or use proxy servers. Decentralized peer-to-peer networks prevent material from being tracked to a specific server, and encryption lets them keep online chats private from those policing the Web. When law enforcement, ISPs, and others take down paedophile Web sites, it does not take them long before they ate back and hosted by a different service (Kierkegaard 2008: 43).

With advances in communications technologies, there will be an increase in avenues for child sexual offenders and cybercriminals to engage in online child exploitation with little risk of being traced. Anonymity of communication can be provided through the use of the Onion Router, an 'anonymising protocol' that allows data to be routed through a network of servers. The latter uses cryptography to obscure the data path and hence make it untraceable for law enforcement. The Onion Router is used in the Wikileaks.org website designed for whistleblowers in authoritarian countries to post sensitive documents on the internet without being traced (Marks 2007).

Child sexual offenders can also hide their online communications, digital images (e.g. pictures chat room users placed in their profiles), and video files by using password authentication, encryption and steganographic techniques. These create serious impediments to law enforcement and investigators in their efforts to combat online grooming of children and other acts of child exploitation.

Once a child sexual offender has initiated contact online, the offender may encourage the targeted child to chat privately, for example, in a private IRC room or in an instant messaging session. When the targeted child continues to engage in the conversation with the offender, a relationship of trust between the child and the offender may be established. During this initial relationship-forming stage, the offender will often continuously seek to lower the child's inhibitions concerning sexual activity 'in order to draw the young person into intimate discussion and actions online and/or physical contact offline' (Muir 2005: 47–48). The nature of this grooming process has been described by O'Connell (2003) as follows:

> [A child sexual offender] may ask whether or not the child has a picture of themselves and if the answer is yes they will request the picture to be sent to them. It seems reasonable to suggest that requests for pictures relate at least in part to the paedophile's desire to ensure that the child he is conversing with is in fact firstly a child and secondly one that matches his particular predilections. Furthermore, for those who choose to target children who live in their immediate vicinity the provision of a picture would serve as a useful way to identify the child in the real world. Typically, at this point in the conversation requests for pictures are confined to pictures of the child without any reference to pictures of a sexual nature … The relationship-forming stage is an extension of the friendship-forming stage, and during this stage the adult may engage with the child in discussing, for example, school and/or home life (O'Connell 2003: 8–9).

# The extent of online grooming

As is the case with most forms of cybercrime, it is difficult to determine with accuracy the actual extent to which children are targeted online for sexual purposes. Quantification of the extent of the problem is exacerbated by the illegal nature of such activities, their sexual focus and the covert manner in which grooming takes place. This makes self-reporting and detection unlikely to occur. There have, however, been a number of reports of children (or undercover law enforcement officers posing as children) having been approached online leading to the prosecution of those responsible (see Smith 2007). Various reports have also been made to international bodies concerning online child exploitation (including online child grooming). The following discussion presents the results of relevant crime victimisation surveys, official police and prosecutions statistics, and a series of illustrative case studies of online child grooming.

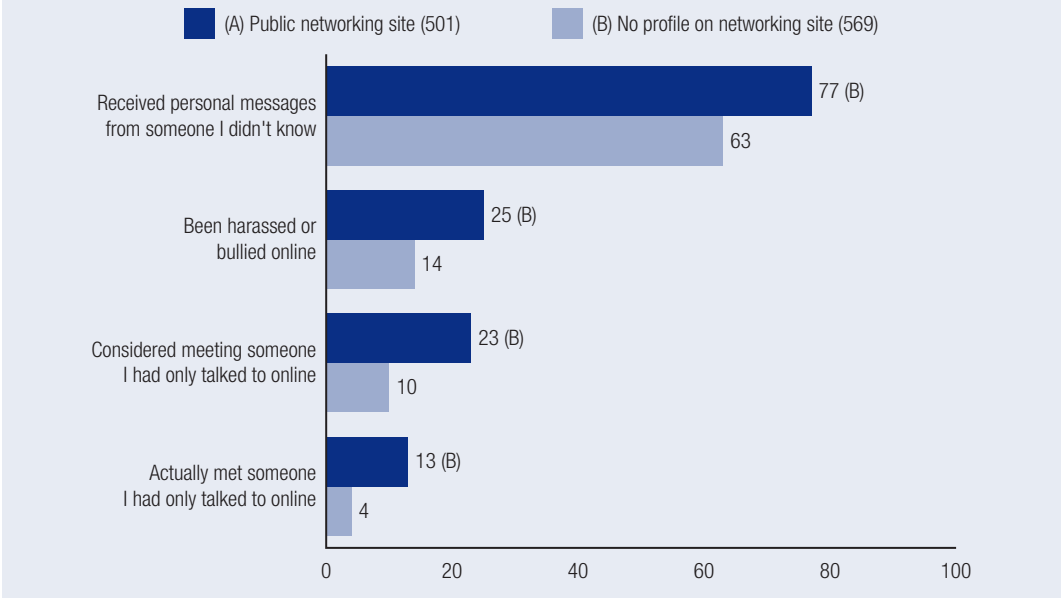
## Victimisation surveys

Online sexual activities (including cybersex) have reportedly increased in recent years. In the study by Daneback, Cooper and Månsson (2005), for example, almost one-third of the 1,828 respondents (of both genders) had reportedly engaged in cybersex – defined as two or more people engaging in sexual talk while online for the purposes of sexual pleasure, which may or may not include masturbation. In another online survey conducted by Cordonnier (2006) over a period of five weeks beginning in March 2005, 33 percent of the 7,588 respondents were self-confessed cybersex addicts aged between 18 and 25 years.

> A [mental health] client experiencing marital conflict who would not have sought out a 'real life' affair may participate in cybersex with someone miles away. People who have thought about acting out sexually but who were inhibited or afraid to purchase pornography from a store or otherwise expose their desires in public might find it difficult to control the desire to search for pornography or other sexual activity while using the Internet (Mitchell, Becker-Blease & Finkelhor 2005: 498).

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 (Figure 3). 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

**Figure 3** Children's experiences with potential online risks (percentage)




Source: Adapted from Cox Communications (2007)

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.

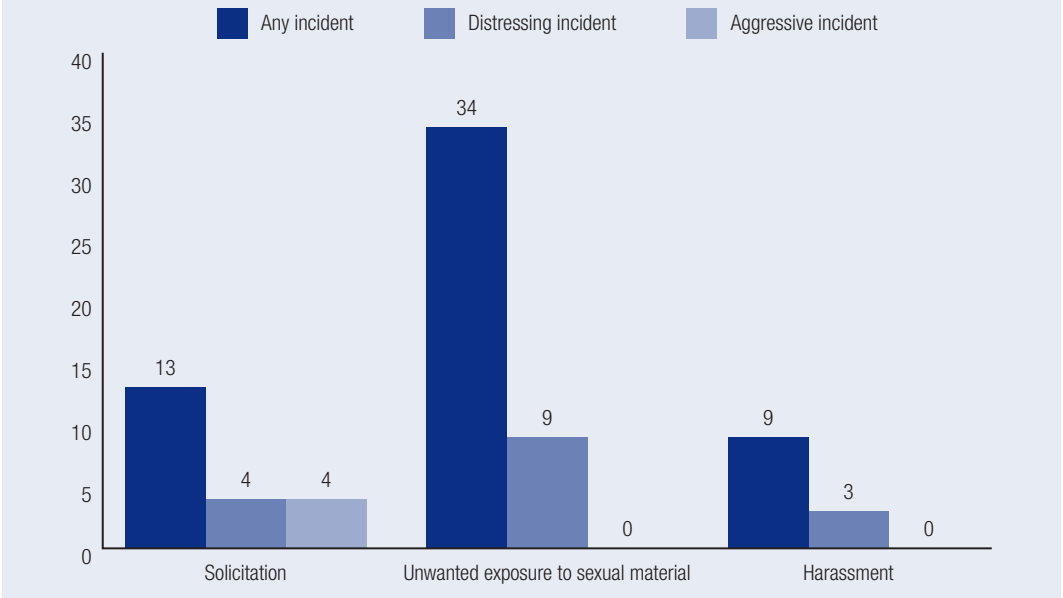
In the 2006 US-based Youth Internet Safety Survey (YISS-2), the 1,500 youths aged between 10 and 17 years who were interviewed reported frequent exposure to unwanted sexual material, sexual solicitations and harassment online (Figure 4; Wolak, Mitchell & Finkelhor 2006). Some four percent of all young 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).

Figure 4 shows the extent to which those surveyed in the Youth Internet Safety Survey were victimised and the seriousness of reported incidents.

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

**Figure 4** Solicitation, unwanted exposure to sexual material and harassment experienced by children (percentage of internet users, 10–17 years old)




Source: Adapted from Wolak, Mitchell and Finkelhor (2006)

- unwanted sexual solicitation only
  - 15 percent reported being victims of unwanted sexual solicitation at least once in the past year and three percent reported at least once a month or more often
  - three percent reported perpetrating unwanted sexual solicitation of others in the past year and one 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.

In the Survey of Children's Use of the Internet that was carried out between December 2005 and January 2006, 848 students aged between nine and 16 years in 21 Irish schools were interviewed (Webwise 2006). The survey found that:

- 19 percent of the respondents indicated they had been harassed, upset, bothered, threatened or embarrassed by someone when chatting online
- seven percent reportedly met someone in real life after knowing them on the internet and 24 percent of these indicated that 'this someone' who introduced themselves as a child on the internet turned out to be an adult.

Professor Greenfield of the University of California Los Angeles also noted that:

> [t]he unsolicited nature of these messages could be daunting for adolescents, particularly younger ones … I was not looking for unsolicited personal messages, sexual or otherwise, but once I decided to enter the chat room, I could not avoid being exposed. I was pursued sexually. I also found aggression, racism and prejudice in this chat room (which no longer exists). Racism and hate are not limited to hate sites (UCLA 2005: unpaginated).

In the 2006 US-based Youth Internet Safety Survey, 1,500 young people between the ages of 10 and 17 years from various backgrounds were interviewed by telephone between March and June 2005. The profile of the survey participants was:

- gender – 49 percent males, 51 percent females
- ethnicity – 76 percent Caucasian, 13 percent African-American, three percent American Indian or Alaskan Native, three percent Asian, one percent 'Other' and three percent unclassified.

In the year prior to the interview, the respondents reported experiencing the following types of victimisation:

- sexual solicitation – request to engage in sexual activities or sexual talk, or to give personal sexual information that was unwanted or (whether wanted or not) made by an adult
- aggressive sexual solicitation – offline contact with the perpetrator through regular mail, by telephone or in person, or attempts at or requests for offline contact
- unwanted exposure to sexual material – without seeking or expecting sexual material, being exposed to pictures of naked people or people having sex when respondents were undertaking online searches, surfing the web, opening email or instant messages, or opening links in email or instant messages
- harassment – threats or other offensive behaviour (excluding sexual solicitation) sent online to the youth or posted online about the youth for others to see
- distressing incident – episode where the youth rated themselves as very or extremely upset or afraid as a result of the incident.

These findings suggest that less than one in 10 respondents reported receiving sexual solicitations of a distressing or aggressive nature. About nine percent suffered unwanted exposure to sexual material of a distressing nature, while nine percent experienced harassment. A number of the respondents 'described chatrooms as unpleasant places attracting unsavoury people [and] were aware of individuals frequenting chatrooms hoping to meet youth for sexual reasons' (Wolak, Mitchell & Finkelhor 2006: 7).

A summary of the profiles of the youth targeted for sexual solicitations or approaches and the perpetrators drawn from the Youth Internet Safety Survey is presented in Table 5.

As seen in Table 5, the exact profile of perpetrators of sexual solicitations and approaches could not be accurately determined, as the youth involved could not be certain of the actual age of the perpetrators.

**Table 5** Profiles of youth targeted for sexual solicitations and approaches, and the perpetrators

| Youth targeted | Perpetrators |
|---|---|
| 70% were females and 30% males.<br><br>81% were 14 years or older.<br><br>3% of 11-year-olds were solicited.<br><br>Aggressive and distressing solicitations were concentrated among older youth with 79% of aggressive incidents and 74% of distressing incidents happening to youth aged 14 and older. | 73% were male and 27% female.<br><br>Females made 16% of aggressive solicitations, and of these perpetrators, 64% were younger than 18 and 36% were aged 18 to 24.<br><br>39% of youth said those committing solicitations were perceived to be adults (18 years or older).<br><br>30% those committing solicitations were perceived to be between 18 and 25 years of age.<br><br>Those committing solicitations perceived to be younger than 18 years of age (because true age cannot be determined online) were identified in a substantial number of incidents; that is, 43% of all solicitations and 44% of aggressive solicitations.<br><br>Youth met 86% of those committing solicitations online, but 14% were people youth knew in person before the solicitation. |

Source: Adapted from Wolak, Mitchell and Finkelhor (2006)

The association between receiving sexual solicitations online by strangers and gender differs across studies. The Irish Survey of Children's Use of the Internet in 2006, for example, reported that boys were more than twice as likely to receive sexual solicitations than girls (Webwise 2006). This contradicts the findings of the Youth Internet Safety Survey (Table 5) in which girls were found to have been targeted more frequently than boys. Regardless, findings from both studies support the view that children were likely to receive sexual solicitations online by strangers.

# Official crime statistics

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 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 et al. 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 data provide an indication of the continually increasing number of cases that have come to the attention of police in Australia, the United Kingdom and the United States. Differences among the numbers of reported offences in these three countries are due partly to different legislative provisions that apply. In the case of grooming, for example, s 15 of the Sexual Offences Act 2003 (UK) in the United Kingdom requires the offender to have met the target child victim or have travelled with the intention of meeting the child. In Australia, this is not a legislative requirement. This and other variations, such as differences in the priorities of police, might explain the considerable differences that exist among the number of online child grooming cases recorded in various countries.

## *Australia*

According to a recent report published by the NSW Parliamentary Library Research Service, there have been 'over 130 completed prosecutions for online procuring, grooming and exposure offences in Australia' (Griffith & Roth 2007: 8):

- 118 cases were prosecuted under Queensland provisions
- four cases were prosecuted under Commonwealth provisions
- eight cases were prosecuted under Western Australian provisions
- one case was prosecuted under Northern Territory provisions.

Griffith and Roth (2007) also reported that there have been at least two prosecutions for offences under South Australian laws, but that it is not clear whether either of these cases involved the use of the internet. Recent cases involving individuals charged in South Australia with online child grooming offences include the following:

- On 5 November 2007, an individual was charged with allegedly using the internet to try to groom a young victim for sex (Would-be pedophile uses net 2007).
- In November 2007, a 40-year-old former Northern Territory police officer was found guilty of using an internet chat room to procure a child for sexual activity and was sentenced to 15 months imprisonment by the South Australian District Court. He will be eligible for parole after serving seven months imprisonment (AAP 2007a).
- In September 2007, a South Australian police officer was reportedly suspended from duty after being accused of using the internet to groom a child for sex (SA police officer charged with internet grooming 2007).

This information confirms that online grooming is being investigated by police, resulting in prosecutions in Australia under both state/territory as well as Commonwealth legislation.

## *United Kingdom*

The number of sexual grooming offences recorded by police in England and Wales is presented in Table 6.The UK-based Child Exploitation and Online Protection Centre has also received '[an] average [of] 10 reports a month concerning children between the ages of 8 and 11 years – the majority of which relate to online grooming' (UK CEOP 2007a: 3).

In the United Kingdom, therefore, it appears that the number of police investigations into online grooming has increased considerably in recent years.

**Table 6** Sexual grooming offences recorded in England and Wales, 2003–04 to 2006–07 (number)

| | 2003–04 | 2004–05 | 2005–06 | 2006–07 |
|---|---|---|---|---|
| Cases reported | 185 | 186 (185) [a] | 237 | 322 |

a: Singapore Home Ministry of Affairs (2007b) reported that the number of sexual grooming offences recorded in England and Wales in 2004–05 was 185

Source: The statistics for 2004 to 2007 were sourced from Nicholas, Kershaw and Walker (2007) and Singapore Ministry of Home Affairs (2007b), and the statistics for 2003–04 from UK Home Office (2006) and Singapore Ministry of Home Affairs (2007b)

**Table 7** Pornography offences and any accompanying offences by incident type, United States, 1997–2000 (percentage)

| | Juvenile victim pornography (n=111) | Child exploitation pornography (n=566) | Adult pornography (n=1,792) |
|---|---|---|---|
| **Any accompanying offence?** | | | |
| Yes | 100 | 4 | 4 |
| No | 0 | 96 | 96 |
| **Any violent or sexual offence?** | | | |
| Yes | 95 | 1 | 1 |
| No | 5 | 99 | 99 |

Note: Derived from the FBI's National Incident-based Reporting System (http://www.fbi.gov/ucr/ucr.htm#nibrs)

Source: Based on Finkelhor and Ormrod (2004)

**Table 8** Reports of online enticement of children received by the US National Center for Missing & Exploited Children through its CyberTipline, 1998–2006 (number)

| | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 |
|---|---|---|---|---|---|---|---|---|---|
| Cases reported | 707 | 1,139 | 1,458 | 1,540 | 2,782 | 2,123 | 2,605 | 2,664 | 6,384 |

Source: NCMEC (2007b)

## *United States*

Table 7 presents statistics on the number of online child exploitation and pornography cases investigated in the United States over the period 1997 to 2000. The offence classifications used in Table 7 are:

- juvenile victim pornography incidents – cases that involve the production of child pornography using identifiable children (child victimisation is usually regarded as sexual abuse and is recorded in the FBI's National Incident-based Reporting System as a forcible sex offence)
- child exploitation pornography incidents – cases in which child exploitation is recorded but additional offences against specified juvenile victims are not included. It is assumed that these pornography offences involve the depiction of juveniles who cannot be identified or recorded as individual victims
- adult pornography incidents – incidents that do not involve juveniles either as identifiable victims or as the victims of child exploitation.

The number of annual reports of online child exploitation (including online child grooming) made to the US-based National Center for Missing & Exploited Children through its CyberTipline (a hotline for reporting child sexual exploitation at http://www.cybertipline.com/) increased from 4,560 in 1998 to 76,584 by the end of 2006 (NCMEC 2007b). The statistics relating to the category of 'Online enticement of children for sexual acts' are presented in Table 8 and show a substantial increase since 1998, particularly over the 12 months since 2005.

The large number of child pornography and child grooming reports received by the National Center for Missing & Exploited Children is, arguably, due to the ease with which child pornography materials can be accessed online and the opportunities that exist for

grooming children via the internet. In addition, the statutory obligation on ISPs to report child pornography on their systems to the National Center for Missing & Exploited Children may have inflated the figures from earlier years when this reporting obligation was not present. The current reporting obligation is found in 42 USC 13032(B)(1):

> Whoever, while engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce, obtains knowledge of facts or circumstances from which a violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 of title 18, involving child pornography (as defined in section 2256 of that title), or a violation of section 1466A of that title, is apparent, shall, as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children, which shall forward that report to a law enforcement agency or agencies designated by the Attorney General.

Although US-based ISPs are required to report child pornography on their systems to the National Center for Missing & Exploited Children, it is 'ambiguous whether mobile phone carriers, social networking websites, and web hosting companies are also required to report [to the National Center for Missing & Exploited Children]'. As a result, there has been a call for the statute to be amended to include mobile phone carriers, social networking websites and web hosting companies in the mandatory reporting requirement (US House of Representatives Committee on Energy and Commerce, Republicans 2007: 5).

The National Juvenile Online Victimization study was a survey of 2,574 police investigators conducted over a 12-month period beginning on 1 July 2000. Structured interviews were conducted with investigators from local, county, state and two federal law enforcement agencies in the United States about internet-related sexual offences committed against minors. It was found that there had been an estimated 1,713 arrests for possession of child pornography materials. Of these, some 36 percent of offenders had shown or given child pornography to identified child victims or undercover investigators posing online as minors (Wolak, Finkelhor & Mitchell 2005). Of these, 36 percent (25% of dual offenders defined as offenders who sexually victimised children and possessed child pornography, with both crimes discovered in the same investigation) had reportedly shown or given child pornography to identified victims with the intention of grooming. An additional two percent of dual offenders were also found to have shown or given child pornography to identified victims, although investigators did not know whether the offenders' purpose was to groom children. The remaining nine percent of dual offenders had sent child pornography to undercover investigators posing online as minors.

# Case studies

To provide an indication of how child grooming occurs and the penalties that have been imposed on convicted offenders, a series of nine case studies has been compiled. These were taken from authorised law reports or official websites of relevant government agencies. Following an outline of the offences alleged in each case, a brief summary is provided of the circumstances relevant to the grooming activities and the penalties imposed, where appropriate.

## *Case 1 (Queensland)*

On 23 April 2005, the offender entered a chat room on the internet and made contact with a police officer posing as a 13-year-old girl. The offender believed he was communicating with a 13-year-old. He said he was 29. He engaged in sexually inquisitive and explicit discussion with her, including giving her detailed, lewd and graphic instructions on how to masturbate herself. She presented as sexually uninformed, sometimes nervous and reluctant. Then via a web camera, he displayed to her a moving, real-time image of himself masturbating – apparently over an appreciable period. The communication covered more than one hour. The applicant engaged in similar conversation with the same supposed child on 31 July 2005, and again displayed a real-time image of himself masturbating – again over an appreciable rather than a fleeting period. This time

he said he was 18. This communication covered about an hour. On that occasion he also asked the person with whom he was communicating to give him the names of any of her friends, then online, so he could talk to them too, and he later communicated similarly with one such 'friend', believing he was speaking to a 13-year-old girl (*R v H* [2006] QCA 20).

The offender was sentenced to 18 months imprisonment, suspended after three months imprisonment for an operational period of two years.

## *Case 2 (New South Wales)*

This offender contacted the same chat service as in Case 1 on 15 June 2006 but on this occasion he spoke with a female undercover police officer conducting an operation. She introduced herself and said she was 15 and wanted to have a talk. The offender sent the police officer a message stating that he was willing to pay her $100 if she performed fellatio on him and $200 (for what I understand to be penile penetration of her vagina). After a number of voice messages were received, the undercover police officer stated that she had not performed fellatio before. She told the offender again she was 15 but would only meet when her mother had left for work. She provided the offender with a mobile phone number stating that the offender could call her in about 20 minutes after her mother left for work. Twenty minutes later the offender called her and entered into further sexual conversations and arranged to meet her at an address in Redfern (*R v P* [2007] NSWCCA 157).

The offender was taken into custody on the same day, 15 June 2006. He was subsequently sentenced to three years imprisonment on each of two counts of offences against s 474.26 of the *Criminal Code Act 1995* (Cth). The court imposed a recognisance release order that the offender be released at the expiration of one year and three months of the term of imprisonment, namely on 14 September 2007, on his entering into a recognisance, subject to conditions including that he be of good behaviour for a period of three years from that date and accept the supervision and guidance of officers of the NSW Probation and Parole Service for a period of two years after his release.

## *Case 3 (United Kingdom)*

The offender, aged 52, posed as a 17-year-old boy online and targeted young, immature and vulnerable girls, in particular those who had not lost their virginity. The victim was one such girl. She was aged 13 at the time of the offences. She spoke to the offender for about six months in an internet chat room, before agreeing to meet him in September 2005. He drove her to an isolated spot and had sex with her. He had worn a condom which had burst. The offender saw the victim on several occasions afterwards, and continued to send text messages. The victim told her family, however, and the offender was arrested. His DNA was recovered from the victim's underwear. The victim was diagnosed with chlamydia, a sexually transmitted disease, and also alopecia brought on by stress. The offender pleaded guilty to one count of rape and to a count of meeting a child following sexual grooming, contrary to s 15 of the Sexual Offences Act 2003 (UK) (*R v K* [2007] EWCA Crim 1411; [2007] All ER [D] 25 [Aug]).

The offender was sentenced to eight years imprisonment on the count of rape and four years on the other count, both sentences to be served concurrently. He was also disqualified from working with children under s 28 of the Criminal Justice and Court Services Act 2000 (UK) for an indefinite period. A sexual offences prevention order was made to last until further order under s 104 of the Sexual Offences Act 2003 (UK).

## *Case 4 (United Kingdom)*

The offender met the victim ('E') through her friend at his workplace. The offender subsequently gave E a mobile phone, which was used to communicate between them. A number of the calls that took place between E and the appellant were suggestive or of an intimate nature. Their mobile telephones were analysed. The analysis showed that E had sent the appellant intimate text messages. Although it was noted that the victim was a willing partner and had initiated the contact between herself and the offender on that particular occasion, there was no evidence that E was in any way harmed or adversely affected by the experience. Further, no sexual act occurred between the offender and E. The offender was sentenced to 3.5 years imprisonment for

meeting a child following a sexual grooming and child abduction (*R v M* [2007] 1 Cr. App. R. [S.] 16).

## *Case 5 (United States)*

The offender met a 15-year-old female victim through the internet web site myspace.com. The victim's MySpace profile identified her as being 15 years of age, and the offender's profile identified him as being 26 years of age. The offender and the victim started communicating often via the internet. Some of their conversations were sexual in nature. The offender and the victim communicated with each other about getting together and engaging in sexual conduct. The offender was subsequently sentenced to 36 months imprisonment, with 10 years supervised release, for travelling in interstate commerce for the purpose of engaging in illicit sexual conduct (US DoJ 2007c).

## *Case 6 (United States)*

On 9 October 2007, a 42-year-old man was sentenced in the Federal Court in Statesville to 10 years imprisonment 'for using a computer via the Internet, to attempt to persuade an individual whom he believed had not attained the age of 18 years, to engage in sexual activity'. The court also ordered the offender to register as a sexual offender (US DoJ 2007d: unpaginated).

## *Case 7 (United States)*

On 3 October 2006, an offender was sentenced to 12 years and four months imprisonment for 'traveling in interstate commerce with intent to engage in illicit sexual contact with a minor', committed in October 2006 (US DoJ 2007e: unpaginated). Some 14 months later, on 14 December 2007, he was further sentenced to 20 years imprisonment for possession of child pornography.

The offender pleaded guilty on 28 September 2007 to one count of possessing child pornography. His guilty plea stemmed from a lead obtained by law enforcement after he was arrested in the Northern District of Alabama for another child exploitation crime. In that case, he travelled from his home in Meridian to Birmingham, Alabama, to have sex with an 11-year-old girl whom he believed was being prostituted. In fact, the offender had been communicating with an undercover law enforcement officer when he responded to an advertisement on the Craigslist website and sought the illegal sexual liaison. While investigating his unlawful travel and online activities, law enforcement officers discovered that he possessed sexually explicit images of minors at his Meridian home. In October 2006, he was sentenced to 12 years and four months in prison for his illegal activities in the Northern District of Alabama. He was then indicted on 7 May 2007 and pleaded guilty. On his release from prison, he will be required to register as a sex offender in any jurisdiction where he lives, works or goes to school and will be prohibited from having any contact with any children under the age of 18 (US DoJ 2007f).

## *Case 8 (United States)*

In January 2006, the offender was alleged to have engaged in numerous conversations with various people whom he believed to be teenage girls under the age of 16 but who were, in fact, undercover law enforcement officers in Vermont and Connecticut posing as girls (US DoJ 2008b). The offender then arranged to meet with one of the people whom he thought to be a 14-year-old girl for the purpose of engaging in unlawful sexual activity. The offender was arrested after arriving at the designated meeting place. He was subsequently released on a US$300,000 surety bond. The Order Setting Conditions of Release specified that the offender was to submit to electronic monitoring, to have no use of the internet and to have no unsupervised contact with anyone under the age of 18, among other restrictions.

Shortly after his release on the bond, the Connecticut Computer Crimes Task Force received information from a detective with the Newtown Police Department regarding internet communications received from a person whose screen name was that of the offender. Before his arrest in November 2006, the offender had been communicating via instant messaging with the detective who, acting in an undercover capacity, had been posing online as a female under the age of 18. On 11 May 2007, the offender initiated contact with the detective via instant messaging to renew their

online conversation. In the course of a subsequent online conversation on 14 May 2007, he admitted that he 'was arrested for trying to meet a young girl', and that 'they still have my computer'. The offender then informed the detective that he 'got a new one' (referring to a computer). He further informed the detective 'I am home but not supposed to be on a computer'. The 14 May 2007 online conversations progressed, with the offender and the undercover detective discussing plans for meeting in person. At one point during the conversation, the offender asked 'do you have any condoms?' (US DoJ 2008b: unpaginated).

The offender was rearrested in May 2007 and his bond revoked. In January 2008, the offender was sentenced to 123 months imprisonment for attempting to entice a minor to engage in sexual activity, a concurrent 10-year term for possessing child pornography, and an additional three months imprisonment for violating his bond (US DoJ 2008b). The offender was also required to register as a sex offender on his release from prison.

## *Case 9 (United States)*

In November 2006, the offender allegedly contacted a minor using myspace.com and managed to convince the child to travel to Bluefield, West Virginia, for the purpose of engaging in prostitution. The child was then transported to Miami, Florida, by the offender for the purpose of continuing to engage the child in prostitution. The offender was subsequently arrested and sentenced to 188 months imprisonment for charges related to child exploitation in January 2008. The offender was also required to register as a sex offender and serve a term of eight years supervised release after his release from prison (US DoJ 2008a).

## *Discussion*

Key facts from these case studies are summarised in Table 9. It is apparent that sexual offenders can use various ICT to facilitate their grooming activities, and often carry them out over many months prior to arranging a physical meeting.

**Table 9** Categorisation of recent online child grooming cases

| Case study no. | Location | Communication medium when first met | Known to offender before the grooming process? | Duration of grooming process | Sex with victim? |
|---|---|---|---|---|---|
| 1 | Australia | IRC room | No | Three months | No ('victim' was an undercover police officer) |
| 2 | Australia | Phone chat services | No | One day | No ('victim' was an undercover police officer) |
| 3 | United Kingdom | IRC room | No | Six months | Yes (victim was 13 years of age at the time of offence) |
| 4 | United Kingdom | Mobile phone | Yes | Three months | No |
| 5 | United States | Online networking site (MySpace) | No | One month | Yes (victim was 15 years of age at the time of offence) |
| 6 | United States | Online networking site | No | Unknown | No ('victim' was an undercover police officer) |
| 7 | United States | Online website (Craigslist) | No | Unknown | No ('victim' was an undercover police officer) |
| 8 | United States | Instant messaging | No | 10 months or longer (as the offender resumed communications with one of his 'victims' when he was released on bond) | No ('victims' were undercover police officers) |
| 9 | United States | Online networking site (MySpace) | No | Less than a month | Not mentioned but the victim was directed by the offender to engage in child prostitution |

The internet offers police an excellent medium for undercover operations, and they have used it considerably to track down and snare would-be child molesters or child pornographers. Methods used include officers entering chat rooms and posing as children seeking excitement, setting up false websites offering illegal pornography, and using well-publicised internet sting operations to create the impression that the internet is a risky place for sexual predators in which their hidden identities can be tracked and discovered (Newman 2007).

Case studies 1, 2, 6, 7 and 8 show that a real child need not be involved in the commission of an offence, as child grooming can be viewed as an act preliminary to commission of a sexual offence. Section 218A(7) of the *Criminal Code Act 1899* (Qld), for example, states that 'it does not matter that the person is a fictitious person represented to the adult as a real person'. Similar provisions are found in s 474.28(9) of the *Criminal Code Act 1995* (Cth), and s 66EB(5) of the *Crimes Act 1900* (NSW).

It is unknown how many would-be sexual offenders and actual sexual offenders have been deterred from trying to contact children online as a result of covert sting operations. The number of individuals involved in online child exploitation is also difficult to determine, although it appears to be substantial. Often figures are given for 'records' or 'subscribers' uncovered by police investigators. This does not equate to the actual number of individuals involved. Where separate records relate to the same individual, then the number of people actually involved will be smaller than the number of 'records' or 'subscribers'.

A number of problems have arisen for police in mounting covert undercover operations to detect and arrest child grooming offenders. In some jurisdictions, such as the United States, the defence of entrapment can be raised, although this is rarely successful in online child exploitation cases (Smith, Grabosky & Urbas 2004). In some legal systems, such as Australia and the United Kingdom, there is no defence of entrapment. It is up to the judge to rule on the admissibility of evidence obtained through 'unconventional' investigative techniques.

> For an entrapment defence to succeed in the United States, the defence must establish that the government originated the criminal design, that the disposition to commit the offence was implanted in the mind of an innocent person, and that the defendant committed the crime at the urging of the government. To defeat a defence of entrapment, it is sufficient to demonstrate that the accused was predisposed to commit the crime. While some individuals might visit 'pre-teen sex' chat rooms for research purposes, out of idle curiosity, or indeed, for purposes of fantasy, many have illegal motives. The prosecution must prove beyond reasonable doubt that the defendant was disposed to commit the criminal act prior to the first time he or she was approached by government agents. This is less difficult when the accused is apparently a habitual visitor in some of the more questionable corners of cyberspace (Smith, Grabosky & Urbas 2004: 81).

Some have argued that covert sting operations are ineffective in preventing serious child exploitation. Fulda, for example, argued that:

> it [is] necessary to cite empirical findings as to whether persons caught in Internet stings are generally dangerous and as to whether genuinely dangerous pedophiles are generally susceptible to being caught in such stings. Since the answer to both these questions is 'No', such stings are not only preventive detention, but they are *epistemically unjustified* preventive detention (Fulda 2007: 64).

Fulda went on to suggest that offenders identified in covert sting operations should:

> not be arrested and tried for the sting itself, but that being implicated in the sting merely provides sufficient evidence of the particularized suspicion necessary for a search warrant to be granted, and that if his premises and computers are searched and no evidence of actual criminality is found, he is to be released and sternly warned, but neither incarcerated nor convicted of a crime, for there is no evidence that he has done anything whatsoever (Fulda 2007: 82).

Further research is needed to determine the objective seriousness of the incidents in which offenders caught in sting operations are involved. Evidence is needed, for example, of the extent to which those caught in sting operations are first-time offenders or have extensive prior experience.

Similarly, evidence is needed of whether those engaging in grooming have actually met with their victims in the past and committed offences, or have committed other offences such as possession of obscene materials. Care is also needed to ensure that police do not engage in activities that could amount to entrapment that may be proscribed in certain countries.

Another defence raised in a number of child grooming cases in the United States relies on the accused claiming that their actions were an expression of 'fantasy' and not indicative of real intentions. One case in which the defence succeeded is:

> In March 1999, a 34-year-old IT executive logged into an Internet chat room called dad&daughtersex.log and made contact with one 'KrisLA,' who identified herself as a thirteen-year-old girl. Over the next several months, the executive, who was using the nickname 'Hotseattle', expressed his interest in meeting KrisLA in Los Angeles and engaging in sexual acts with her. He claimed to be 'totally for real', and not just engaging in fantasy behavior. They arranged to meet at the Santa Monica Pier on September 16th. Unfortunately for 'Hotseattle,' who was arrested upon his arrival in Santa Monica, he had been corresponding not with a 13-year-old girl but rather with one Bruce Applin, a special agent of the Federal Bureau of Investigation.
>
> The accused was indicted on three felony counts … He pleaded not guilty to the three counts, and claimed that he had no intention of having an illicit encounter with a child. Rather, he claimed to have been operating in the online fantasy world of cyberspace, that he visited fantasy-based chat rooms to relieve stress, and that he assumed most people there were role-playing. Therefore, his travel to Santa Monica was not for the purpose of committing a crime. The defendant argued that almost everyone in chat rooms engages in what he called 'real-time' fiction, or role-playing, and that the person he would meet in Santa Monica could just as easily have been a 40-year-old woman. An expert witness for the defence stated that as many as two-thirds of participants in internet chat rooms (in addition to undercover police investigators) state a false age or sex. After four days of deliberation, the jury found the defendant guilty of possessing child pornography, but was unable to reach a verdict on the other charges. All but one of the men on the jury accepted the fantasy defence, while the six women did not (Smith, Grabosky & Urbas 2004: 77).

Cases such as this demonstrate the difficulties that police and prosecutors face in investigating cases of online grooming of children. Over time, as the jurisprudence develops globally, prosecutions may become less difficult, but for the moment they remain somewhat burdensome, with their outcomes often uncertain. This, of course, has implications for the general deterrence effects that criminal action has in these cases.

# Victim profiles

A number of studies have sought to determine the demographic characteristics of the victims of sexual abuse, including the victims of internet-related exploitation such as online grooming. Research has also sought to establish the harmful consequences of exploitation and abuse, many of which endure throughout adulthood. The following discussion reviews the principal studies that show that children of all ages have been victimised, although adolescents tend to be those most often at risk of online grooming. However, various methodological difficulties are present in a number of these studies as sexual abuse of young children is under-reported and young boys, in particular, are often unwilling to report their experiences. Self-reports of victimisation often, therefore, underrepresent the true extent of the problem and distort the true profile of victims. Nonetheless, it is clear that victims of both conventional sexual abuse (i.e. non-online sexual abuse) and online sexual abuse come from all walks of life in terms of social class, geographic area, and ethnic and cultural background.

> Children and adolescents, regardless of their race, culture, or economic status, appear to be at approximately equal risk for sexual victimization. Statistics show that girls are sexually abused more often than boys are. However, boys' and, later, men's, tendency not to report their victimization may affect these statistics (McDaniel 2001: 205).

## Age

In terms of the age of victims of sexual exploitation, a number of studies have documented the wide age range of children at risk. Lang and Frenzel (1988), for example, interviewed 52 adult males convicted of intra-familial sexual contact with their daughters (incest offenders) and 50 males convicted of stranger-perpetrated sexual assault against female minors under the age of 14 during the course of their in-hospital treatment in the Sex Offender Program at Alberta Hospital Edmonton, Canada. It was found that sexual abuse often began with fondling preschool-aged children, but shifted to oral–genital contact or mutual masturbation in pubertal boys or girls. Abuse then progressed to vaginal or anal penetration as children reached early to late adolescence. Most victims were pubertal girls with a mean age of between seven and 12 years, although preschool children of both sexes and even infants were not immune from sexual abuse (Lang & Frenzel 1988). Although the study by Lang and Frenzel (1988) was carried out two decades ago, sexual abuse of pubertal girls is still reported today.

In 2003, Wells and Mitchell (2007) surveyed 31,382 US-based professionals predominantly from the social work, psychology and psychiatry industries. Participants were randomly selected from their respective professional organisations' membership lists. They were asked to complete a postal survey

in which they were required to indicate if their clients over the preceding five years had reported any problematic internet experiences such as exposure to adult pornography, child pornography, sexual approaches, sexual solicitations or sexual behaviour, romantic or sexual relationships, close relationships or friendships, fraud or other scams, gaming or role-playing, racist or hate material, violent material and aggressive behaviour such as harassment and stalking.

Of the 7,841 professionals who responded, 7,232 (92 percent) had provided treatment to patients who had been exposed to any of these experiences during the preceding five-year period. Some 2,170 respondents completed a follow-up survey that involved semi-structured interviews and of these, 512 (24%) reported incidents involving people under the age of 18. The findings relating to these individuals are summarised in Table 10.

**Table 10** Demographic characteristics of people under the age of 18 with internet-related problems (percentage)

| Characteristics | People under 18 years of age (n=512) | People under 18 years of age who were victims of sexual exploitation (n=132) | People under 18 years of age who had other internet-related problems [a] (n=380) |
|---|---|---|---|
| **Gender** | | | |
| Male | 57 | 23 | 68 |
| Female | 43 | 77 | 32 |
| **Age** | | | |
| 6–9 years | 1 | 1 | 2 |
| 10–12 years | 17 | 12 | 19 |
| 13–14 years | 32 | 34 | 31 |
| 15–17 years | 50 | 53 | 49 |
| **Race/ethnicity** | | | |
| European-American | 91 | 90 | 91 |
| African-American | 3 | 5 | 3 |
| Hispanic or Latino | 3 | 4 | 3 |
| Asian or Pacific Islander | 3 | 2 | 4 |
| Native American or Alaska Native | 1 | 1 | 1 |
| In school at time of internet problem | 92 | 96 | 90 |
| **Referral** | | | |
| Family member | 31 | 33 | 29 |
| Mental health professional | 27 | 27 | 27 |
| Self-referred | 11 | 10 | 12 |
| Legal professional | 11 | 14 | 9 |
| Friend, neighbour or acquaintance | 5 | 4 | 5 |
| Someone else (school personnel, insurance company, clergy and employer) | 16 | 11 | 17 |
| **Authorities involved** | | | |
| Some other authority involved | 53 | 63 | 49 |
| School | 30 | 24 | 33 |
| Local, state or county law enforcement | 25 | 42 | 19 |
| Child protective services | 14 | 26 | 9 |
| Federal law enforcement | 5 | 10 | 3 |
| ISP | 5 | 8 | 4 |

a: Internet-related problems include problems of internet over-usage

Source: Wells and Mitchell (2007)

Table 10 shows that most sexual assault victims were pubertal girls, most often aged between 13 and 17 years. Preschool children of both sexes were, however, not immune from sexual abuse. The study also found that online sexual exploitation victims were more likely than youth with other internet-related problems to be female, but a notable minority (one-quarter) of victims were male (Wells & Mitchell 2007).

Similarly, in the National Juvenile Online Victimization survey by Wolak, Mitchell and Finkelhor (2003), it was found that a majority of the offenders arrested for possession of child exploitation materials were men. Most of these offenders possessed images of children who had not yet reached puberty:

- 83 percent had images of children between the ages of six and 12
- 39 percent had images of three to five-year-old children
- 19 percent had images of toddlers or infants younger than three.

# Impact

There is clear evidence in the academic literature that sexual abuse during childhood creates long-term problems for those who have been victimised. Many exhibit serious mental health problems as well as behaviour disorders and addictions. This occurs not only with children who experience offline sexual abuse, but also online exploitation.

For example, Watkins and Bentovim 1992 (cited in Craissati, McClurg & Browne 2002) found evidence to demonstrate that the long-term effects of childhood sexual victimisation are associated with psychological disorders in adult males, with particular risks relating to alcohol and drug misuse. Others including Harrison (2006) have also highlighted the wide-ranging psychological and interpersonal problems found in victims of child exploitation.

Psychiatric disorders relating to anxiety, post-traumatic stress disorder, mood and substance abuse have all been documented. These may lead to other issues such as post-traumatic stress disorders, cognitive disorders, emotional pain, avoidance behaviours, low self-esteem, guilt, self-blame, delinquency, substance abuse, vulnerability to repeated victimisation, interpersonal difficulties, dissociation and disbelief about the abuse, functional amnesia and effects on relationships with others.

In a study by Westenberg and Garnefski (2003), 81 adolescents aged between 11 and 18 years, comprising 46 boys and 35 girls, were asked to anonymously fill in a questionnaire. At the time of the study, the participants were either placed with a family supervision agency or were receiving Youth After-care and Resettlement Service (penal unit) in the Netherlands. The questionnaire was designed to measure experiences of child abuse (physical abuse, sexual abuse and low care) and associated depressive symptoms. The study found that:

- 42.3 percent of the adolescents classified as having behavioural problems with depressive symptoms that fulfilled the criteria of a major depressive episode as defined in the *Diagnostic and statistical manual of mental disorder*s (4th edition), reported experiences of sexual abuse, compared with 9.8 percent of the non-major depressive episode group)
- 20.8 percent of all the adolescents with behavioural problems reported experiences of sexual abuse as a child. Of these, only one of the victims was a boy. It was concluded that this might be the result of boys being less willing to reveal such experiences because of sex role socialisation (Hussey, Strom & Singer 1992 cited in Westenberg & Garnefski 2003). McDaniel (2001) also noted that male victims were less likely to report their victimisation.

Female victims tended to exhibit more internalised behaviours such as depression, anxiety, post-traumatic stress and suicidal ideation (Table 12), while male sexual victims were more likely to have externalised problems such as oppositional behaviour, aggression, substance abuse and impulsivity. They also demonstrate symptoms of disturbed adult sexual functioning, poor social adjustment, confusion over their sexual identity (if abused by offenders of the same gender), inappropriate attempts to reassert their masculinity and recapitulation of the abuse experience (Table 13).

For example, 'a male perpetrator might give his male victim serious doubts about his sexual identity' (Gianotten 1988 cited in Westenberg & Garnefski 2003: 207).

In Wells and Mitchell's study (2007), 61 percent of clients aged under 18 years who were victims of online sexual exploitation had a current, and 68 percent had a lifetime, diagnosis that fulfilled the criteria of various disorders in the *Diagnostic and statistical manual of mental disorders* (American Psychiatric Association 1994; Table 11).

In the same study, Wells and Mitchell (2007) found that 101 of the female clients who were victims of sexual exploitation had problems relating to depression (71%), anxiety or phobias (45%), specific life stressors (34%), suicidal ideation or attempted suicide (27%), parent–child conflict (83%), disciplinary problems at home (47%), social withdrawal (35%), trouble making friends (31%), failing grades at school (47%), disciplinary problems at school (30%), sexual victimisation (56%) and sexual acting out (35%) (Table 12).

**Table 11** Current and lifetime Diagnostic and Statistical Manual of Mental Disorders among victims of online sexual exploitation (percentage)

| | People under 18 years of age (n=512) | | People under 18 years of age who were victims of sexual exploitation (n=132) | | People under 18 years of age who had other internet-related problems (n=380) | |
|---|---|---|---|---|---|---|
| DSM-IV disorder | Current DSM-IV diagnosis (n=297) | Lifetime DSM-IV diagnosis (n=338) | Current DSM-IV diagnosis (n=81) | Lifetime DSM-IV diagnosis (n=90) | Current DSM-IV diagnosis (n=216) | Lifetime DSM-IV diagnosis (n=248) |
| **Mood disorder** | 44 | 52 | 41 | 49 | 45 | 54 |
| Depressive | 25 | 45 | 22 | 45 | 27 | 45 |
| Bipolar | 3 | 8 | 2 | 5 | 3 | 9 |
| **Disorders first diagnosed in childhood** | 24 | 33 | 23 | 28 | 28 | 35 |
| Conduct and disruptive | 10 | 14 | 9 | 13 | 10 | 15 |
| Attention deficit | 5 | 17 | 5 | 11 | 5 | 19 |
| Pervasive developmental | 2 | 5 | 1 | 1 | 2 | 6 |
| Learning | 1 | 3 | 1 | 3 | 1 | 3 |
| Learning retardation | 0 | 1 | 0 | 2 | 0 | 1 |
| Anxiety disorders | 21 | 24 | 30 | 31 | 19 | 22 |
| **Post-traumatic stress disorder** | 6 | 8 | 16 | 19 | 3 | 4 |
| Obsessive-compulsive | 3 | 6 | 1 | 3 | 4 | 7 |
| Other anxiety | 7 | 12 | 5 | 11 | 8 | 13 |
| Adjustment disorders | 12 | 12 | 16 | 17 | 10 | 10 |
| Personality disorders | 6 | 6 | 9 | 9 | 5 | 4 |
| Substance-related disorders | 5 | 5 | 9 | 9 | 4 | 4 |
| Other conditions that may be focus of clinical attention | 7 | 6 | 5 | 4 | 7 | 7 |
| Sexual and gender identity disorders | 3 | 3 | 5 | 4 | 2 | 2 |
| Impulse-control disorders | 3 | 3 | 2 | 2 | 4 | 4 |
| Schizophrenia and other psychotic disorders | 2 | 2 | 1 | 1 | 2 | 2 |
| Not ascertainable | 11 | 10 | 11 | 9 | 11 | 10 |

Note: 512 respondents who were also mental health professionals reported cases involving people under the age of 18

Source: Wells and Mitchell (2007)

**Table 12** Co-occurring mental health issues among females under 18 years of age (percentage)

| Co-occurring mental health issue | All females under 18 years of age (n=221) | Females under 18 years of age who were victims of sexual exploitation (n=101) | Females under 18 years of age who had other internet-related problems (n=120) |
|---|---|---|---|
| **Mental and physical health problems** | | | |
| Depression | 72 | 71 | 73 |
| Anxiety or other phobias | 46 | 45 | 47 |
| Specific life stressor | 33 | 34 | 32 |
| Suicidal ideation or suicide attempt | 27 | 27 | 27 |
| Somatic complaints or insomnia | 15 | 21 | 11 |
| Diagnosed mental illness | 9 | 8 | 9 |
| Drug or alcohol use | 11 | 14 | 8 |
| Grief | 9 | 10 | 9 |
| Physical disability or chronic health problem | 5 | 3 | 6 |
| **Family and/or relationship problems** | | | |
| Parent–child conflict | 76 | 83 | 70 |
| Disciplinary problems at home | 40 | 47 | 35 |
| Social withdrawal | 33 | 35 | 32 |
| Trouble making friends | 33 | 31 | 36 |
| Running away from home | 14 | 22 | 7 |
| Substance abuse problems within family | 9 | 10 | 8 |
| Marital conflict or divorce | 10 | 8 | 13 |
| **School problems** | | | |
| Failing grades at school | 43 | 47 | 39 |
| Disciplinary problems at school | 30 | 30 | 30 |
| School failure or drop-out | 18 | 19 | 17 |
| **Victimisation** | | | |
| Sexual victimisation | 35 | 56 | 17 |
| Bully victimisation | 13 | 11 | 14 |
| Physical victimisation | 8 | 10 | 6 |
| Emotional victimisation | 7 | 6 | 7 |
| **Aggression** | | | |
| Aggressive acting out or conduct problems | 22 | 23 | 21 |
| Sexual acting out | 25 | 35 | 17 |
| Bullying others | 7 | 6 | 7 |
| Sexual abuse to others | 1 | 2 | 0 |
| Criminal history | 4 | 5 | 3 |

Source: Wells and Mitchell (2007)

Of the 31 males under the age of 18 who were victims of sexual exploitation, 68 percent were diagnosed with depression, 55 percent with anxiety or phobias, 45 percent had specific life stressors, 10 percent had suicidal ideation or attempts at suicide, 81 percent had evidence

**Table 13** Co-occurring mental health issues among males under 18 years of age (percentage)

| Co-occurring mental health issue | Males under 18 years of age (n=291) | Males under 18 years of age who were victims of sexual exploitation (n=31) | Males under 18 years of age who had other internet-related problems (n=260) |
|---|---|---|---|
| **Mental and physical health problems** | | | |
| Depression | 64 | 68 | 64 |
| Anxiety or other phobias | 41 | 55 | 39 |
| Specific life stressor | 33 | 45 | 32 |
| Suicidal ideation or suicide attempt | 12 | 10 | 13 |
| Somatic complaints or insomnia | 10 | 19 | 9 |
| Diagnosed mental illness | 17 | 32 | 15 |
| Drug or alcohol use | 10 | 26 | 9 |
| Grief | 6 | 16 | 5 |
| Physical disability or chronic health problem | 5 | 7 | 4 |
| **Family and/or relationship problems** | | | |
| Parent–child conflict | 72 | 81 | 71 |
| Disciplinary problems at home | 42 | 58 | 40 |
| Social withdrawal | 41 | 39 | 41 |
| Trouble making friends | 38 | 29 | 39 |
| Running away from home | 7 | 35 | 4 |
| Substance abuse problems within family | 9 | 19 | 8 |
| Marital conflict or divorce | 12 | 23 | 11 |
| **School problems** | | | |
| Failing grades at school | 45 | 35 | 46 |
| Disciplinary problems at school | 39 | 45 | 38 |
| School failure or drop-out | 20 | 26 | 19 |
| **Victimisation** | | | |
| Sexual victimisation | 17 | 55 | 12 |
| Bully victimisation | 12 | 19 | 11 |
| Physical victimisation | 10 | 16 | 9 |
| Emotional victimisation | 6 | 10 | 6 |
| **Aggression** | | | |
| Aggressive acting out or conduct problems | 33 | 32 | 33 |
| Sexual acting out | 25 | 48 | 22 |
| Bullying others | 13 | 19 | 12 |
| Sexual abuse to others | 14 | 16 | 13 |
| Criminal history | 10 | 10 | 10 |

Source: Wells and Mitchell (2007)

of parent–child conflict, 58 percent had disciplinary problems at home, 39 percent showed social withdrawal, 29 percent had trouble making friends, 35 percent were failing at school, 45 percent had disciplinary problems at school, 55 percent had experienced sexual

victimisation, and 48 percent were sexually acting out (Table 13).

Findings from Tables 12 and 13 suggest that a high percentage of both male and female clients who were victims of sexual exploitation were diagnosed with depression, anxiety or phobias, or suffered specific life stressors.

## The relationship between victimisation and offending

Prior research has found conflicting evidence of the relationship between sexual victimisation in childhood and subsequent sexual offending in adulthood. Wells and Mitchell (2007), for example, found little evidence to support the proposition that the majority of childhood abuse victims were destined to become adult sexual offenders.

In England, Craissati and McClurg (1996), and Craissati, McClurg and Falla (1999), found that approximately 50 percent of convicted child sexual abusers were themselves sexually victimised, and this finding was similar to that reported by other English studies (Craissati, McClurg & Browne 2002).

In a study by Craissati, McClurg and Browne (2002), 178 participants were assessed over a period of seven years. The participants were 'convicted perpetrators of child sexual abuse in South East London routinely referred to the Challenge Project – a community assessment and treatment program for sex offenders – for psychological reports, prior to sentencing (63 percent) or at the point of release from custody (28 percent)' (Craissati, McClurg & Browne 2002: 229). During the study, a number of psychometric tests were administered to the participants. Of the 178 participants:

- 82 (46%) indicated sexual victimisation in childhood
- 96 (54%) did not report sexual victimisation as a child, and 32 of these participants had no reported history of physical abuse, sexual abuse or emotional neglect.

Although these findings suggest that sexually victimised child abusers were more likely to have a range of psychosexual difficulties and to be recidivists, it should not be assumed that 'the characteristics of convicted sex offenders are comparable with those of the larger group of undetected or unconvicted sex offenders' (Craissati, McClurg & Browne 2002: 234).

Lower prevalence rates were found in a Scottish study in which only 17 percent of 213 child sexual abuse case files involved an offender who was a victim of sexual assault as a child (Dobash, Carnie & Waterhouse 1993 cited in Craissati, McClurg & Browne 2002: 227).

Hanson and Slater (1988; cited in Craissati, McClurg & Browner 2002), in their review of North American studies on the proportion of child sexual abusers who were themselves sexually victimised as children, found that overall, 28 percent of the sex offenders studied were sexually victimised (with studies ranging from between 0 and 67%). However, the rate of sexual victimisation among molesters of young boys was nearly twice as high as that for offenders who molested young girls.

More generally, Weeks and Widom (1998) (cited in Craissati, McClurg & Browne 2002: 227) found that sex offenders were more likely to have been sexually abused (26%) than any other type of offender (12–18%). Langevin (1983; cited in Craissati, McClurg & Browne 2002: 227) found that there were over five times as many victims of child sexual abuse among incest offenders compared with non-offender controls.

Various factors contribute to the likelihood that a victim of child sexual abuse will become an abuser later in life. It is clear that the detrimental impact and the potentially long-term effects of living with the consequences of abuse vary greatly among victims. Factors that contribute to the probability that a victim may become an offender include:

- the age of the child when the abuse began
- the length of time over which the child was abused
- the relationship with the abuser
- the degree of violence used
- whether the child's allegations were believed
- the availability of therapeutic and support networks (Harrison 2006).

There is no research that specifically examines whether victims of online grooming are more or less

likely to become perpetrators themselves, than is the case with other victims of sexual exploitation.

## The involvement of illegal images of abuse

It has been argued that the impact that grooming has on child victims is exacerbated if pornography is involved as this can make incidents more enduring in the minds of victims.

> [T]he chances of being able to help the child to recover from the trauma of the initial involvement in the abuse can be seriously compromised if the child learns or comes to believe that images of them engaged in the abusive behaviour might have been scanned, or converted into a digital format in some other way, for storage on a computer or for transmission between computers e.g. over the Internet. This, in effect, makes the image part of a permanent public record. It could suddenly appear on the screen of their next-door neighbour or classmates. It may become part of the stock that is offered repeatedly for sale by online pornography sites or other types of real world businesses dealing in child pornography (Jones & Skogrand 2005: 18).

Davidson (2007: 27) explained that '[a] child is re-victimised each time their image is accessed, and images on the internet can form a permanent record of abuse'. Harrison also confirmed this view:

> [a]n exacerbating factor for many child victims is knowledge that a record exists of their abuse and the trauma, powerlessness, and shame they have experienced … Th[ose] images may be accessed in perpetuity in cyberspace [and] repeats the children's victimization … and may be used by perpetrators to threaten children and young people into silence and to manipulate their fears that they were responsible (Harrison 2006: 370).

Victims of child exploitation are unlikely to get over their experiences easily. In Victoria recently, an assertion to the contrary by His Honour Judge Michael Kelly in which he suggested that most people 'simply get over it' led to a rebuke by the head of Victoria's Sexual Offences Prosecution Unit, Michelle Williams, SC. Ms Williams submitted that Judge Kelly's comments were 'clearly inappropriate'. At a pre-sentence hearing in September, Judge Kelly dismissed a victim impact statement as 'a waste of time' and questioned suggestions the young man, who was sexually assaulted by an older male from the age of 13, might not recover (Hagan 2007: unpaginated).

Insensitive comments at the time of sentencing by judges or others can further exacerbate the impact of grooming or sexual abuse on child victims. There is, arguably, a need for judicial officers, lawyers and others involved in such cases to be trained to recognise and understand the impact that child sexual abuse has on victims of exploitation.

# Offender profiles

Although the popular image of paedophiles is that they belong to a homogenous group sharing similar characteristics (McAlinden 2006), the reality is that the perpetrators of child sexual abuse come from various demographic, economic and social backgrounds. As noted in a 2006 US hearing investigating the sexual exploitation of children over the internet, some sexual offenders were individuals in respectable professions such as lawyers and teachers.

Tuesday's lead witness was Justin Berry. Beginning at age 13, he was repeatedly sexually exploited over the Internet by a number of men during the course of several years. Berry testified that within minutes of connecting a webcam to his computer, he was contacted by multiple men seeking to establish a sexual connection with him. These men showered money, gifts and attention on Justin, manipulating Justin to perform progressively more graphic sexual activities at their request. Berry's story was first brought to light by Kurt Eichenwald, a reporter with the New York Times who testified with Berry at the hearing. Eichenwald, who wrote several articles for the Times about the online sexual exploitation of children, helped Berry escape his sordid situation and persuaded him to turn over the names of more than 1,500 online pedophiles to federal law enforcement. Eichenwald found that some of the names disclosed by Berry revealed individuals that were true pillars in their respective communities, including paediatricians, lawyers and teachers (Whitfield n.d.: unpaginated).

## Relationship to victim

Offenders are often known acquaintances or family members of the children whom they abuse and may have known their victims in real life prior to using the internet and other communications technologies to further their grooming activities. McDaniel (2001) for example, suggested that between 85 and 95 percent of child sexual abuse cases involved perpetrators whom the child victim already knew or on which they depended. In the National Juvenile Online Victimization survey by Wolak, Mitchell and Finkelhor (2003), it was suggested that of the estimated 2,577 arrests for sex crimes against minors in the 12-month period commencing 1 July 2000, some 490 of the arrests (19%) involved offenders who were either family members or prior acquaintances of the victims (see Table 14 for other findings relating to the demographic characteristics of offenders).

## Age

Sexual offences against children can be committed by both adults and juveniles. The

**Table 14** Demographic characteristics of offenders arrested for possession of child exploitation materials (percentage)

| Demographic | Child exploitation material possessors |
|---|---|
| **Gender** | |
| Male | 100 |
| Female | <1 |
| **Age** | |
| Younger than 18 | 3 |
| 18–25 | 11 |
| 26–39 | 41 |
| 40 or older | 45 |
| **Marital status** | |
| Single, never married | 41 |
| Married or living with partner | 38 |
| Separated or divorced | 20 |
| Widowed | 1 |
| **Education** | |
| Did not finish high school | 5 |
| High-school graduate | 38 |
| Some college education or technical training | 21 |
| College graduate | 16 |
| Post-college degree | 4 |
| Don't know | 17 |
| **Employed full time** | |
| Yes | 73 |
| No | 25 |
| **Income** | |
| Less than US$20,000 | 18 |
| US$20,000–$50,000 | 41 |
| More than US$50,000–$80,000 | 17 |
| More than US$80,000 | 10 |
| Don't know | 13 |
| **Had adult or minor biological children** | |
| Yes | 42 |
| No | 53 |
| **Lived with minor child** | |
| Yes | 34 |
| No | 65 |
| **Had direct access to minors through job, organised youth activity or in home** | |
| Yes | 46 |
| No | 48 |
| Don't know | 6 |
| **Diagnosed mental illness** | |
| Yes | 5 |
| No | 89 |
| Don't know | 6 |
| **Diagnosed sexual disorder** | |
| Yes | 3 |
| No | 87 |
| Don't know | 10 |
| **Evidence of deviant sexual behaviour not involving minors** | |
| Yes | 12 |
| No | 84 |
| **Any known problems with drugs or alcohol** | |
| Yes | 18 |
| No | 75 |
| **Any known incidents of violence** | |
| Yes | 11 |
| No | 85 |
| **Any known prior arrest for non-sexual offence** | |
| Yes | 22 |
| No | 73 |
| **Any known prior arrest for sexual offence committed against a minor** | |
| Yes | 11 |
| No | 87 |

Notes: Weighted sample size=1,713 and unweighted sample size=429. Due to either rounding or missing data, categories may not add up to 100 percent.

Source: Adapted from Wolak, Finkelhor and Mitchell (2005)

1997–2000 crime statistics collected by the FBI's National Incident-based Reporting System, for example, indicated that approximately 2,900 (based on extrapolations from the data) nation-wide crime incidents of pornography with child/juvenile involvement were known to state and local police in 2000, and the proportion of all pornography incidents with child/juvenile involvement increased

from 15 percent in 1997 to 26 percent in 2000 (Finkelhor & Ormrod 2004).

Similar concerns were raised in the 2005–06 annual report of Stop It Now!:

> [u]p to 50 percent of sexual harm toward children is perpetrated by other minors, and half of that is by children under age 13. By failing to offer understanding and treatment to youth with sexual behavior problems, our society compounds the harm done to children – and multiplies it into the future (Stop It Now! 2007: 2).

A summary of juvenile sexual offenders' typologies is presented in Table 15.

**Table 15** Typologies of juvenile sexual offenders

| Classifications |
|---|
| Child molesters |
| Rapists |
| Sexually reactive children |
| Fondlers |
| Paraphiliac offenders |
| Others that do not fit into the above classifications |
| Naive experimenters |
| Under-socialised child exploiters |
| Sexual aggressives |
| Sexual compulsives, disturbed impulsives, group influenced, pseudo-socialised |
| Paedophilic |
| Sexual assault |
| Undifferentiated |

Source: Adapted from Robertiello and Terry (2007)

In the case of juvenile sexual offenders, Vizard (2007: 434) argued that '[s]tudies of general delinquent populations confirm that a "criminogenic family background is common" which subsequently leads to poor behavioural and sexual boundaries in juvenile sexual offenders'.

# Occupation

The following recent online child exploitation cases in Australia provide examples of the occupations of offenders that were generally of a white-collar nature:

- In December 2007, a former police officer, a trainee teacher, a swimming teacher, a truck driver and forensic psychologist were allegedly among the 31 Australians arrested in a nation-wide child pornography ring with overseas links (AAP 2007c; AFP 2007; Buttler 2007; Men refused bail over alleged child porn ring 2007). It was also alleged that some of the offenders arrested were 'involved in grooming the children for sex' (AAP 2007c).
- A former crown prosecutor from New South Wales who was sentenced to a minimum of eight months imprisonment 'after 433 images of child pornography and 31 child pornography videos – some depicting sex acts involving children aged under 10 – were uncovered' in 2006 (Power out on bail: and now DPP faces questions 2007).
- A 56-year-old unemployed man on a disability pension with an equivalent of Year 10 education was sentenced to a net total of two years and 11 months imprisonment for online child grooming and possession of child pornography materials offences (*State of Western Australia v George Singarayar* [WA District Court] 2006).
- A 40-year-old former NT police officer was found guilty of using an internet chat room to procure a child for sexual activity (Lower 2007). In November 2007, he was sentenced to 15 months imprisonment at the South Australian District Court. He will be eligible for parole after seven months (AAP 2007a).
- A 28-year-old US sailor stationed in New South Wales pleaded guilty to using the internet to groom an under-age girl for sex. He was given an 18-month suspended sentence in the NSW District Court (US sailor walks free after grooming 'girl' 2007).
- In November 2007, a 48-year-old former volunteer with the Starlight Children's Foundation Australia, who was also the website administrator of a gay website, was jailed for eight years with a five-year non-parole period for unlawful sexual intercourse, procuring a child for an act of gross indecency and possessing child pornography (Fewster 2007).

**Table 16** Child pornography offender recidivism outcomes based on prior or concurrent criminal histories (percentage)

| Outcome | Child pornography only (n=76) | Contact sexual offending (n=76) |
|---|---|---|
| Any failure of conditional release | 6.6 | 15.8 |
| Any reoffence | 6.6 | 26.3 |
| Any contact sexual reoffence | 1.3 | 9.2 |
| Any non-contact sexual reoffence | 5.3 | 6.6 |
| Any pornography reoffence | 3.9 | 5.3 |

Notes: Data for the study were drawn from adult individuals listed on the Ontario Sex Offender Registry who had ever been convicted for possession, distribution or production of child pornography, as defined by Canadian criminal law. Juvenile sex offenders (defined as individuals aged between 12 and 17 years of age) are not registered unless they are tried as an adult, nor are people who have been pardoned or who have received absolute or conditional discharges at trial.

The age of offenders at the time of their index offences ranged from 19 to 76 years (mean of 38.3 with a standard deviation of 12.2). Their age at first-ever criminal charge or conviction ranged from 13 to 76 years (mean of 32.0 with a standard deviation of 13.2).

Of the full sample (n=201), 135 subjects had only child pornography index and 15 percent had prior child pornography offences

Source: Adapted from Seto and Eke (2005)

# Prior criminal history and recidivism

In terms of recidivism, a significant percentage of sexual offenders do not have prior criminal histories involving offences against minors, or even non-sexual offences. One recent study of recidivism, for example, examined a sample of 201 adult male child pornography offenders (Seto & Eke 2005). It was suggested that child pornography offenders who had committed a prior or concurrent contact sexual offence were significantly more likely to offend again, although only 27 percent of the sample had previous convictions involving child pornography alone (Table 16).

In another study by Waite et al. (2005) based on data obtained from 256 male juvenile sexual offenders, it was found that 50 (19.9%) had a history of sexual abuse. Based on a number of data sources, including the treatment regime provided to offenders, it was found that regardless of the intensity of treatment during incarceration, all offenders had low rates of recidivism. A total of 144 of the subjects received a more intense 'self-contained' treatment program that operated in specialised living units, which were separate from those of the general juvenile incarcerated population. The remaining 112 received the less intense 'prescriptive' program in which subjects remained housed with the general population of juvenile offenders. The results were that:

- seven (4.9%) who received self-contained treatment were rearrested for sexual offences
- five (4.5%) who received prescriptive treatment were rearrested for sexual offences (Waite et al. 2005).

Despite the low adolescent sex recidivism rates based on rearrest rates, the finding of the study indicated that juvenile sexual offenders do 'continue their sexual offending into adulthood' (Waite et al. 2005: 330).

# Co-offenders

Another study based on 1997–2000 crime statistics collected by the FBI's National Incident-based Reporting System also suggested that '[p]ornography incidents of all types were likely to involve a lone offender, typically an adult male' (Finkelhor & Ormrod 2004: 5; Table 17).

# Psychopathology

## *Personality profiles*

Egan, Kavanagh and Blair (2005) argued that people committing sexual offences against children were generally inadequate in their social functioning and

**Table 17** Co-offender status of those arrested for possession of pornography and child exploitation materials (percentage)

| | Juvenile victim pornography [a] | Child exploitation pornography [b] | Adult pornography [c] |
|---|---|---|---|
| **Age** | **(n=108)** | **(n=428)** | **(n=1,201)** |
| Lone adult | 71 | 81 | 76 |
| Multiple adults | 12 | 9 | 8 |
| Multiple mixed age | 3 | 2 | 2 |
| Multiple juveniles | 4 | 1 | 3 |
| Lone juvenile | 10 | 7 | 11 |
| **Gender** | **(n=108)** | **(n=452)** | **(n=1,291)** |
| Lone male | 75 | 81 | 80 |
| Multiple males | 10 | 5 | 7 |
| Multiple mixed gender | 7 | 6 | 4 |
| Multiple females | 1 | 0 | 1 |
| Lone female | 7 | 8 | 8 |

a: Cases that involve the production of child pornography using identifiable children are included in this category (the child victimisation is usually regarded as sexual abuse and is recorded in the National Incident-based Reporting System as a forcible sex offence)

b: Cases in which child exploitation is recorded but additional offences against specified juvenile victims are not included. It is assumed that these pornography offences involve the depiction of juveniles who cannot be identified or recorded as individual victims

c: Incidents that do not involve juveniles either as identifiable victims or with the code for child exploitation

Source: Adapted from Finkelhor and Ormrod (2004)

**Table 18** Typologies of adult sexual offenders

| Offender type | Offender characteristics |
|---|---|
| **Situational offenders** | |
| Regressed | Poor coping skills |
| | Tend to target victims who are easily accessible |
| | Abuse children as a substitute for adult relationships |
| | Since this type of offender is generally not sexually fixated on children, they are at a lower risk of reoffending if treated |
| Morally indiscriminate | No particular preference for children |
| | Tend to use children (or anyone accessible) for their own interests (sexual and otherwise) |
| Sexually indiscriminate | Mainly interested in sexual experimentation and abuse children out of boredom |
| Inadequate | Social misfits who are insecure, have low self-esteem and see relationships with children as their only sexual outlet |
| **Preferential offenders** | |
| Seductive | Court children and give them much affection, love, gifts and enticements to carry on a relationship |
| | Very high risk of recidivism and the risk increases according to the number of victims |
| Fixated | Poor psycho-sexual development, desire affection from children and are compulsively attracted to children |
| Sadistic | Aggressive, sexually excited by violence, target stranger victims and are extremely dangerous |

Source: Adapted from Terry and Tallon (2004)

diverse in their psychopathology. Similar views have been expressed by other psychologists:

> From a psychological profile perspective, psychologist Kimberly Young and psychiatrist Alvin Cooper, two experts who have studied online sexual behaviour, maintain that cyber sex (whether it involves minors or not) is a form of psychopathology and a symptom of neurotic, compulsive behaviour. It is, without question, a type of addiction. Viewed as a type of socio- and psychopathology, cyber child pornography, in particular, is as an element of unhealthy power relations, whereby an adult abuses minors for his own pleasures. These acts of real-world abuse are often set into motion by adults having unhealthy sexual fantasies involving minors. For the most part, the cyber-supported sexual fantasy fulfilment with minors is found in ritualized practices and fixations, primarily of a sadistic sort (Schell et al. 2007: 47).

Adult sexual offenders can be broadly categorised into situational and preferential offenders as described in Table 18.

## *Pathways leading to child sexual offending*

Apart from individual personality characteristics, child sexual offenders carry out a range of patterns of offending. Ward and Siegert 2002 (cited in Middleton et al. 2006) suggested that there are multiple etiological pathways leading to child sexual abuse as described in Table 19.

The subjects in the replication study of Ward and Siegert's pathways model conducted by Middleton et al. (2006) were drawn from 15 Probation Service regions of the National Probation Service of England and Wales. The characteristics of the subjects were:

- 72 male sexual internet offenders with an average age of 43.17 (with a standard deviation of 12.38) were convicted of an index offence involving possessing and/or distributing images of child pornography, or the production, possession and/or distribution of pseudo-sexual images involving child pornography
- 48 percent of the offenders were married or cohabiting, 48 percent were single or divorced and the remaining four percent were widowed.

The study found that internet sexual offenders were a diverse group:

- 60 percent of male subjects (43 cases) displayed signs of dysfunctional psychological disorders
- most of the subjects in the study could be assigned to one of the five etiological pathways in Ward and Siegert's pathways model
- the intimacy deficits pathway was the most populated pathway where subjects had reportedly high levels of emotional loneliness and no problems in managing negative emotions, and did not report high levels of emotional congruence with children or demonstrate cognitive distortions about children and sex
- the emotional dysregulation pathway was the second most populated pathway where subjects reportedly used the internet to access pornography (including child pornography) to alleviate the strong negative emotions associated with emotional dysphoria.

According to Armagh and Battaglia (2006), the behaviour of offenders involved in online child exploitation cases usually develops in four stages:

1 Awareness – once the offender is aware of their sexual preference for children, they may research or gather as much information as possible on the subject in an attempt to understand their feelings. This may be done through various ways, including the internet, printed and online articles, newscasts, pornographic websites and chatting with other like-minded individuals online.

2 Fantasy – materials and information gained from the earlier awareness-exploration stage can be leveraged as a source for both sexual fantasising and stimulation. The fantasy eventually becomes more fixated, with an emphasis on child pornography. The offender may then start to communicate with other like-minded individuals to obtain child exploitation materials.

3 Stalking – the offender has now moved on to the actual grooming stage by loitering at physical venues frequently visited by children or online venues such as IRC rooms. It is suggested that hardcore child pornography plays an important role at this stage and the offender might send, or request from, child victims sexually explicit photographs.

**Table 19** Ward and Siegert's pathways model of sexual offending

| Distal factors | Sexual preference | Associated deficits | Primary deficit | Behaviour |
|---|---|---|---|---|
| **Intimacy and social skills deficits (intimacy deficits):** individuals with no distortions in their sexual scripts, offending only at times such as prolonged emotional loneliness | | | | |
| • Insecure attachment styles<br>• Problems initiating and maintaining adult relationships | • Sexual preference for adult partners<br>• Normal sexual scripts<br>• May substitute child for preferred partner after rejection or blockage | • Emotional loneliness<br>• Maladaptive attachment styles<br>• Low self-efficacy<br>• Low self-esteem<br>• Low social skills<br>• Cognitive distortions regarding sexual entitlement | • Emotional loneliness | • Sexual arousal in the context of a sexual encounter with a child<br>• Create adult-like relationship with child |
| **Distorted sexual scripts (arousal):** individuals with subtle distortions of sexual scripts and dysfunctional attachment styles, could only achieve interpersonal closeness via sexual contact | | | | |
| • Premature sexualisation<br>• Possible victims of sexual abuse | • Flaws in context of sexual scripts<br>• Seek reassurance through sex and equate sex with intimacy<br>• May turn to children during periods of rejection and/or blockage | • Low self-esteem<br>• Cognitive distortions to justify behaviour<br>• Sensitive to rejection | • Emotional congruence | • Relationships seen as purely sexual<br>• May result in unhappy and frustrating adult sexual encounters<br>• Child partners are a question of opportunity and/or emotional needs |
| **Emotional dysregulation (emotional):** individuals having difficulties in the self-regulation of their emotions but are hypothesised to have normal sexual scripts | | | | |
| • Use sex as a coping strategy<br>• Link between sex and emotional wellbeing | • May use children and sex to punish partners<br>• Emotional need drives choice of partner<br>• Sexual arousal in context of strong emotional states | • Problems controlling anger<br>• External locus of control<br>• Personal distress | • Personal distress | • Problems identifying emotions<br>• Impaired ability to modulate emotions<br>• Problems utilising social supports |
| **Antisocial cognitions:** individuals who do not have distortions in their sexual scripts but possess general pro-criminal attitudes and beliefs, and whose offending reflects this anti-social tendency | | | | |
| • Anti-social attitudes and beliefs<br>• Feelings of superiority over children | • Sexual offending against children reflects anti-social tendency<br>• Cognitive distortions, sexual need and opportunity can lead to offending | • Cognitive distortions to initiate and justify behaviour<br>• Impulsivity | • Cognitive distortions | • Patriarchal attitudes<br>• Extensive criminal history<br>• Disregard social norms about children and sex<br>• Exploit any opportunity for gratification |
| **Multiple dysfunctional deficits:** individuals with multiple distorted sexual scripts and are likely to exhibit a multitude of offending behaviours | | | | |
| • Early sexualisation<br>• Impaired attachment styles<br>• Anti-social cognitions | • Deviant sexual preferences | • High self-esteem due to legitimacy of goals<br>• Entrenched cognitive distortions | • Emotional loneliness, emotional congruence, personal distress and cognitive distortions | • Inappropriate self-regulation<br>• Multiple offence-related behaviours |

Source: Ward and Siegert (2002) cited in Middleton et al. (2006)

4 Molestation – the offender sets up a meeting with the child victim with the intention of sexual contact.

## *Treatments*

A recent report by the US-based Center for Sex Offender Management highlighted that offenders convicted of sex crimes against children are at risk of being stigmatised and ostracised by other inmates during periods of incarceration and are at increased risk of sexual and other violent victimisation themselves. The report also noted that:

> [l]ike other victims of violence, individuals who are sexually assaulted or otherwise victimized while incarcerated can experience a range of short and long term negative after-effects which, if unaddressed, can impact adjustment and stability, and may ultimately have a negative impact on re-entry (Bumby, Talbot & Carter 2007: 6).

The risks of offenders convicted of sex crimes against children being sexually or violently attacked during periods of incarceration has been an issue for more than a century. Aytes et al. (2001) argued that sexual assaults or victimisation while incarcerated may increase the risk of reoffending, and untreated offenders may return to the community on their release with a more ingrained pattern of sexual aggression and few coping strategies with which to confront it.

> A comprehensive review of treatment programs by Marshall and Pithers (1994) concluded that sexual offenders participating in specialized treatment had lower re-offence rates than offenders who had not engaged in such treatment. Preliminary results of a longitudinal study supported by the California State Departments of Mental Health and Corrections and the National Institute of Mental Health suggested that treatment subjects were less likely to commit new sexual offences than subjects who refused treatment … and a long-term study that followed sexual offender treatment completers from 6 months to 17 years in Minnesota, reported lower sexual recidivism among successful treatment completers or near-completers … Even so, there continues to be little specific treatment for sexual offenders available in prisons. Although it may be expensive, the alternative of not providing treatment during incarceration is even more costly when offenders return to the community (Aytes et al. 2001: 224).

The importance of treatment for sexual offenders was also emphasised in a meta-analysis of controlled outcome evaluations of sexual offender treatment conducted by researchers from the University of Erlangen in Germany. In the study, 2,039 documents published in five languages, and 69 studies containing 80 independent comparisons between treated and untreated offenders were reviewed. The researchers found that the majority of the documents and studies reviewed 'confirmed the benefits of treatment [and that t]reated offenders showed 6 percentage points or 37 percent less sexual recidivism than controls' (Losel & Schmucker 2005: 117).

Child sexual offenders may also be supervised in the community either as a community sentence or as a form of post-custody supervision under the state's probation service and other agencies. This form of supervision is designed to reduce the offender's propensity to reoffend, to assist in the rehabilitation of the offender and to enable a degree of reparation to be made in the community (Thomas 2001). McAlinden (2006: 210–211) also noted that '[i]nvolving the community [in the rehabilitation of sexual offenders] may also help to reduce the social exclusion and stigmatization of offenders … [and] could deliver some tangible benefit in the form of reducing future offending behaviour'.

Supervision and rehabilitation of sexual offenders is a difficult and demanding process that requires appropriate education, training and a degree of devolved autonomy. Howells et al. (2004: 54) pointed out that 'rehabilitation of sexual offenders presents particular challenges'. This is particularly so for child sexual offenders. It is important for prison, correction, probation and other relevant authorities and professionals working with child sexual offenders (e.g. mental health professionals) to be aware of the existence of difficulties and problems to intervene and help offenders during their incarceration.

# Legislative responses

The threat of technology-enabled crime has given rise to a growing demand for strategies for prevention and control, particularly in the area of online child exploitation. Some of the key approaches relate to reducing opportunities for the commission of online child exploitation, making such activities more difficult to commit, increasing the risks of detection, enhancing the level and certainty of sanctions, and reducing the benefits likely to be derived from committing such criminal activities.

To keep children safe in the online environment, international conventions such as the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse have been introduced to deal with child exploitation offences. Countries such as Australia, Canada, the United States and the United Kingdom have also introduced online child grooming offences. Legislation that seeks to regulate the behaviour of sexual offenders on release from custody, such as sex offender registration and community notification, has also been introduced in several countries such as the United States. As recently as December 2007, the New Jersey Senate approved Bill S1979, which is aimed at limiting internet access for convicted sexual offenders to prevent them from luring children into meetings in the physical world (Hepp 2007; Jones 2007).

> Senate President Richard J. Codey (D-Essex) today praised the full Senate for unanimously approving bill S1979, which will give New Jersey some of the toughest tools in the nation to crack down on the growing threat of Internet predators. Bill S1979 would provide the state with nearly unparalleled authority to monitor or restrict Internet access by convicted sex offenders. The measure, which was first approved by the Senate in March, is part of a three-bill package that Sen. Codey introduced last year. The other two bills – S1977 and S1978 – would respectively require online dating companies to conduct criminal background checks on all members or clearly post notice if they do not, and impose stiffer penalties for anyone caught using the Internet to lure a victim (England and Wales; New Jersey Senate Democrats 2007: unpaginated).

A discussion of the principal normative developments overseas and in Australia follows. It is important to note the different statutory definitions of age that are relevant to child exploitation offences in various countries. Ages of consent to sexual activity and ages used to delimit the scope of child pornography offences differ from country to country, as shown in Table 20.

**Table 20** Age of consent by country (years)

| Country | Age of consent to sexual activity | Age in child pornography legislation |
|---|---|---|
| Australia | 12–17 (see Table 21) | 16 |
| Austria | 14 | 18 |
| Belgium | 16 | 18 |
| Denmark | 15 | 17 |
| Finland | 16 | 18 |
| France | 15 | 18 |
| Germany | 14 | 14 [a] |
| Greece | 15 | 18 |
| Iceland | 14 | 18 |
| Ireland | 17 | 17 |
| Italy | 13/14/16 | 18 |
| Netherlands | 16 | 18 |
| Spain | 13 | 18 |
| Sweden | 15 | 18 |
| United Kingdom | 16 | 18 (16 in Scotland) |

a: Due to a change in the German legislation 'posing photos', that is, photos showing a person under 18 in an unnatural sexual pose are illegal as well

Source: Adapted from https://www.inhope.org/en/hotlines/facts.html; Griffith and Roth (2007)

# Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse

The Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (CETS No. 201) was adopted by the Committee of Ministers on 12 July 2007. The Convention opened for signature on 20 October 2007 and had been signed by 26 countries at 29 January 2008, but none has, as yet, ratified the Convention. It has provisions that deal with child exploitation (Articles 20 to 22) and more specifically online child grooming (Article 23). Under the Convention a child is defined as a person under the age of 18 years (Article 3[a]). The principal relevant articles are:

**Article 20 – Offences concerning child pornography**

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:
   a producing child pornography;
   b offering or making available child pornography;
   c distributing or transmitting child pornography;
   d procuring child pornography for oneself or for another person;
   e possessing child pornography;
   f knowingly obtaining access, through information and communication technologies, to child pornography.

2 For the purpose of the present article, the term 'child pornography' shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:
   – consisting exclusively of simulated representations or realistic images of a non-existent child;
   – involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.

4 Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.

**Article 21 – Offences concerning the participation of a child in pornographic performances**

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:
   a recruiting a child into participating in pornographic performances or causing a child to participate in such performances;

b coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes;

c knowingly attending pornographic performances involving the participation of children.

2 Each Party may reserve the right to limit the application of paragraph 1.c to cases where children have been recruited or coerced in conformity with paragraph 1.a or b.

**Article 22 – Corruption of children**

Each Party shall take the necessary legislative or other measures to criminalise the intentional causing, for sexual purposes, of a child who has not reached the age set in application of Article 18, paragraph 2, to witness sexual abuse or sexual activities, even without having to participate.

**Article 23 – Solicitation of children for sexual purposes**

Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.

The focus of Article 23 is on intentional proposals by adults to meet with children for the purpose of committing specified offences. The emphasis is, therefore, on the fact that acts preparatory to the commission of sexual offences with children will be committed, rather than the process of grooming itself.

# Australia

In recent years, Australia has introduced legislation to counter the online grooming or luring of children for sexual purposes. For example, on 28 November 2007, New South Wales amended its *Crimes Act 1900* with the Crimes Amendment (Sexual Procurement or Grooming of Children) Bill 2007 to criminalise an adult procuring or grooming a child for unlawful sexual activity. Most jurisdictions within Australia also have legislation in place that criminalises online child grooming for the purposes of sexual contact (Table 21).

Already prosecutions have taken place under state legislation. For example, in Queensland a 25-year-old man had groomed what he had thought to be a 13-year-old girl ('becky_boo 13') in an IRC room by sending emails inviting her to engage in sexual activity. In fact, the emails were sent to an undercover police officer who was pretending to be the child in question. The defendant was convicted and sentenced to imprisonment for two-and-a-half years, suspended after having served nine months. This was reduced on appeal to an 18-month term, suspended from the time of the appeal, the defendant having already served 90 days in custody (*R v Kennings* [2004] QCA 162). In a more recent incident, Steven Woods was sentenced to two years imprisonment for using 'online chat rooms to proposition children to engage in sexual acts' (Queensland Crime and Misconduct Commission 2006: unpaginated). This sentence was suspended after Woods served three months imprisonment, with a condition that he not reoffend for a period of three years.

The fact that an adult pretends to be a child to establish contact with the victim is not an impediment to a prosecution as child grooming can be viewed as an act preliminary to commission of a sexual offence. This is clarified in some legislation. For example, s 218A(7) of the *Criminal Code Act 1899* (Qld) states that 'it does not matter that the person is a fictitious person represented to the adult as a real person'. Similar provisions are found in s 474.28(9) of the *Criminal Code Act 1995* (Cth) and s 66EB(5) of the *Crimes Act 1900* (NSW). Successful prosecutions of cases involving covert sting operations where investigators pose as children online have been achieved in other countries including the United States (US DoJ 2007a, 2007b). The circumstances of police covert sting operations are described in Box 2.

**Table 21** Offences relating to the use of ICT to procure or groom children for the purposes of sexual contact in Australia

| Jurisdiction | Provision | Maximum penalty | Definition of a child or young person by age |
|---|---|---|---|
| Commonwealth | *Criminal Code Act 1995*, s 474.26: Using a carriage service to procure persons under 16 years of age | 15 years imprisonment | Under 16 years of age |
| | *Criminal Code Act 1995*, s 474.27: Using a carriage service to 'groom' persons under 16 years of age | 12 years imprisonment (15 years imprisonment if s 474.27[3] applies) | Under 16 years of age |
| Australian Capital Territory | *Crimes Act 1900*, s 66: Using the internet etc. to deprave young people | s 66(1): 10 years imprisonment (five years imprisonment if this is the first offence) | Under 16 years of age |
| | | s 66(3): 100 penalty units, five years imprisonment or both | Under 16 years of age |
| Queensland | *Criminal Code Act 1899*, s 218A: Using internet, etc. to procure children under 16 years | s 218A(1): Five years imprisonment | Under 16 years of age |
| | | s 218A(2): 10 years imprisonment | Under 12 years of age |
| Northern Territory | *Criminal Code Act*, s 131: Attempts to procure child under 16 years | s 131(1): Three years imprisonment | Under 16 years of age |
| | | s 131(2): Five years imprisonment | Under 16 years of age |
| | *Criminal Code Act*, s 132: Indecent dealing with child under 16 years | s 132(2): 10 years imprisonment | Under 16 years of age |
| | | s 132(4): 14 years imprisonment | Under 10 years of age |
| New South Wales | *Crimes Act 1900* (as amended by Crimes Amendment [Sexual Procurement or Grooming of Children] Bill 2007 s 66EB: Procuring or grooming child under 16 years for unlawful sexual activity | s 66EB(2)(a): 15 years imprisonment | Under 14 years of age |
| | | s 66EB(2)(b): 12 years imprisonment | Under 16 years of age |
| | | s 66EB(3)(a): 12 years imprisonment | Under 14 years of age |
| | | s 66EB(3)(b): 10 years imprisonment | Under 16 years of age |
| South Australia | *Criminal Law Consolidation Act 1935*, s 63B: Procuring child to commit indecent act, etc. | ss 63B(1)(a), 63B(3)(a): 10 years imprisonment | Under 16 years of age |
| | | ss 63B(1)(b), 63B(3)(b): 12 years imprisonment | Under 12 years of age |
| Tasmania | *Criminal Code Act 1924*, s 125D: Communications with intent to procure person under 17 years, etc. | No statutory maximum penalty – at the discretion of the court with a maximum of 21 years imprisonment (House of Assembly Hansard 2005) | Under 17 years of age |
| Western Australia | Criminal Code: s 204B: Using electronic communication to procure, or expose to indecent matter, children under 16 years | s 204B(2): Five years imprisonment | Under 16 years of age |
| | | s 204B(3): 10 years imprisonment | Under 13 years of age |

Sources: Compiled from legislative databases including http://www.comlaw.gov.au/ (Cth), http://www.legislation.act.gov.au/ (ACT), http://www.legislation.qld.gov.au/OQPChome.htm (Qld), http://www.nt.gov.au/dcm/legislation/current.html (NT), http://www.legislation.sa.gov.au/index.aspx (SA), http://www.thelaw.tas.gov.au/index.w3p (Tas), http://www.slp.wa.gov.au/statutes/swans.nsf (WA), and http://www.legislation.nsw.gov.au/ (NSW)

In Australian jurisdictions with no specific online child grooming legislation, Commonwealth legislation can, in certain circumstances, be used to prosecute offenders. For example, Richard Gerard Meehan was charged with one count of using a carriage service to transmit communications to a person under 16 years of age with the intention of procuring that person to engage in sexual activity, contrary to s 474.26(1) of the *Criminal Code Act 1995* (Cth). On 21 July 2006, Meehan was sentenced in the Victorian County Court to 24 months imprisonment, with an order that he be released after serving three

months (Commonwealth Director of Public Prosecutions 2006).

Recent instances where individuals have been charged under Commonwealth, state or territory grooming provisions suggest that they provide a valuable tool for early intervention in child exploitation activity. The fact that the victim is located in another country is also not an impediment to prosecution. For example, a man was charged in New South Wales in March 2007 with 'child grooming offences after explicit photographs and messages were allegedly sent to a teenage boy in the United States via the internet' (NSW Police 2007: unpaginated). This case is yet to be finalised, but shows the wide reach of some legislation.

**Box 2** A typical covert sting operation

A law enforcement investigator posts a profile on the internet or goes into an IRC room posing as a child aged between 12 and 16 years. The investigator responds to conversations initiated by offender(s) seeking a child for sexual encounter contacts, and allows the offender(s) to develop a relationship that culminates in a face-to-face meeting. During the conversation, the investigator is careful not to initiate conversations about sexual topics, propose sexual activity or engage in illegal activities that may improperly induce a person to commit a criminal act (e.g. sending offenders child exploitation materials). Logs of all online interactions, which constitute evidence of the crime, are recorded by the investigator. The offender is arrested during the face-to-face meeting and charged with online grooming offences.

Source: Adapted from Wolak, Mitchell and Finkelhor (2003)

# Canada

Bill C-15A, an act to amend Canada's Criminal Code (RSC 1985 c. C-46) with respect to online child grooming for sexual purposes, received royal assent on 4 June 2002. Section 172.1 criminalises electronic communication with a person believed to be a child for the purpose of facilitating the commission of sexual offences. Depending on the offence, the requisite age (real or believed) of the intended victim varies from between 14 and 18 years, although the legal age of consent to sexual activity in s 151 (sexual interference) is 14 years.

**172.1** (1) Every person commits an offence who, by means of a computer system within the meaning of subsection 342.1(2), communicates with:

(*a*) a person who is, or who the accused believes is, under the age of eighteen years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155 or 163.1, subsection 212(1) or (4) or section 271, 272 or 273 with respect to that person;

(*b*) a person who is, or who the accused believes is, under the age of sixteen years, for the purpose of facilitating the commission of an offence under section 280 with respect to that person; or

(*c*) a person who is, or who the accused believes is, under the age of fourteen years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 281 with respect to that person.

(2) Every person who commits an offence under subsection (1) is guilty of:

(*a*) an indictable offence and liable to imprisonment for a term of not more than five years; or (*b*) an offence punishable on summary conviction.

(3) Evidence that the person referred to in paragraph (1)(*a*), (*b*) or (*c*) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age.

(4) It is not a defence to a charge under paragraph (1)(*a*), (*b*) or (*c*) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.

Although Canadian citizens or permanent residents may be prosecuted for the commission of certain sexual offences outside Canada (including sexual offences against children), this does not apply to the offence specified in s 172.1 (luring a child).

## Singapore

On 17 September 2007, the Penal Code (Amendment) Bill was introduced in the Singapore Parliament, which included a proposed grooming provision that would make it an offence to meet or travel to meet a minor under 16 years of age after sexual grooming (s 376E – Sexual grooming of minor under 16) (Singapore Ministry of Home Affairs 2007a). The bill was passed on 23 October 2007.

A person of or above the age of 21 years (A) commits an offence under this new provision if:

- having met or communicated with another person (B) on two or more previous occasions
- A intentionally meets B or travels with the intention of meeting B (in or outside Singapore)
- at the time of the acts referred to in the previous point:
  - A intends to do anything to or in respect of B, during or after the meeting, which if done will involve the commission by A of a relevant offence (i.e. an offence under ss 354, 354A, 375, 376, 376A, 376B, 376F, 376G or 377A, s 7 of the Children and Young Persons Act [Cap. 38], or s 140[1] of the Women's Charter [Cap. 353])
  - B is under 16 years of age
  - A does not reasonably believe that B is of or above the age of 16 years.

The penalty is a maximum imprisonment term of three years, or a fine, or both.

Although the provision provides that A's previous meetings or communications with the child can have taken place in any part of the world (including over the internet), the meeting or travelling must take place in Singapore (Singapore Ministry of Home Affairs 2007b). For an offence to be made out under the new provision, there must have been a prior meeting/communication (which can take place in or outside Singapore) on at least two occasions as an indication of the offender's intention of grooming the minor for sexual activities; and the offender must travel to meet or intentionally meet the victim in Singapore, with the intention of committing a sexual offence with the minor. This provision was modelled on s 15 of the UK's Sexual Offences Act 2003, although there are differences between the legislation in Singapore and that in the United Kingdom as indicated in Table 22.

**Table 22** Principal differences between the United Kingdom's and Singapore's online child grooming provisions by penalty and definition of offender's age

| Country | Provision | Penalty | Definition of an offender by age |
|---|---|---|---|
| United Kingdom | s 15 | On summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both<br><br>On conviction on indictment, to imprisonment for a term not exceeding 10 years | 18 years or above |
| Singapore | s 376E | Three years imprisonment, or fine or both | 21 years or above |

The Penal Code (Amendment) Act also includes a provision for criminalising the procurement of sexual activity with a person with a mental disability.

## United Kingdom

In England and Wales, child grooming is proscribed by ss 14 and 15 of the Sexual Offences Act 2003. Section 14 proscribes the grooming process, while s 15 proscribes subsequent meetings. These provisions are as follows:

**14 Arranging or facilitating commission of a child sex offence**

(1) A person commits an offence if:

(a) he intentionally arranges or facilitates something that he intends to do, intends another person to do, or believes that another person will do, in any part of the world, and

(b) doing it will involve the commission of an offence under any of sections 9 to 13.

(2) A person does not commit an offence under this section if:

(a) he arranges or facilitates something that he believes another person will do, but that he does not intend to do or intend another person to do, and

(b) any offence within subsection (1)(b) would be an offence against a child for whose protection he acts.

(3) For the purposes of subsection (2), a person acts for the protection of a child if he acts for the purpose of:

(a) protecting the child from sexually transmitted infection,

(b) protecting the physical safety of the child,

(c) preventing the child from becoming pregnant, or

(d) promoting the child's emotional well-being by the giving of advice, and not for the purpose of obtaining sexual gratification or for the purpose of causing or encouraging the activity constituting the offence within subsection (1)(b) or the child's participation in it.

(4) A person guilty of an offence under this section is liable:

(a) on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum or both;

(b) on conviction on indictment, to imprisonment for a term not exceeding 14 years.

**15 Meeting a child following sexual grooming, etc.**

(1) A person aged 18 or over (A) commits an offence if:

(a) having met or communicated with another person (B) on at least two earlier occasions, he:

(i) intentionally meets B, or

(ii) travels with the intention of meeting B in any part of the world,

(b) at the time, he intends to do anything to or in respect of B, during or after the meeting and in any part of the world, which if done will involve the commission by A of a relevant offence,

(c) B is under 16, and

(d) A does not reasonably believe that B is 16 or over.

(2) In subsection (1):

(a) the reference to A having met or communicated with B is a reference to A having met B in any part of the world or having communicated with B by any means from, to or in any part of the world;

(b) 'relevant offence' means:

(i) an offence under this Part,

(ii) an offence within any of paragraphs 61 to 92 of Schedule 3, or

(iii) anything done outside England and Wales and Northern Ireland which is not an offence within sub-paragraph (i) or (ii) but would be an offence within sub-paragraph (i) if done in England and Wales.

(3) In this section as it applies to Northern Ireland:

(a) subsection (1) has effect with the substitution of '17' for '16' in both places;

(b) subsection (2)(b)(iii) has effect with the substitution of 'sub-paragraph (ii) if done in Northern Ireland' for 'sub-paragraph (i) if done in England and Wales'.

(4) A person guilty of an offence under this section is liable:

(a) on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum or both;

(b) on conviction on indictment, to imprisonment for a term not exceeding 10 years.

Although s 15(2)(a) provides that A's previous meetings or communications with the child can have taken place in or across any part of the world (including outside the United Kingdom), the travel to the meeting itself must at least partly take place in England, Wales or Northern Ireland (UK OPSI 2004).

The main factors in determining the degree of seriousness of this offence include:

- the seriousness of the intended offence
- vulnerability of the victim and any harm caused to the victim
- the degree of planning involved (UK CPS n.d.).

A sexual offences prevention order (SOPO) and a risk of sexual harm order (RSHO) are also introduced in the Sexual Offences Act 2003:

- Section 104: SOPO, replacing the sex offender orders and restraining orders enacted under the Sex Offenders Act 1997, allows orders to be made against individuals without previous convictions as long as it is satisfied that it is necessary to make such an order, for the purpose of protecting the public or any particular members of the public from serious sexual harm from the defendant.
- Section 123 allows police to apply for RSHO, a civil preventative order, from a Magistrates' Court if when an individual's behaviour is deemed to present a sexual risk to children and young people. That is, if the individual has on at least two occasions, whether before or after the commencement of this Part, done any of the following act (sub-s 123(3)) and as a result of those acts, there is reasonable cause to believe that it is necessary for such an order to be made.
  1 engaging in sexual activity involving a child or in the presence of a child
  2 causing or inciting a child to watch a person engaging in sexual activity or to look at a moving or still image that is sexual
  3 giving a child anything that relates to sexual activity or contains a reference to such activity
  4 communicating with a child, where any part of the communication is sexual.

Breaching an interim RSHO or a RSHO, the individual is liable:

- on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both
- on conviction on indictment, to imprisonment for a term not exceeding five years (see s 128).

Under s 80 of the Sexual Offences Act 2003, a person convicted of an offence listed in Schedule 3 (including child grooming), found not guilty of such an offence by reason of insanity, found to be under a disability and to have done the act charged against him in respect of such an offence, or in England and Wales or Northern Ireland, he is cautioned in respect of such an offence, is required to register as a registered sex offender with law enforcement agencies within three days beginning with the relevant date. Information required under sub-s 83(5):

The information is:

- the relevant offender's date of birth
- his national insurance number
- his name on the relevant date and, where he used one or more other names on that date, each of those names
- his home address on the relevant date
- his name on the date on which notification is given and, where he uses one or more other names on that date, each of those names
- his home address on the date on which notification is given
- the address of any other premises in the United Kingdom at which, at the time the notification is given, he regularly resides or stays.

The United Kingdom is one of few countries to require registered sex offenders to notify authorities about their intention to travel abroad. A notification under s 86 of the Sexual Offences Act 2003 must disclose:

- the date on which the offender will leave the United Kingdom
- the country (or, if there is more than one, the first country) to which he will travel and his point of arrival (determined in accordance with the regulations) in that country
- any other information prescribed by the regulations that the offender holds about his departure from, or return to, the United Kingdom or his movements while outside the United Kingdom.

In Scotland, on 7 October 2005, the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 came into force. Section 1 of the Act is as follows:

**1. Meeting a child following certain preliminary contact**

(1) A person ('A') commits an offence if:

(a) having met or communicated with another person ('B') on at least one earlier occasion, A:

(i) intentionally meets B;

(ii) travels, in any part of the world, with the intention of meeting B in any part of the world; or

(iii) makes arrangements, in any part of the world, with the intention of meeting B in any part of the world, for B to travel in any part of the world;

(b) at the time, A intends to engage in unlawful sexual activity involving B or in the presence of B:

(i) during or after the meeting; and

(ii) in any part of the world;

(c) B is:

(i) aged under 16; or

(ii) a constable;

(d) A does not reasonably believe that B is 16 or over; and

(e) at least one of the following is the case:

(i) the meeting or communication on an earlier occasion referred to in paragraph (a) (or, if there is more than one, one of them) has a relevant Scottish connection;

(ii) the meeting referred to in sub-paragraph (i) of that paragraph or, as the case may be, the travelling referred to in sub-paragraph (ii) of that paragraph or the making of arrangements referred to in sub-paragraph (iii) of that paragraph, has a relevant Scottish connection;

(iii) A is a British citizen or resident in the United Kingdom.

(2) In subsection (1) above:

(a) the reference to A's having met or communicated with B is a reference to A's having met B in any part of the world or having communicated with B by any means from or in any part of the world (and irrespective of where B is in the world); and

(b) a meeting or travelling or making of arrangements has a relevant Scottish connection if it, or any part of it, takes place in Scotland; and a communication has such a connection if it is made from or to or takes place in Scotland.

(3) For the purposes of subsection (1)(b) above, it is not necessary to allege or prove that A intended to engage in a specific activity.

(4) A person guilty of an offence under this section is liable:

(a) on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum or both;

(b) on conviction on indictment, to imprisonment for a term not exceeding 10 years or a fine or both.

(5) Subsections (6A) and (6B) of section 16B of the Criminal Law (Consolidation) (Scotland) Act 1995 (c.39) (which determines the sheriff court district in which proceedings against persons committing certain sexual acts outside the United Kingdom are to be taken) apply in relation to proceedings for an offence under this section as they apply to an offence to which that section applies.

Under both s 15 of the Sexual Offences Act 2003 and s 1 of the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, an offence is not committed if the accused reasonably believes the child to be 16 or over. In both Acts, the meeting or intended meeting with the child is key to the offence. Although this provides a clear point at which to intervene (i.e. when the sexual offender travels to meet a child):

> [i]n reality it would be extremely difficult to police and [gain evidence of] grooming behaviour in the 'real world' so it is therefore unsurprising that few cases have been brought to court on this basis under the *Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005* and the *Sexual Offences Act 2003* (England and Wales) (Davidson 2007: 25).

# United States

Under the various provisions of the Protection of Children from Sexual Predators Act of 1998, it is an offence to use a computer to attempt to persuade and entice a minor to engage in sexual conduct. For example:

- Section 101 amends 18 USC 2425 and criminalises the use of interstate facilities to transmit information about a minor.

  > Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, knowingly initiates the transmission of the name, address, telephone number, social security number, or electronic mail address of another individual, knowing that such other individual has not attained the age of 16 years, with the intent to entice, encourage, offer, or solicit any person to engage in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title, imprisoned not more than 5 years, or both.

- Section 102 amends 18 USC 2422 and criminalises coercion and enticement of an individual below the age of 18 to engage in prostitution or any sexual activity for which any person can be charged with a criminal offence, or attempts to do so, shall be fined under this title, imprisoned for not more than 15 years, or both.
- Section 401 amends 18 USC 1470 and criminalises the use of mail or any facility or means of interstate or foreign commerce, to knowingly transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempts to do so, shall be fined under this title, imprisoned for not more than 10 years, or both.

## *Sex offender registries*

A sex offender registration framework has been enacted in a number of countries as a means of regulating the behaviour of sexual offenders on their release from custody and providing law enforcement with an additional investigative tool. The National Sex Offender Registry Assistance Program, established by the Bureau of Justice Statistics in the Department of Justice, is one such initiative designed to assist other states to comply with federal sex offender registration and community notification laws (Appendix A).

The requirements for sex offender registration and community notification laws vary from state to state. As noted by Levenson et al. (2007: 2), '[s]ome states notify the public only about sex offenders who pose a high risk to the community, but other states employ broad notification practices and disseminate information about all registered sex offenders'.

- The website for Arizona Sex Offender InfoCenter, for example, only contains information on sexual offenders with risk assessment scores of Level 2 (Intermediate – http://az.gov/webapp/portal/sows.jsp?name=sows230-13-3826#level2) or Level 3 (High – http://az.gov/webapp/portal/sows.jsp?name=sows230-13-3826#level3). This is the same for several other sites such as the Washington State Sex Offender Information Center.
- The Colorado Convicted Sex Offender site does not contain information concerning sexual offenders, only those convicted of misdemeanour sex offences and juveniles adjudicated for sex crimes.
- On the Maine Sex Offender Registry, offenders' information is only limited to individuals required to register pursuant to Title 34-A MRSA, Chapter 15 (http://janus.state.me.us/legis/statutes/34-A/title34-Ach15sec0.html), and sentenced for a requisite offence on or after 1 January 1982.

An overview and history of the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act follows (http://www.ojp.usdoj.gov/BJA/what/2a1jwacthistory.html):

- 1994 – Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act passed as part of the federal Violent Crime Control and Law Enforcement Act of 1994, which requires states to implement a sex offender and crimes against children registry.

- 1996 – Federal Megan's Law (named after seven-year-old New Jersey girl Megan Kanka who was raped and killed by a known child molester who had moved across the street from the family without their knowledge) amends the Violent Crime Control and Law Enforcement Act of 1994, requiring the release of relevant information to protect the public from sexually violent offenders (http://www.megannicolekankafoundation.org/federal_law.htm).
- The Pam Lychner Sexual Offender Tracking and Identification Act of 1996 (http://thomas.loc.gov/cgi-bin/query/z?c104:S.1675.ENR:) also becomes an amendment to the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act, which requires lifetime registration for recidivists and offenders who commit certain aggravated offences.
- 1998 – Provisions contained in s 115 of the General Provisions of Title I of the Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act amend the requirements of the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act to include heightened registration requirements for sexually violent offenders, registration of federal and military offenders, registration of non-resident workers and students, and participation in the National Sex Offender Registry.
- 2000 – The Campus Sex Crimes Prevention Act amends the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act, which requires sexual offenders to report information regarding any enrolment or employment at an institution of higher education and to provide this information to a law enforcement agency whose jurisdiction includes the institution.

The federal Adam Walsh Child Protection and Safety Act of 2006 (Public Law 109–248) was signed by President Bush on 27 July 2006, and significantly expands efforts to monitor sexual offenders in the community and establishes financial penalties for states that do not meet deadlines to comply with its provisions.

Despite the absence of any compelling evidence about the efficacy and impact of internet sex offender registries and community notification on sex offence recidivism rates, these initiatives allow the community access to information regarding incarcerated sex offenders living within their community. This, arguably, allows the community to undertake additional precautionary steps to protect their children.

## Internet filtering

Several countries have introduced internet filtering regimes, which seek to restrict users from accessing online social networking sites and websites that host potentially objectionable materials (e.g. child exploitation and racial vilification materials), using various internet filtering technologies.

Governments in the Middle East are reportedly stepping up a campaign of filtering and surveillance in an effort to prevent an estimated 33.5 million internet users from viewing a variety of websites whose topics range from human rights to pornography. As a result, millions of Middle Easterners are finding it harder by the day to access popular news and entertainment sites such as Facebook, MySpace, YouTube and Flickr (Allam 2007).

> In Syria, Facebook, the secondmost popular social-networking site after News Corp's MySpace, has been blocked … After a series of moves to tighten government control over the Internet, a human rights group has said that increased Internet censorship has sparked the creation of several Facebook protest groups only accessible to Syrians living outside the country and those who have discovered a proxy address to bypass the block. The groups include 'Don't block Facebook in Syria' with 1,467 members and the 'Why the Regulator in Syria is Barring Facebook!' group with 136 members (Syria blocks public access to Facebook 2007: unpaginated).

In October 2007, a Malaysia-based newspaper reported that:

> [a] total of 11 websites, including those created by bloggers, have been shut down by the Malaysian Communications and Multimedia Commission (MCMC) this year for contravening

> rules and regulations concerning the publication of information on the Internet. Energy, Water and Communications Deputy Minister Datuk Shaziman Abu Mansor said two cases have also been brought to the Attorney-General's Chambers for action. He added the Government could take action under Section 211 and 233 of the *Communications and Multimedia Act 1998* against owners, operators or writers of websites who misused the Internet to spread slanderous comments, insulting the country's leaders, religious sensitivities and race. Those who broke the law could be slapped with a RM50,000 fine, one year's jail or both, he said (Abd Rahman 2007: unpaginated).

In China, between May and June 2007, 300 websites allegedly hosting links to pornographic websites and 10,000 online pornographic games were reportedly shut down by Chinese authorities (Online porn merchants dodge internet dragnet 2007). A recent report published by the Chinese Human Rights Defenders group also suggested that:

> [v]arious forms of communication have been established between the leading commercial websites and the supervisory bodies – phone, email, SMS text messages, MSN, QQ and RTX (Real Time eXchange) instant messaging, web platforms and a weekly meeting. The Beijing Internet Information Administrative Bureau uses these different means of communication to instruct sites to not publish an article, to not cover an event or issue, or to put a stop to certain comments. The employees of these privately-owned sites are expected to liaise with the bureau and respond to its orders as quickly as possible … In order to comply with the bureau's orders, all the online companies have set up a section dedicated solely to monitoring all of the letters, comments, articles and other messages on their websites. Content of a sensitive nature is immediately masked or erased, and the username or IP address of the person who posted it is also blocked (CHRD 2007: 6).

The extent of internet filtering varies among countries. Leyden (2007b: unpaginated), for example, suggested that Middle Eastern countries such as Burma, Iran, Pakistan, Saudi Arabia, Syria, Tunisia, the United Arab Emirates, and Yemen were among the most restrictive regimes, while countries such as 'China, India, Singapore, South Korea, and Thailand … apply controls, albeit to a lesser extent'. It should come as no surprise to long-time political observers that internet content is more closely monitored and controlled by governments in authoritative countries, which can be achieved either through legislation or via direct ownership of state monopolies.

Internet filtering is not, however, limited to Asian and Middle Eastern countries. While there is a great deal of concern about the states that traditionally filter the internet such as China, Cuba, Myanmar and Turkey there are other states that appear on the list that are traditionally not understood to be filtering regimes. These include the United States, France and Germany. These states rarely receive the same amount of bad publicity for their filtering since it is commonly understood that they are advocates of freedom of information. It is easy to see how this stance becomes problematic since even these states filter access to information online (Klang 2006).

Gorman (2005: 453) further suggested that liberal Western democracies such as '[the United States], Britain, Australia, New Zealand, Canada and members of the [European Union] all censor the internet at some level'.

> The recent report of the NCH about child abuse, child pornography and the Internet is alarming and claims that there is a strong link between Internet use and child abuse … A civil society will not simply sit back and accept these developments. It looks as if privacy and anonymity on the Internet will become something of the past. Not only totalitarian countries are filtering or blocking information. Modern western democracies are putting legislation in place that limits this freedom (Nijboer 2004: 257).

In the United States, for example, the CIPA was enacted as part of the Consolidated Appropriations Act of 2001 by Congress in December 2000. It mandates the installation of internet filtering software to block access to materials that are obscene, child pornography, or harmful to minors at schools and libraries receiving federal funds for internet access

(http://www.fcc.gov/cgb/consumerfacts/cipa.html and http://ifea.net/cipa.html). CIPA, s 1721, for example, imposes certain types of requirements on any school or library that receives funding support for internet access.

**CIPA, section 1721(b):**

'Internet safety' codified at 47 USC 254(h)(6)(A)(i): mandates that a library having one or more computers with internet access may not receive services at discount rates under paragraph (1)(B) unless the library:

- submits to the Commission the certifications described in subparagraphs (B) and (C); and
- submits to the Commission a certification that an internet safety policy has been adopted and implemented for the library under subsection (l) of this section; and
- ensures the use of such computers in accordance with the certifications.

'Certification with respect to minors' codified at 47 USC 254(h)(6)(B): A certification under this subparagraph is a certification that the library:

- is enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are – obscene; child pornography; or harmful to minors; and
- is enforcing the operation of such technology protection measure during any use of such computers by minors.

Shortly after the CIPA was enacted, several organisations including the American Civil Liberties Union, American Library Association and Electronic Frontier Foundation filed a lawsuit challenging the Act. On 31 May 2002, Chief Circuit Judge Becker, and District Judges Fullam and Bartle of the District Court for the Eastern District of Pennsylvania wrote:

> [i]n view of the severe limitations of filtering technology and the existence of these less restrictive alternatives, we conclude that it is not possible for a public library to comply with CIPA without blocking a very substantial amount of constitutionally protected speech, in violation of the First Amendment. Because this conclusion derives from the inherent limits of the filtering technology mandated by CIPA, it holds for any library that complies with CIPA's conditions. Hence, even under the stricter standard of facial invalidity proposed by the government, which would require us to uphold CIPA if only a single library can comply with CIPA's conditions without violating the First Amendment, we conclude that CIPA is facially invalid, since it will induce public libraries, as state actors, to violate the First Amendment. Because we hold that CIPA is invalid on these grounds, we need not reach the plaintiffs' alternative theories that CIPA is invalid as a prior restraint on speech and is unconstitutionally vague. Nor need we decide whether CIPA is invalid because it requires public libraries, as a condition on the receipt of federal funds, to relinquish their own First Amendment rights to provide the public with unfiltered Internet access, a theory that we nonetheless feel constrained to discuss (at length) in the margin (*American Library Association, Inc., et al. v. United States, et al.* no. 01-1303 and *Multnomah County Public Library, et al. v United States of America, et al.* no. 01-1322: 185–186).

The three-judge District Court ruled that:

> Sections 1712(a)(2) and 1721(b) of the Children's Internet Protection Act, codified at 20 U.S.C. §9134(f) and 47 U.S.C. § 254(h)(6), respectively, to be facially invalid under the First Amendment and permanently enjoining the defendants from enforcing those provisions (*American Library Association, Inc., et al. v. United States, et al.* no. 01-1303 and *Multnomah County Public Library, et al. v United States of America, et al.*: no. 01-1322: 195).

On 23 July 2003, the Supreme Court of the United States reversed the ruling of the District Court for the Eastern District of Pennsylvania and upheld the CIPA as 'the need for libraries to prevent minors from accessing obscene materials outweighs the free speech rights of library patrons and website publishers' (Kierkegaard 2008: 53).

> Chief Justice Rehnquist announced the judgment of the Court and delivered an opinion, in which Justice O'Connor, Justice Scalia and Justice Thomas joined. To address the problems associated with the availability of Internet pornography in public libraries, Congress

> enacted the Children's Internet Protection Act (CIPA), 114 Stat. 2763A–335. Under CIPA, a public library may not receive federal assistance to provide Internet access unless it installs software to block images that constitute obscenity or child pornography, and to prevent minors from obtaining access to material that is harmful to them. The District Court held these provisions facially invalid on the ground that they induce public libraries to violate patrons' First Amendment rights. We now reverse (*United States, et al. v. American Library Association, Inc., et al.* no. 02-361: 1).

The Australian Government has also indicated its intention to introduce mandatory internet filtering to protect children from potentially objectionable and harmful materials online:

> Every Australian with an internet connection could soon have their web content automatically censored. The restrictions are planned by the Federal Government to give greater protection to children from online pornography and violent websites. Under the plan, all internet service providers will have to provide a 'clean' feed to households and schools, free of pornography and other 'inappropriate' material (Heywood 2007: unpaginated).

ISP filtering is one component of the Australian Government's Cyber-safety plan. The Government is examining the introduction of ISP-level filtering for Refused Classification (RC) material. Content defined under the National Classification Scheme as RC material includes child sexual abuse imagery, bestiality, sexual violence, detailed instruction in crime, violence or drug use and/or material that advocates the doing of a terrorist act. The Government is also considering additional ISP content filtering options for those families who wish to have such a service.

The Restricted Access System Declaration 2007 came into effect on 20 January 2008, and places obligations on all content service providers to check that individuals accessing restricted content provided in Australia are at least 15 years of age for MA15+ content or 18 years of age for R18+ content (ACMA 2007b). The restriction, however, applies only to content hosted either in Australia or provided from Australia (see *Broadcasting Services Act 1992* [Cth], Schedule 7). Deibert (2002) suggested that the authority of any country's regulations against internet content extends only to their territorial borders. As a result, such laws may not effectively serve the government's interest in protecting children as they might still be able to access potentially objectionable materials originating from outside of Australia or receive such material using other communications technologies hosted outside of Australia (e.g. email servers hosted in countries with lax cybercrime legislation).

Where content is not hosted in Australia and is prohibited, the Australian Communications and Media Authority (ACMA) will notify the content to the suppliers of approved internet content filters, so that access to the content can be blocked by use of such filters. Regardless of where the content is hosted, if ACMA considers the content to be of a sufficiently serious nature, it must notify the content to an Australian police force.

It is not an easy task to restrict access to all potentially objectionable materials online as the range of such content to be filtered out, blocked or banned is extensive.

> According to Bernadette McMenamin, the chief executive of anti-child-abuse group Child Wise, more than 100,000 commercial websites offer child pornography and more than 20,000 images of child pornography are posted on the internet every week. Various international groups have estimated the number of child pornography websites alone to be in the millions, while one local internet service provider told *The Australian* it could be as high as 30 million sites globally (Dearne & Foo 2008a: unpaginated).

There is a need for continued development of software to trace, analyse and block websites hosting or disseminating online child exploitation and other potentially objectionable materials. Allbon and Williams (2002: 38) argued that 'it is incumbent upon the government, schools and libraries to decide the balance between the right to information and the need for protection. The question is not an easy one to answer, but could be made a little less daunting by increased training, information and general education for teachers, pupils and parents'.

The Government's *Plan for Cyber-safety* aims to increase cyber-safety education, to ensure that young Australian children are provided with

important cyber-safety tools from the time they are introduced to computers and the internet. ACMA is developing outreach activities to provide parents, teachers and children with up-to-date, comprehensive and age-appropriates online cyber-safety resources and assistance.

Through work with children, educators and IT specialists, the current online safety website (netalert.gov.au) is being improved and will contain relevant and effective cyber-safety education material for teachers and parents. A specific online safety website for children is also being developed.

Privacy advocates and some academics have been known to oppose internet filtering, particularly in liberal Western democracies. Müller from Stanford University, for example, argued that:

> censorship may have the best possible intentions, but it remains a violation of people's autonomy of information. I do not see a sufficient reason to practice censorship as long as we cannot be certain that some particular information will be harmful. (Even the case of minors is doubtful, though there we can presumably argue that they need to be protected precisely because they are not yet fully autonomous persons.) Note that we can be certain that an information is harmful if it violates one of the personality rights mentioned at the outset. Accordingly, no form of political censorship is covered by the argumentation presented here. Al Qaeda should have the right to a web-site to defend their views. It is only if they spread bomb-making guidelines or the like that this would fall under the category of 'dangerous information' proposed here (Müller 2006: 6).

Sandy from the Victoria University of Technology also advocated that:

> IT professionals should: As the Australian Computer Society reminds us … start with the premise that the internet is an adult medium. If minors use the internet, it is a parental responsibility to decide what images the minor consumes … Oppose government regulation of the professional activities of development and use of the internet … Vigorously oppose and counter advocacy of internet censorship … Advocate that the online services bill be repealed along with much of the censorship legislation governing other media (Sandy 2000: 52–53).

Internet filtering, via mandatory ISP filtering, can however be a useful means of restricting access to potentially objectionable materials online although parents, internet users and agencies tasked with protecting children from online evils should not be lulled into a false sense of security. Craig Middleton, speaking on behalf of Telstra BigPond, was reported to have argued that: 'We stand alongside the IIA and other ISPs in the view that PC-based filtering, in the hands of a responsible parent, is the only workable solution'. Similarly, Warren Cann, Executive Director of the Parenting Research Centre in Melbourne, said that although filters offered some protection, parents still needed to monitor their children's activities online (Dearne & Foo 2008b: unpaginated).

Australian child protection agencies have been vocal in their support of removing access to child abuse images from the Internet. Child Wise CEO Bernadette McMenamin stated, 'As a parent and a child protection advocate I call on Australians to support the federal Government's mandatory ISP filtering initiative to block child pornography'. Further, studies undertaken by Child Wise delivered some unexpected outcomes. 'Child Wise has also received calls from child sex offenders who support mandatory ISP filtering, stating that this blocking mechanism would have reduced their desire to abuse children' (McMenamin 2008).

Potentially objectionable and harmful materials can also be countered through the promotion of awareness, good practice and better education.

> Automated tools and manual monitoring are used by some service providers to monitor content; other industry representatives argue that large information flows make manual monitoring impossible. Both stress that awareness and education remain key to effective online security (European Commission Information Society and Media Directorate-General 2007: 36).

It is also important for regulators and the general public to acknowledge that no internet filtering technology is foolproof and that it may be circumvented by computer and technology savvy

children and cybercriminals. MacKinnon, for example, has suggested that:

> [a]ccording to a 2000 Chinese Academy of Social Sciences (CASS) survey of Internet use in five Chinese cities, 10% of users surveyed admitted to regularly using, and 25% to occasionally using, proxy servers to circumvent censorship … A 2005 CASS Internet user survey, asking the same question in door-to-door interviews in five major Chinese cities, received the following response: 'never': 71.2%; 'seldom': 19.7%; 'sometimes': 5.9%; 'often': 2.5%; 'frequently': 0.6% … Anecdotal evidence further suggests that while many people – especially university students – are aware of proxy servers and know how to use them, the percentage of people using proxy servers daily to access blocked sites is relatively small (MacKinnon 2008: 33).

In a paper presented at the 6th Workshop on Privacy Enhancing Technologies held in Cambridge in June 2006, researchers from the University of Cambridge's Computer Laboratory described how the Great Firewall of China can be circumvented:

> The so-called 'Great Firewall of China' operates, in part, by inspecting TCP packets for keywords that are to be blocked. If the keyword is present, TCP reset packets (viz: with the RST flag set) are sent to both endpoints of the connection, which then close. However, because the original packets are passed through the firewall unscathed, if the endpoints completely ignore the firewall's resets, then the connection will proceed unhindered. Once one connection has been blocked, the firewall makes further easy-to-evade attempts to block further connections from the same machine. This latter behaviour can be leveraged into a denial-of-service attack on third-party machines (Clayton, Murdoch & Watson 2006: 20).

In another independent yet related piece of research, Crandall et al. (2007) discovered 122 keywords on the Great Firewall of China's blacklist previously unknown to the general public. They then argued that the list of known keywords on the blacklist could be used by individuals to circumvent internet filtering via keyword-based filtering in the following five ways:

> 1. IP packet fragmentation: … When the keywords are known, it is possible to implement a network stack replacement in the server's kernel that would automatically break up packets so as to divide keywords. 2. Insert HTML comments: It has also been suggested that HTML comments could be inserted into the middle of keywords [28], for example 'Fa<!-Comment ->lun Gong 3'. Use different encodings: Limited testing by ourselves and others [28] has demonstrated that often the GFC implementation does not check control characters in URL requests. Thus 'F%61lun Gong' and similar types of encodings may evade the firewall. 4. Captchas: For HTML responses (not URL requests) it may be possible to replace filtered keywords with captchas [23] that are an image of that word. 5. Spam: Given the empirical evidence that keyword filtering has not stopped the flood of unsolicited e-mail on the Internet, spam techniques would perhaps be the most effective way to evade keyword-based censorship, for example 'F@1un G0-ng'. The use of spam to evade the GFC's keyword filtering of e-mails has been reported … (Crandall et al. 2007: 361–362).

The CleanFeed system, a server-side internet filtering system, developed by British Telecom in consultation with the Home Office (Bright 2004), may also be circumvented as illustrated by Clayton:

> BT's CleanFeed was designed to be a low cost, but highly accurate, system for blocking Internet content. At first sight it is a significant improvement upon existing schemes. However, CleanFeed derives its advantages from employing two separate stages, and this hybrid system is thereby made more fragile because circumvention of either stage, whether by the end user or by the content provider, will cause the blocking to fail. This paper has described attacks on both stages of the CleanFeed system and set out various countermeasures to address them. Some attacks concern the minutiae of comparing URLs, while others address fundamentals of the system architecture. In particular, the CleanFeed system relies on data returned by the content provider, especially when doing DNS lookups. It also relies on the content provider returning the same data to

everyone. All of this reliance upon the content providers' probity could well be entirely misplaced. The CleanFeed design is intended to be extremely precise in what it blocks, but to keep costs under control this has been achieved by treating some traffic specially. This special treatment can be detected by end users and this means that the system can be used as an oracle to efficiently locate illegal websites. This runs counter to its high level policy objectives (Clayton 2005: 90).

The availability of a market in which to trade child exploitation materials for monetary gain will provide criminals with financial incentives to commit crimes. For example, cybercriminals can operate subscription-based private (by invitation only) IRC rooms that involve the highly disturbing practice of live child sexual abuse videos being streamed to these rooms, with the actual perpetrator responding in real time to commands from paying participants who can see the images. The future will see the development of new hardware devices and software programs that seek to circumvent internet filtering technologies.

> If CleanFeed is used in the future to block other material, which may be distasteful but is legal to view, then there will be no bar to anyone assessing its effectiveness. It must be expected that knowledge of how to circumvent the system (for all material) will then become widely known and countermeasures will become essential … A few days after this paper was presented at the PET Workshop, Brightview (a subsidiary of Invox plc) announced … that the oracle attack it describes was also effective against 'WebMinder', their own two stage content filtering system, used by the UK ISPs that they operate. Their design is architecturally similar to that of CleanFeed, but they are employing Cisco's proprietary Web Cache Communication Protocol version 2 (WCCPv2) to redirect suspect traffic to a number of patched squid proxy servers. In their announcement, Brightview also claimed that although their system had been vulnerable, they had now made the oracle attack 'no longer effective'. What they had done was to change stage one of the system to discard all packets with a TTL of less than 24 (Clayton 2005: 90).

## The need for harmonisation of online child grooming legislation

Despite increased awareness of online child exploitation in recent years, the recent enactment of international conventions such as the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse and the introduction of online child grooming offences in countries such as Australia, Singapore, the United Kingdom and the United States, there are jurisdictions that have yet to introduce legislation to criminalise online child exploitation. A recent report by the International Centre for Missing and Exploited Children (ICMEC 2006) found that 95 countries did not have legislation that criminalises child pornography, while 27 countries did not provide for computer-facilitated child exploitation offences at all (Appendix B).

This could, perhaps, be due to different policy priorities among differing countries. Grabosky (2007) observed:

> One of the most compelling illustrations of this is the current status of offences relating to Internet child pornography in the criminal justice systems of many nations. Heightening concerns about sexual exploitation of children in the 1990s happened to coincide with the growth in telecommunications and computing technology. These technological developments served greatly to facilitate the production, reproduction and dissemination of child pornography. Additional developments such as the widespread availability of strong encryption have further assisted in concealing this activity from the attention of law enforcement or other adversary interests. Given the technological, legal and cultural diversity of the world's nations, it is not surprising that priorities differ. Some nations are deeply concerned about theft of intellectual property; for others, blasphemous or seditious communications are of paramount concern. Others still are concerned about the application of digital technology for the sexual exploitation of children (Grabosky 2007: 207).

The use of online child grooming legislation often seeks to proscribe transnational criminal activity.

Recent legislation deals with this by enabling prosecutions to take place even if the accused or victim are located in different jurisdictions as long as there remains a sufficient connection with the place in which the prosecution is commenced. Where an accused is located in another country, however, it may be necessary to seek extradition. Australia, for example, may request the extradition from other countries of people who have committed acts online that adversely affect Australian citizens or interests to be returned to Australia to face prosecution (as governed by the *Extradition Act 1988* [Cth]).

As noted by Grabosky (2007), the 'nullum crimen sine lege' principle is relevant in most legal systems:

> Under this principle, behaviour, no matter how harmful, cannot be prosecuted unless it is formally prohibited by law. The person who released the I LOVE YOU virus in May 2000, for example, could not be prosecuted in the Philippines because there was no law in that country at the time that prohibited the release of malicious code (Grabosky 2007: 208).

Satisfying the criterion of dual criminality – the alleged misconduct must constitute an offence under both the laws of the extradition country and Australia – is invariably necessary in both extradition and mutual assistance requests.

> The concept of 'dual criminality' has been a procedural backbone of many, if not most, existing treaties on mutual legal assistance, but can also preclude more cooperative relationships in the investigation and prosecution of criminal matters. The use of the principle varies from one State to another, with some requiring dual criminality for all requests for assistance, some for compulsory measures only, some having discretion to refuse assistance on that basis, and some with neither a requirement or discretion to refuse (Dandurand, Colombo & Passas 2007: 268).

The lack of online child grooming legislation in some countries could impede police investigations and prosecutions as it may be impossible to extradite an offender identified in child grooming matters from countries with no online child grooming offences. There is, accordingly, a need for concerted law enforcement and international legislation to combat online child exploitation. Countries such as Australia, Singapore, the United Kingdom and the United States have a relatively comprehensive legislative framework in place to deal with online child grooming but, until the process of harmonisation of laws and sanctions is more advanced, disparities within and among countries will continue to create risks. A report prepared for the Committee on Energy and Commerce in the United States, for example, noted that:

> [w]hile the federal sentencing guidelines for criminal offenses relating to the sexual exploitation of children [in the United States] involve strict penalties, there is a wide discrepancy in state criminal codes both in covering all the substantive offenses, as well as in sentencing. Because approximately 70 percent of all cases involving the sexual exploitation of children over the Internet are prosecuted at the state level, state legislatures should consider enhancing the penalties for these offenses and, in some instances, passing additional criminal laws that address the sexual exploitation of children over the Internet (United States House of Representatives Committee on Energy and Commerce, Republicans 2007: 3).

Achieving some measure of uniformity will help to minimise the risk of 'jurisdiction shopping' where offenders seek out countries from which to base their activities that have the least severe punishments or which have no extradition treaties. With the recent creation of the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, Article 23, problems of lack of harmonisation may begin to be addressed, at least in European member states (Kierkegaard 2008).

# Non-legislative responses

This section 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. Fighting 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), where it was noted that tracking child pornography peddlers around the globe requires better international cooperation, agreed US investigators and leaders of NGOs.

Because most online environments are commercially owned and operated, there is an imperative for organisations to respond to corporate and shareholder interests (Grimes 2006). 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).

Private-sector involvement is, therefore, crucial in improving internet safety for children. As noted by McNulty (2007: unpaginated), '[e]ffective community outreach strategies will involve many nongovernmental organizations'.

## 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, for example, have been proactive in working with law enforcement agencies to protect children against sexual offenders online.

MySpace 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. 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 nonemergency cases. The MySpace safety team interfaces directly with law enforcement and helps agencies discover how MySpace can be helpful in their investigations (Nigam 2007: unpaginated).

Terms of use on social networking sites prohibit users from abusing the sites for activities such as harassment of other users and dissemination of objectionable materials.

- Facebook's terms of use (available at http://www.facebook.com/terms.php) include prohibiting their users from uploading, posting, transmitting, sharing, storing or otherwise making available any content that is deemed to be harmful, threatening, unlawful, defamatory, infringing, abusive, inflammatory, harassing, vulgar, obscene, fraudulent, invasive of privacy or publicity rights, hateful or racially, ethnically or otherwise objectionable.
- MySpace's terms of use (http://collect.myspace.com/misc/terms.html) include prohibiting their users from including telephone numbers, street addresses, last names and any photographs containing nudity, or obscene, lewd, excessively violent, harassing, sexually explicit or otherwise objectionable subject matter.
- Friendster's terms of use (http://www.friendster.com/info/tos.php) include prohibiting their users from harassing or advocating harassment of another person.

Users who violate these terms may have their accounts deactivated and in situations of a criminal nature, users may be reported to appropriate law enforcement agencies. One Facebook user, for example, had been disabled for 'misuse of the site'. Facebook explained to the user that 'It is a violation of Facebook's Terms of Use to harass users on the site, whether through unsolicited messages, friend requests, pokes or other features. We will not be able to reactivate your account for any reason. This decision is final' (Havenstein 2007b: unpaginated).

There are, however, concerns that these terms of use are not being enforced 'as vigilantly as they could and, thus, sexual predators are using these websites to find potential victims' (United States House of Representatives Committee on Energy and Commerce, Republicans 2007: 6).

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 Florida known sex offenders from MySpace (Kierkegaard 2008).

## Role of financial services industry

Because child pornography invariably involves payment, 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 (Hagenbuch 2006). 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 (Bank, credit card company efforts to combat child porn examined n.d.: unpaginated).

> [A]buse of children through child pornography is based on economic exploitation. The Landslide case which started in Texas, USA in which the perpetrators made millions of dollars from hosting child pornographic web sites, is a classic example of the third party child sexual exploiter. This case also led to the identification of over 7,000 people in the UK (know as Operation Ore) where their credit card had been used to access child abuse images through the Landslide website (Jones & Skogrand 2005: 22).

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, in March 2006 to eradicate commercial child pornography over the internet by 2008 (Shelby 2006). The Financial Coalition comprises major financial processors and internet service companies such as America Online, American Express Company, Authorize.Net, Bank of America, Bank of New York, Capital One, Chase Paymentech Solutions, CheckFree, Citigroup, Deutsche Bank Americas, Discover Financial Services LLC, e-gold, First Data Corporation, First National Bank of Omaha, First PREMIER Bank/PREMIER Bankcard, Global Payments Inc., Google, HSBC – North America, JP Morgan Chase, MasterCard, Microsoft, North American Bancard, Nova Information Systems, PayPal, ProPay Inc., Standard Chartered Bank, Visa, Washington Mutual, Wells Fargo and Yahoo! Inc.

The Prevention Working Group of the Financial Coalition identifies best practice associated with stopping the distribution and sale of child pornography over the internet and assists 'other Coalition members in evaluating their respective procedures for detecting commercial child pornographers and preventing commercial child pornographers from obtaining access to services offered by Financial Coalition members' (Financial Coalition Against Child Pornography 2007: 1). Examples of some of the best practices adopted by the Financial Coalition include:

- merchants exercising due diligence based on their own internal policies, regulatory requirements and procedures
- monitoring internet merchants on an ongoing basis by confirming the products being sold on the website, investigating links to the merchant's website, if any, to verify that no additional products or services are being processed through the merchant's account, and cross-referencing any known adult merchants with card information that might provide information on potentially illegal merchants
- using red flag indicators of suspicious activities such as variations in deposit frequency, transaction volume, average ticket price of each sale transaction, change in level of refunds and chargebacks, refunds to credit cards without any corresponding sales, and lack of merchant activity.

Financial institutions have recognised their responsibility to not knowingly contributing to illegal acts such as allowing their customers to pay for child exploitation 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 (Association of Banks in Singapore 2007: unpaginated).

Under another joint initiative, Microsoft and the International Centre for Missing and Exploited Children (http://www.icmec.org/) 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 pornography monitoring and oversight system, and developing and promoting systems for

identifying the victims of child pornography (Microsoft 2004a, 2004b). 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 exploitation materials.

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

> Involving financial institutions was necessary, particularly to impose effective sanctions on all who use a credit card to purchase illegal content. They have also experience with age verification methods (European Commission Information Society and Media Directorate-General 2007: 17).

## Online reporting and monitoring systems

Online reporting and monitoring systems are important tools in containing online child exploitation. 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 (European Commission Information Society and Media 2007a).

### *International*

The International Association of Internet Hotlines (https://www.inhope.org/), 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 (Table 23).

These hotlines monitor activities on the internet and allow members of the general public to report illegal internet content such as child pornography (see https://www.inhope.org/en/makereport.html).

**Table 23** Members of the International Association of Internet Hotlines

| Country | Website |
|---|---|
| Australia | http://www.au.inhope.org/ |
| Austria | http://www.at.inhope.org/ |
| Belgium | http://www.be.inhope.org/ |
| Canada | http://www.ca.inhope.org/ |
| Chinese – Taiwan | http://www.tw.inhope.org/ |
| Cyprus | http://www.cy.inhope.org/ |
| Czech Republic | http://www.cz.inhope.org/ |
| Denmark | http://www.dk.inhope.org/ |
| Finland | http://www.fi.inhope.org/ |
| France | http://www.fr.inhope.org/ |
| Germany | http://www.de.inhope.org/ |
| Greece | http://www.gr.inhope.org/ |
| Hungary | http://www.hu.inhope.org/ |
| Iceland | http://www.is.inhope.org/ |
| Ireland | http://www.ie.inhope.org/ |
| Italy | http://www.it.inhope.org/ |
| Japan | http://www.jp.inhope.org/ |
| Malta | http://www.mt.inhope.org/ |
| Netherlands | http://www.nl.inhope.org/ |
| Poland | http://www.pl.inhope.org/ |
| Portugal | http://www.pt.inhope.org/ |
| Slovenia | http://www.si.inhope.org/ |
| South Korea | http://www.kr.inhope.org/ |
| Spain | http://www.es.inhope.org/ |
| United Kingdom | http://www.uk.inhope.org/ |
| United States | http://www.us.inhope.org/ |

Source: https://www.inhope.org/

### *Europe*

The European Commission-funded Safer Internet plus Programme (2005 to 2008), in its third edition and with a budget of €45m, has established a European network of hotlines for the reporting of illegal content (e.g. the hotline in Ireland (http://www.hotline.ie/) run by the Internet Service Providers Association of Ireland) and a European network of national nodes performing awareness-raising activities and running helplines (European Commission Information Society and Media 2007b).

## United Kingdom

The Internet Watch Foundation (http://www.iwf.org.uk/), which is based in the United Kingdom, is predominantly an internet and mobile industry-funded self-regulatory body. It works in partnership with law enforcement and government departments in Britain to combat online abuse. The online hotline reporting system operated by the Internet Watch Foundation allows members of the public and information technology professionals to report their exposure to potentially illegal content, particularly images of child abuse hosted anywhere in the world, criminally obscene images hosted in the United Kingdom and criminally racist content hosted in the United Kingdom. The system also assists content providers such as ISPs to combat abuse of their services with a 'notice and take-down' service that alerts them to any potentially illegal content on their systems and simultaneously invites the police to investigate the publisher (IWF 2007). Other services provided by the Internet Watch Foundation include providing lists of websites that contain child abuse content and lists of newsgroups that regularly contain or advertise child abuse content for organisations such as ISPs, mobile network operators, software companies and search engines so they can block access to potentially illegal child abuse images.

## United States

In the United States, the Association of Sites Advocating Child Protection (http://www.asacp.org/) is the equivalent of the Internet Watch Foundation. The Association of Sites Advocating Child Protection operates an online hotline that allows the public and information technology professionals to report suspected child pornography, investigates these reports and determines the hosting, billing, IP address, ownership and linkage of suspected child pornography sites. The Association then forwards red flag reports to appropriate government agencies and associations such as the FBI and the National Center for Missing & Exploited Children, as well as their counterparts in other countries.

## Canada

The Canadian Centre for Child Protection operates the 24-hour Cybertip.ca hotline (http://cybertip.ca/en/cybertip/), which is based in Winnipeg. Reports of online sexual exploitation of children are then forwarded to appropriate law enforcement agencies. In November 2007, a proposed bill to amend the existing Child and Family Services Act so that individuals will be required to report any suspected cases of child abuse (directed through the Cybertip.ca website) was introduced in the Province of Manitoba. Several successful arrests attributed to the hotline have since been recorded (http://cybertip.ca/en/cybertip/success_stories/).

Since its launch, Cybertip.ca has received close to 25,000 reports resulting in 2,800 websites being shut down, at least 30 arrests and the removal of a number of children from abusive environments (Province of Manitoba 2007: unpaginated).

## Sharing information among hotlines

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 pornography 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 (Jones & Skogrand 2005). In the case of Ireland, for example, in 2006 no report received by the Hotline referred to illegal child pornography 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 (Save the Children Denmark 2005). 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 n.d.: 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 (e.g. age of consent as illustrated in Table 20 and lack of legislation to criminalise online child exploitation as illustrated in Appendix B). 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. A recent report published by the National Institute of Justice highlighted one such example:

> In Virginia, for example, an Internet service provider called the National Center for Missing & Exploited Children's CyberTipline to report that a subscriber had posted pornographic photos involving children to an online group. Analysts used Internet search engines to find the suspect's name, address, and Social Security number. The local sheriff, working with the FBI, secured warrants and arrested the suspect, who pled guilty to distributing child pornography (Albanese 2007: 8).

In another example highlighted by the Save the Children Europe Group, a Danish couple (a stepfather and his wife) were reportedly convicted for sexually abusing their 11-year-old daughter. Photo and video images of the sexual abuse were allegedly distributed over the internet and traded with members of an online network of sexual abusers. The sexual abuse reportedly occurred within the families of the members of the network.

> The abuse [allegedly] involved sado-masochism and torture of children in Europe and USA. The cooperation between Interpol, Danish police, FBI, and US Customs Service led to arrests worldwide and massive media attention. Over 100 children who were abused by the network were identified in the USA. The Danish girl was allegedly trafficked within Denmark and abroad to be sexually abused. Information leading to the arrest of the Danish abuser was passed onto the police by the Save the Children Sweden Hotline who became aware that abusive images found in a newsgroup contained information suggesting the male abuser was Danish (his T-shirt had a Danish Company Logo). This led to the infiltration of the worldwide network of sexual abusers (Jones & Skogrand 2005: 28).

A submission by British Telecom to the European Commission's Safer Internet and Online Technologies for Children program also highlighted the effectiveness of online reporting and monitoring systems:

> BT strongly commends INHOPE and its hotlines in their coordinating work. We believe that the body has been a major factor in the successful fight against child abuse images being hosted in the EU and third countries. Therefore, BT calls on the [European] Commission to continue its support for the coordination node and to invest greater effort in global cooperation (British Telecom 2007: 1–2).

These success stories underscore the importance of establishing good working relationships among online reporting and monitoring systems (including ISPs), law enforcement agencies and overseas counterparts.

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 and social network analytical tools

## *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 our use of ICT increases and evolves. Ferraro and Russell, for example, noted that:

> [p]olice officers cannot keep pace with the evolution of technology. Their role is reactive, not proactive. There is a great need for forensic scientists to develop tools and tactics to retrieve and preserve evidence from emerging and complex technologies … Computer forensic experts should be responsible for obtaining data from networked environments. Intrusion investigations require sophisticated log analysis that one could not expect the average police officer to conduct. We need scientists to pioneer methods of extracting evidence and ensuring its stability and integrity (Ferraro & Russell 2004: 9).

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 pornography. 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 (LexisNexis 2007). 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 (http://www.sentryweb.com/safe.aspx), 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 (http://ncecc.ca/cets_e.htm), has reportedly been adopted by various international law enforcement agencies (including Romania, see Zaharia 2007).

> Even during beta testing, CETS proved its value by helping police investigate a man accused of sexually assaulting a four-year-old girl. CETS also figured prominently in the March 2006 arrest of 27 people in four countries who operated a private chat room to groom vulnerable children (http://www.microsoft.com/industry/publicsector/government/cetsnews.mspx).

BlueBear Law Enforcement Services (http://www.bb-les.ca/) is another example of a Canadian company that designs software specifically for use in online child exploitation investigations by law enforcement agencies.

> LACE (Law Enforcement Against Child Exploitation) software, in the final stages of development from BlueBear Inc. located in Gatineau, Quebec, Canada, helps investigators sort and categorize images found on seized computer hard drives in child exploitation cases. First used in 2006 in an alpha version by the York Regional Police, located in Ontario, Canada, LACE also helps agencies avoid duplicating efforts by enabling the sharing of image categorizations (Kanable 2007: unpaginated).

The software reportedly allows users to perform automated image appearance matching, automated face detection and extraction, face identification and fast-speed evidence media categorisation, and provides integrated reporting and case writing systems and interfaces to existing computer forensic tools (http://www.bb-les.ca/En/solutions/LACE-features.html). These features allow investigators to more easily manage massive amounts of child exploitation materials.

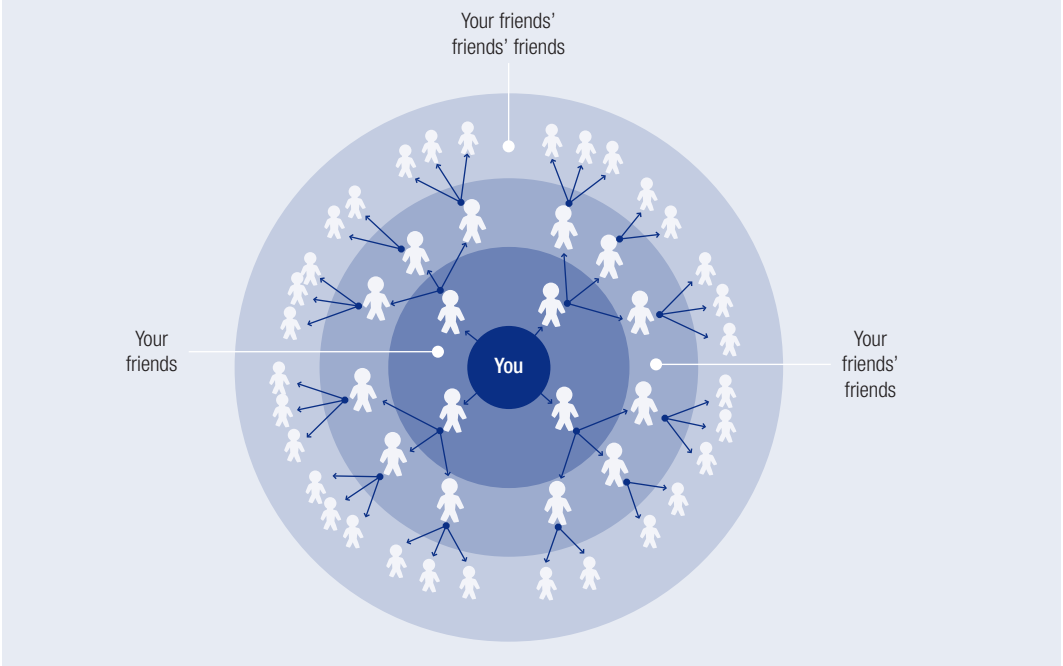
In Australia, the collaboration between computer science researchers from the University of South Australia's Enterprise Security Management Laboratory and law enforcement officers from South Australia Police's Electronic Crime Section has resulted in the development of several investigative tools designed to assist South Australia 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 pornography, 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.

Despite the controversy surrounding the use of surveillance tools – such as keylogging tools (Hilley 2007), spyware (Keizer 2007) and Trojan programs (Hilley 2007; Leyden 2007a) – 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 researchers from Rensselaer Polytechnic Institute's Department of Computer Science is one such example (Camtepe, Krishnamoorthy & Yener 2004). 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.

## *Social network analytical tools*

Any individual can create multiple online identities or have multiple avatars (virtual representations of themselves) and be a member of more than one social networking site at any one time. As illustrated in Figure 5, there are various types of relationships (or degrees of linkage) between individual user identities in online social networking sites such

**Figure 5** Virtual network of friends




Source: Adapted from http://computer.howstuffworks.com/myspace.htm

as MySpace and Friendster. These virtual relationships in online social networking sites can be broadly categorised into:

- direct linkages between two online user identities (e.g. friends)
- quasi-direct linkages between two online user identities (e.g. friends' friends)
- indirect linkages between two online user identities (e.g. user identities who are 'somehow' connected to a particular user identity via quasi-direct linkages).

Social network analytical tools such as mapping tools can be extremely useful for law enforcement investigators when establishing virtual relationships and connections between sexual offenders and their potential victims, understanding these relationships and connections, and analysing their implications in online social networking sites. For example, a researcher from the Queensland University of Technology presented a social network analytical framework to measure the level of activity of individual members of the Jemaah Islamiyah 2002 cell in Bali, their ability to access others, and the degree of control over the flow of information within the network (Koschade 2006). In another independent work, researchers from the Chinese University of Hong Kong and the University of Pennsylvania developed two visualisation techniques that could facilitate the exploration of terrorist social networks (Yang, Liu & Sageman 2006). Such techniques can also be used to facilitate the extraction of the hidden relationships among child sexual offenders in the social networking sites through user interactions.

Another freely available mapping tool, MySpace Friend Mapper (http://www.lococitato.com/), uses an individual's MySpace profile and generates animated clickable maps of the relationships between the individual and their MySpace friends. The tool, as suggested by Wagner (2007), can facilitate investigators establishing connections between MySpace friends, visually provide connections between user identities without having to manually build a graph of these connections, establish connections between user identities that might not have been obvious by just viewing a particular user identity's top friends, and provide a useful diagram that can be added to a case file and used in court.

Klerks (2001) from the Dutch National Police Academy in Apeldoorn has categorised social network analytical tools into first-generation, second-generation and third-generation tools. First-generation tools are non-computer aided tools designed to 'describe' criminal activities as a network of associations. Second-generation tools, such as Netmap (http://www.netmap.com.au/) and i2 Analyst's Notebook (http://www.i2.co.uk/Products/Analysts_Notebook/default.asp) provide pattern identification and graphic representations of simple raw data obtained from phone taps and physical surveillance reports. These tools assist investigators understand the relationships between entities. Third-generation tools have a more in-depth focus on the content of the contacts, the social context and the interpretation of such information. Research into third-generation tools is still ongoing and as Marshall and Chen (2006: 16) noted, '[third-generation social network analytical tools are] yet to be widely deployed [although these] techniques and methodologies have been explored in the research literature'.

## *The need for further research*

The future will see the need for investigative and social network analytical tools designed for law enforcement to be validated and accredited by international standard bodies to ensure that the results obtained using such tools can be used in judicial proceedings. Governments might also need to consider whether it is necessary to either introduce new legislation, or to amend existing legislation, so that evidence garnered through the use of surveillance tools such as keylogger, spyware and Trojan programs is admissible.

Defendants may also argue that their computer was infected with 'malicious' surveillance tools that made it perform functions beyond their control and without their knowledge when child exploitation materials are discovered on their personal computers. For example, the successful installation of a Trojan program on a defendant's computer cedes control of the computer in question to the Trojan operator. The latter may then be in a position to plant incriminating material or perform illegal actions using the defendant's computer and identity, thus bringing in a reasonable doubt that the defendant

committed an offence. It can be expected that such arguments will continue to be advanced. Law enforcement officers, prosecutors and the research community will need to determine the types of tests that could be applied to ensure that evidence collected via such covert and intrusive technical means was not planted by anyone other than the accused.

# Internet filtering

The increasing amount of potentially objectionable material online underscores the need for internet filtering and parental control technologies.

> Some 'frustration' was expressed over the non-use of existing technology to block sites. The online industries have a responsibility to assist with blocking access to sites (e.g. via the 'cleanfeed' method), while filtering and parental control software were also mentioned by many (European Commission Information Society and Media Directorate-General 2007: 16).

Content classification and filtering systems, developed to control access to undesirable content online, include rating systems designed to confer values on content, based on certain criteria. Filtering systems are designed to enforce certain predetermined filtering policies and to evaluate, according to those policies, whether a user can or cannot access specified material. One of the oldest and more commonly utilised internet filtering techniques is based on proprietary URL collections. Each URL is associated with a specific content category. When a webpage is requested, the classifier checks its address in the database in search of its category (e.g. http://www.friendster.com will be classified as a social networking site). With the definition of the category, the filter can block or release access to the site, according to the policy of internet use configured by the organisation, individual or ISP (Forte, de Souza & do Prado 2006).

There are various definitions and types of internet filtering systems (Bertino, Ferrari & Perego 2003; Clayton 2005; Rosenberg 2001; Zittrain & Edelman 2003). The American Library Association, for example, defines blocking/filtering software as a mechanism used to restrict access to internet content based on an internal database of the product, or to restrict access to internet content through a database that is external to the product. Such software can also restrict access to internet content due to certain ratings assigned to those sites by a third party, or restrict access to internet content by scanning text based on a keyword or phrase or text string. It is also possible to restrict access to internet content by scanning pixels, based on colour or tone, or to restrict access to internet content based on the source of the information (http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13090).

Internet filtering software can be broadly categorised into server-side filtering systems and client-side (or user-side) filtering systems:

- In server-side filtering systems, the filtering or content rating software is installed on the servers of internet content providers or ISPs.
- In client-side filtering systems, the responsibility for blocking potentially objectionable materials is shifted away from internet content providers or ISPs to individuals as the software is installed on personal computers of consumers.

## *Server-side filtering systems*

ISPs, as Ellison (2000) observed, need to work in collaboration with governments and regulators. Telenor (Norway's ISP), for example, jointly developed a server-side filtering system with KRIPOS (Norway's National Criminal Investigation Service). The filtering system, operative from October 2004, applies to all Telenor's dial-up lines and broadband internet subscribers. Website requests from Telenor's internet subscribers are checked against a blacklist of websites to be blocked (e.g. websites that allegedly host child pornography) provided by KRIPOS.

> Should any of Telenor's customers attempt to open a web site containing child pornography, a blocking site will automatically pop up, containing information about the filter, as well as a link to KRIPOS. Several hundred sites containing illegal child pornography are currently registered in KRIPOS' files (Telenor 2004: unpaginated).

Another similar server-side filtering system is the CleanFeed system developed by British Telecom in consultation with the Home Office (Bright 2004).

> Subscribers to British Telecom's internet services such as BTYahoo and BTInternet who attempt to access illegal sites will receive an error message as if the page was unavailable. BT will register the number of attempts but will not be able to record details of those accessing the sites. A list of illegal sites compiled by the Internet Watch Foundation, the industry's watchdog, has been available for some time, but until now there has been no way to prevent people accessing them because most are based outside the UK (Bright 2004: unpaginated).

However, not all ISPs will agree to install server-side filtering systems or terminate offending websites, particularly in countries where ISPs are not legally obliged to do so.

### *Client-side filtering systems*

Children may inadvertently access material or may have material sent to them as part of a grooming process. In such circumstances, parents can play a role in regulating potentially objectionable content by using (client-side) internet filtering software. Client-side internet filtering software allows individuals such as parents, teachers and librarians to self-select the types of content to be blocked on their computers. Blue Coat® K9 Web Protection software (http://www1.k9webprotection.com/) is an example of a freely available client-side internet filtering tool. After installing the software on a computer, individuals (e.g. parents) can manually configure the software to block access to inappropriate content based on various settings. For example, people can specify the following internet protection levels on their computer:

- 'high' protects against all default-level content, chat, newsgroup and unrated sites
- 'default' protects against all adult content, security threats, illegal activity, sexually related sites and online community sites
- 'moderate' protects against all adult content, security threats and illegal activity
- 'minimal' protects against pornography and security threats
- 'custom' allows individuals to select their own categories of content to be blocked (e.g. phishing category).

Individuals can also specify time restrictions on internet access such as blocking access during school hours, provide website exceptions in which access to specific sites is explicitly blocked, or introduce blocking effects such as an audible alert when a user attempts to access a blocked site. It is also possible to specify selected URL keywords and, for example, block access to webpages based on keywords such as 'sex'. In addition, individuals can specify search options that seek to reduce the amount of adult material that might be returned as a result of an internet search. The K9 Web Protection software also allows parents to view the internet browsing activity of their child on the computer on which the software is installed (Blue Coat 2007).

## Rating systems

Effective regulation of internet and gaming content through the use of rating systems requires coordination at regional, national and international level. The Pan-European Game Information age-rating system (http://www.pegi.info/en/index/id/175) is one such system. It uses a voluntary self-regulated framework to promote the safe use of video games. The Pan-European Game Information, established in 2003, is designed to help European parents make informed decisions when buying interactive games and to ensure that minors are not exposed to games that are unsuitable for their particular age group.

The system is supported by the major console manufacturers, including PlayStation, Xbox and Nintendo, as well as by publishers and developers of interactive games throughout 28 European countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Sweden, Switzerland and the United Kingdom (PEGI 2007).

Categories of game ratings established by members of the game industry itself are:

- Bad language – game contains bad language
- Discrimination – game contains depictions of, or material that may encourage, discrimination
- Drugs – game refers to or depicts the use of drugs
- Fear – game may be frightening or scary for young children
- Gambling – game encourages or teaches gambling
- Sex – game depicts nudity and/or sexual behaviour, or sexual references
- Violence – game contains depictions of violence.

Although technologies such as content classification and filtering systems on their own cannot solve problems of online child exploitation, regulators and the general public can use them to restrict or deny children and younger people access to known sites containing potentially objectionable materials, social networking sites, IRC rooms or games that promote sexual behaviour or sexual references.

> A combination of hardware and software methods, and awareness raising and education, can counter the threat of accessing 'non-advisable content' … Parents, held responsible for ensuring safety through technology, would benefit from easier application methodologies for security features. Many are unaware [or] unable to use access control tools and safe filters (European Commission Information Society and Media Directorate-General 2007: 36).

Parents, teachers and other individuals have responsibilities to mitigate risks encountered by children online. Other effective strategies that can be adopted by parents and others include promoting responsible usage of the internet and using child-oriented search engines such as Yahooligans! (http://kids.yahoo.com/) and Google SafeSearch. This requires the internet browser to be configured to ensure that the Google SafeSearch filtering system is activated. This can be done by:

1 visiting http://www.google.com
2 clicking on 'Preferences'. In 'SafeSearch Filtering', select either of the following filtering options by clicking on the button next to the option:
   – strict filtering (filters both explicit text and explicit images)
   – moderate filtering (filters explicit images only – default behaviour)
3 clicking on 'Save Preferences'.

There is, arguably, a need for continued support from both the public and private sectors to develop and enhance existing technological tools such as internet filtering and content-rating software for use in tracing, analysing and blocking websites that host potentially objectionable materials. For example, the design of client-side internet filtering and content-rating software should be easy to use for the average individual.

> User-end/client side filtering was therefore seen by many as the way forward – though this puts the responsibility often firmly on parents' shoulders. Hence many argued that filtering methods need to be easy to install, use and handle. Some contributors raised concerns about the low take-up of effective filtering software even when costs are marginal; some children's NGOs (especially in the UK) are campaigning to have internet safety software pre-installed on PCs. Where filtering has been felt to be complicated to use (e.g. in some schools) 'users are put off and either don't use it at all or just accept the manufacturer's default and are then subsequently frustrated' by over-blocking (European Commission Information Society and Media Directorate-General 2007: 23).

Programs to inform and educate the general public, particularly parents and school staff, of the choice of technological tools available should also be in place. There is also a need to develop robust age-identification and verification systems that can restrict or deny access to children and younger people to known sites containing potentially objectionable or adult materials.

## International task forces

Establishing international collaboration among international law enforcement agencies will assist in identifying perpetrators, leading to charges and success in prosecutions. The use of police task

forces is likely to provide an effective means of sharing intelligence among law enforcement agencies in multiple jurisdictions.

The Virtual Global Taskforce (http://www.virtualglobaltaskforce.com/) is an excellent example of how law enforcement agencies from various countries work together to fight online child exploitation. It comprises members from Australia (Australian Federal Police Online Child Sex Exploitation Team), Canada (National Child Exploitation Coordination Centre as part of the Royal Canadian Mounted Police), Italy (Italian Postal and Communication Police Service), the United Kingdom (Child Exploitation and Online Protection Centre), the United States (United States Immigration and Customs Enforcement) and Interpol.

More than 700 suspects associated with an organised paedophile ring operating in the UK-based IRC room, Kids, the Light of Our Lives, were arrested worldwide following the international operation led by the Child Exploitation and Online Protection Centre, a member of the Virtual Global Taskforce (UK CEOP 2007b). Jewkes and Andrews (2007) also noted that:

> [t]he online reporting facility was instrumental in securing CEOP's first successful arrest and prosecution, when a woman in Nottinghamshire, UK, reported via the http://www.virtualglobal taskforce.com site that her 14-year-old daughter had been sexually abused after being groomed on the Net. In June 2006, the judge in the trial of 21-year-old Lee Costi endorsed the tough message of the CEOP Director by sentencing Costi to nine years in prison on three counts of sex with children, three counts of Internet child grooming, five of making indecent images of children and one of possessing over 40 indecent images (Jewkes & Andrews 2007: 71).

On the Most Wanted website (http://www.ceop.gov.uk/wanted/ and http://www.crimestoppers-uk.org/wanted/), operated by a partnership between the Child Exploitation and Online Protection Center, and Crimestoppers (an independent charity organisation), details of child sexual offenders are recorded. These include photographs, names and aliases, dates of birth and other identifying information of individuals who have gone missing from police management while on the sex offenders register, including failing to comply with the Notification Requirements under the Sexual Offences Act 2003. Nine of the United Kingdom's highest-risk child sexual offenders, missing for a combined total of over 20 years, have been reportedly located in the last 12 months as a direct result of the Child Exploitation and Online Protection Centre's Most Wanted website (UK CEOP 2007c).

The multidisciplinary Internet Taskforce for Child Protection on the Internet (http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce), established in March 2001, is an example of a public–private partnership that brings together government, law enforcement, children's agencies and the internet industry in the fight against online child exploitation. The task force, currently chaired by Vernon Coaker, Home Office Under-Secretary for Police and Security, provides information and recommendations for the moderation of public interactive communication services aimed at, or very likely to attract, children in the following areas: information and advice to users, risk assessment, recruitment, training, data security, management and supervision, and escalation procedures.

In the United States, the Innocent Images International Task Force, which became operational in June 2004, comprises law enforcement officers from Europol and: Australia, Belarus, Canada, Croatia, Cyprus, Fiji, Finland, Germany, Latvia, Netherlands, New Zealand, Norway, Philippines, Sweden, Thailand, the United Kingdom and Ukraine (FBI 2006). The task force allows real-time transfer of information between the FBI and other task force members and their countries. More than 30 international law enforcement officers have reportedly worked side-by-side with their FBI counterparts at the Innocent Images Unit. Table 24 sets out the most common crimes investigated under the Innocent Images National Initiative, a component of the FBI's Cyber Crimes Program.

The total number of arrests made as a result of the Innocent Images National Initiative between fiscal years 1996 and 2006 was 7,700, and the number of convictions and pre-trial diversions for the same period was 5,840.

**Table 24** Most common crimes investigated under the Innocent Images National Initiative

| United States Code | |
|---|---|
| 18 USC 1462 | Importation or transportation of obscene matters |
| 18 USC 1465 | Transportation of obscene matters for sale or distribution |
| 18 USC 1466 | Engaging in the business of selling or transferring obscene matter |
| 18 USC 1467 and 18 USC 2253 | Criminal forfeiture |
| 18 USC 1470 | Transfer of obscene material to minors |
| 18 USC 2241(a)(b)(c) | Aggravated sexual abuse |
| 18 USC 2251(a)(b)(c) | Sexual exploitation of children |
| 18 USC 2251A(a)(b) | Selling or buying of children |
| 18 USC 2252 | Certain activities relating to material involving the sexual exploitation of minors |
| 18 USC 2252A | Certain activities relating to material constituting or containing child pornography |
| 18 USC 2254 | Civil forfeiture |
| 18 USC 2257 | Record-keeping requirements |
| 18 USC 2260(a)(b) | Production of sexually explicit depictions of a minor for importation into the US |
| 18 USC 2421 | Transportation generally |
| 18 USC 2422 | Coercion and enticement |
| 18 USC 2423(a) | Transportation of minors with intent to engage in criminal sexual activity |
| 18 USC 2423(b) | Interstate or foreign travel with intent to engage in a sexual act with a juvenile |
| 18 USC 2425 | Use of interstate facilities to transmit information about a minor |
| 18 USC 13032 | Reporting of child pornography by electronic communication service providers |

Source: http://www.fbi.gov/publications/innocent.htm

In Australia, the Australian Federal Police's Online Child Sex Exploitation Team performs an investigative and coordination role for multijurisdictional and international online child sex exploitation matters. The cases include those from Australian state and territory police, government and non-governmental organisations (including ISPs and internet content hosts), the Australian High Tech Crime Centre, the Virtual Global Taskforce, international law enforcement agencies, Interpol and members of the public. In September 2004, the Online Child Sex Exploitation Team conducted Operation AUXIN in which over 700 suspects were investigated for a variety of offences in connection with accessing child pornography via web access groups in which payments were made using personal credit card accounts. Operation AUXIN was the Australian component of the larger Falcon Operation conducted in the United States, France, Spain and Belarus, which led to over 2,000 arrests. Statistics obtained from Operation AUXIN indicated that the dominant profile of offenders arrested was that they were male and were over 30 years of age. Female offenders, often thought to be far less visible and overlooked, composed 3.1 percent of the offenders. Statistics, however, indicated that they were more likely (1.6 times) to have dependant children and greater access to children.

## Specialist units

Specialist behavioural units are another invaluable resource for law enforcement. In the United States, the Behavioral Analysis Unit provides the FBI with 'behavioural-based investigative and operational support by applying case experience, research, and training to complex and time-sensitive crimes, typically involving acts or threats of violence', which include crimes against children (FBI n.d.: unpaginated).

In the United Kingdom, the Child Exploitation and Online Protection Behavioural Analysis Unit, a specialist unit comprising forensic psychologists and specialists in forensic behaviour analysis focused on improving and sharing understanding of how sexual offenders operate and think, was launched by the Home Secretary the Rt Hon. Jacqueline Smith MP. Members of the Behavioural Analysis Unit who have backgrounds in child sex offence investigation and behavioural analysis conduct de-briefing interviews with incarcerated sexual offenders to examine how they went about their crimes to learn more about offenders and their motivations (UK CEOP 2007a).

> CEOP conducts interviews overseas through its membership of the Virtual Global Task Force, an international alliance of law enforcement agencies working to prevent online child abuse. If a British national was imprisoned in Australia, for example, members of CEOP's behavioural

> analysis unit would liaise with Australian police to enter their prison and conduct an interview. 'There are no incentives offered for offender participation. What our staff do say to them is that they're in prison, on the sex offenders' register and this is their chance to give something back, to explain their side of the story and help us understand better the minds of offenders. It's a confidential interview, it doesn't go beyond our building. But if someone discussed an unsolved crime then that information would be passed on to the police. The offenders are made aware of this' (Sex offenders explain how and why 2007: unpaginated).

The National Center for Missing and Exploited Children Child Victim Identification Program (http://www.cybertipline.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=2444) is another specialist unit that provides technical assistance to both US and international law enforcement agencies in the investigation of child exploitation cases. Program analysts examine files involving seized child pornography submitted by law enforcement agencies using the National Center for Missing and Exploited Children's Child Recognition and Identification System. Child victims can then be identified by visually inspecting the images. Analysts can reportedly review an average of 1,000 files in 30 minutes (NCMEC 2006), and age verification is also provided for each identified child victim. More than six million child exploitation images have reportedly been reviewed by Child Victim Identification Program analysts (United States House of Representatives Committee on Energy and Commerce, Republicans 2007).

During the image analysis, investigative clues that may lead to the location of the child victim are forwarded to appropriate law enforcement agencies for the possible location of the child victim. Information regarding newly identified victims of child pornography is also added to the National Center for Missing and Exploited Children's database. The Children's Child Victim Identification Program has been instrumental in the rescue of 880 children to date (United States House of Representatives Committee on Energy and Commerce, Republicans 2007). Interpol also has a similar database of 475,899 child exploitation images, with 426 child exploitation victims having been rescued up to May 2006.

## Training in computer forensics

With increased digitisation of information, digital content will increasingly become source of disputes or part of underlying evidence to support or refute a dispute in judicial proceedings.

> What is lacking, however, are studies that examine how law enforcement agencies are dealing with the ubiquity of digital evidence in criminal investigations, not just those involving electronic crimes. Certain [US] federal agencies have indicated at least 80% of all cases involve digital evidence, and the volume of evidence per case is increasing (albeit not as rapidly as Moore's law). The quantity and complexity of digital evidence are expected to overwhelm law enforcement capabilities. Moreover, the legal community and the judiciary are unprepared to deal with the digital evidence brought into legal proceedings. According to a preliminary study by Losavio and colleagues, judges, in general, are uncomfortable with their knowledge of digital evidence. Furthermore, they are unsure about the weight that should be given to digital evidence and whether or not digital evidence should admitted at trial (Rogers et al. 2007: 42).

Better-educated criminals are likely to explore alternatives to hiding data over the internet. These include storing data on password-protected file-sharing websites, email accounts and less reputable content providers hosted in countries with lax cybercrime legislation. Criminals are also likely to leverage the use of anti-forensic tools and information-hiding tools, including steganography, to further impede collection of evidence.

Digital evidence, typically the first step in any computer forensic process, can be broadly defined as any relevant information or data in electronic storage used to support or prove a fact at issue in judicial proceedings. The three broad ways in which digital evidence can be categorised are:

- records that are computer-stored, examples include email messages, word processing files, digital images and digital videos
- records that are computer-generated, examples include log files generated by web servers and IRC room servers
- records that are partially computer-stored and partially computer-generated, examples include Excel spreadsheets that contain both human statements and computer processing (Standards Australia International 2003).

Digital evidence differs from traditional evidence in a number of respects. The former is intangible and often transient in nature, and can easily be duplicated, copied, shared, disseminated, modified and damaged. A recent case involving Jim Selim of the now-defunct Pan Pharmaceuticals (AAP 2007d) is an indication of how easily electronic data can be destroyed to prevent investigators from acquiring forensic information.

To ensure all elements of a proper (digital) evidentiary foundation are correctly established, an understanding of fundamental characteristics underlying digital evidence is crucial, in addition to traditional evidential procedures being maintained (e.g. thorough documentation to ensure chain of custody). For example, volatile storage media such as hard drives should be stored in static-free bags and recorded. They should be marked as evidence and not be stored near anything – particularly magnets – that could damage evidence on the device.

With the advent of more complex data storage and dissemination technologies, forensic investigators face an increasingly difficult task. These developments (in data storage and dissemination technologies) can impede forensic investigators and prevent police from acquiring digital evidence and analysing digital content forensically in terms of time and resources. Examples include:

- different formats and platforms used to store digital content – constantly evolving formats are independently being developed by different vendors according to different standards. The proprietary storage media (e.g. iPod, flash memory and USB memory stick) and proprietary cryptographic algorithms used (e.g. encryption) could be incompatible with one another and compromise the integrity of the data during extraction or when converting from incompatible proprietary formats. Therefore, an in-depth understanding of how different technologies and applications operate is crucial in collecting digital evidence. Moreover, in response to changing contexts, various computer forensic tools and techniques have to be redesigned and re-engineered
- increased data storage capacities – the best form of immediate back-up to make is a binary disk image (also referred to as bit stream back-up or mirror image back-up). Enhanced data storage capacities (e.g. large-volume datasets) and more complicated data accessibility (e.g. networks of interconnected computers located in different locations) will impede bit stream back-up in terms of time and resources.

In a recent National Institute of Justice-sponsored survey, 667 US state and local law enforcement agencies selected from the National Public Safety Information Bureau's database were contacted by mail and asked to answer a series of questions about digital evidence (Rogers et al. 2007). A total of 279 agencies responded to the survey (Table 25).

**Table 25** Respondents to Rogers, Scarborough, Frakes and San Martin's law enforcement survey (number)

| Type of agency | Responses |
|---|---|
| Municipal | 138 |
| County sheriff | 70 |
| County police | 19 |
| State police | 43 |
| Marshal | 3 |
| FBI | 3 |
| Merged county and municipal | 1 |
| State sheriff | 1 |
| City sheriff | 1 |
| Total | 279 |

Source: Adapted from Rogers et al. (2007)

The survey found that:

- 80 percent of the respondents reported that no more than 25 percent of their cases involved digital evidence

respondents from municipal departments reported that most of their cases did not involve digital evidence.

The findings, as suggested by the authors, contradicted the estimates reported by federal law enforcement agencies (e.g. approximately 80 percent of cases handled by the FBI involved some form of digital evidence). This could, perhaps, be due to state and local law enforcement agents mainly focusing on traditional physical and/or document-based evidence because they have limited knowledge and resources to deal with digital evidence (Rogers et al. 2007). Armagh and Battaglia (2006: 7) also noted that '[i]nvestigating cases of child sexual exploitation in which computers were used is complex. The demands of these investigations may exceed the resources available to a jurisdiction'.

Other organisations, such as ISPs and IRC operators, may also record information such as logs of network activity on computers and email servers located in other countries. In online child exploitation cases, evidence is likely to be stored on hundreds or thousands of computers and various ISPs and IRC servers located in various jurisdictions.

> The modern criminal, using the same devices as today's teenagers, communicates with Voice over Internet Protocol, video instant messaging, cellular camera phone, and text messaging in a computer slang that is foreign to most police officers and parents. The trail to uncover this valuable investigative resource often starts with a forensic examination, but this trail quickly grows cold as Internet Service Providers overwrite logs and data retention periods expire. All police agencies are facing the same challenge when dealing with computer forensics. Police managers must find a way to examine an increasing number of digital devices, each containing an immense volume of data, in a timely manner and with limited resources (Cohen 2007: unpaginated).

This would require computer forensic investigators and incident handlers to have in-depth knowledge of computer forensic principles, guidelines, procedures, tools and techniques, as well as anti-forensic tools and techniques.

> Microsoft's Xbox game console can be modified to run additional operating systems, enabling it to store gigabytes of non-game related files and run various computer services. Little has been published, however, on procedures for determining whether or not an Xbox console has been modified, for creating a forensic duplicate, and for conducting a forensic investigation. Given the growing popularity of Xbox systems, it is important to understand how to identify, image and examine these devices while reducing the potential of corrupting the media (Burke & Craiger 2007: 269).

> File system journals contain valuable evidence pertaining to cases ranging from child pornography and software piracy to financial fraud and network intrusions. Digital forensic investigators should be aware of the data cached in file system journals and its use in digital investigations. Meanwhile, the digital forensics research community should focus its efforts on file system journal forensics and develop novel journal data extraction and analysis techniques that could be implemented in the next generation of computer forensic tools (Swenson, Phillips & Shenoi 2007: 243).

Increasingly, forensic analysis of computers for law enforcement purposes is being undertaken by well-organised groups of computer forensic examiners working in government facilities or private-sector workplaces, such as leading consulting practices. Only specially trained and authorised computer forensic examiners should process and examine electronic evidence, as evidence not retrieved by a computer forensic expert may result in the reliability of the evidence itself being called into question and potentially be ruled inadmissible in court.

> Delayed examinations produce other, harsher consequences. Imagine a scenario in which the computer examiner discovers a folder in the file structure of a suspect's hard drive containing homemade pornographic images of the suspect molesting a pre-teen girl. Further, imagine that this examination takes place one year after the computer's seizure during the execution of a search warrant at a suspect's residence. Finally, imagine that the images are of a neighbour and

that there was insufficient evidence to establish probable cause for the suspect's arrest before examining the hard drive. In this scenario, on-scene computer forensic examinations could have prevented the victim from being at risk for an additional year (Cohen 2007: unpaginated).

To ensure that the results of computer forensic examinations can be used in judicial proceedings, accreditation of individual examiners and validation of computer forensic analysis tools are desirable.

The importance of computer forensic evidence being called into question in judicial proceedings and the need to carry out forensic examinations of seized electronic storage devices (e.g. hard drives) carefully is demonstrated in the case of *Peach v Bird* 159 A Crim R 416 (2006) NTSC 14 (21 February 2006). In that case, the defendant had been acquitted of charges of possessing child pornography images. An appeal under s 163(3) of the *Justices Act 1928* (NT) was lodged. Although no images of child pornography were able to be recovered from the hard drive, the forensic examiner, using EnCase© software found various incriminating file names as well as evidence that the hard drive had been erased and overwritten in an attempt to remove evidence. The forensic examiner reported that:

> [T]he hard drive of the computer contained a word document named 'untitled document.wps' ('the untitled word document'). The document was found in the computer folder, C:\\My Documents. The word document contained a number of links to or addresses of websites, including the link, 'http:// mx.photos.yahoo.com/ pishanito2002' (the pishanito website). The hard drive of the computer also contained a directory of 70 images and one temporary storage file of a word document that had been stored in the C:\\My Documents\\My Pictures folder of the computer. The 70 images and the one word document contained in the directory had been overwritten or erased with the use of eraser programs on the computer. This meant that the 71 files could no longer be recovered. All that could be seen was the name of each file that had been saved to the C:\\My Documents\\My Pictures folder of the hard drive; the date that each file was created and the date that each file was overwritten or erased. Unlike a file which has been merely deleted, a file which has been overwritten or erased cannot be recovered. The erasing programs on the computer had been run on the files/images rather than the whole of the folder including the directory of file names of the 70 images and one word document. One of the files of the 70 erased images in the directory was named 8087053lg0.jpg. A jpg file is an image or picture file as opposed to a text file. The file named 8087053lg0.jpg was created on 17 March 2003 and overwritten or erased on 18 March 2003 (*Peach v Bird* 159 A Crim R 416 [2006] NTSC 14 (21 February 2006)).

Based on this evidence, the acquittal was set aside and a retrial ordered. On 28 August 2006, an appeal was also dismissed.

Therefore, to develop an effective response to online exploitation cases, strategic alliances among law enforcement agencies with other professionals and the community need to be established.

> Child sexual abuse, in all its forms, is an enormously complex social problem that demands a high level of professional competence and co-operation between a number of professional groups. These include: police officers, social workers, psychologists, probation officers, lawyers, doctors, hotline staff etc. This inter-agency co-operation has been highlighted as being of great importance in cases of child abuse. It is only recently that professionals have been trained in this complex new area of child protection (Jones & Skogrand 2005: 24).

The Indiana State Police, for example, established a partnership with the Department of Computer and Information Technology at Purdue University and the National White Collar Crime Center that allows knowledge sharing:

- the National White Collar Crime Center provides police training and networking in matters related to financial crime and, as part of this partnership, produces tailored training opportunities relevant to computer forensics and cybercrime investigations
- Indiana State Police provides subject matter experts with real-world experience and an ideal environment to beta test the newly developed courses

- Purdue University provides an academic perspective and credibility to the curriculum and in return, their students have access to practitioners working in this specialised field (Cohen 2007).

The Internet Crimes Against Children Task Force program (http://ojjdp.ncjrs.gov/Programs/ProgSummary.asp?pi=3&ti=1&si=1&kw=&strItem=&strSingleItem=&p=topic&PreviousPage=SearchResults#Resources), funded under Title IV of the Juvenile Justice and Delinquency Prevention Act of 1974 (as amended), provides law enforcement and other professionals with the necessary skills to develop an effective response to online exploitation cases nation-wide.

> While most cases involving possession of child pornography begin at state or local level, these agencies frequently look to federal agencies and ICAC (Internet Crimes Against Children) Task Forces for assistance and support. The majority of cases involve more than one law-enforcement agency, with around half of all cases involving assistance from federal agencies (Wolak, Finkelhor & Mitchell 2005). As in the UK, the need for cooperation across multiple agencies and jurisdictions at local, state and federal levels heightens the need for staff to be specially trained on an ongoing basis (Jewkes & Andrews 2007: 70).

As of December 2007, there are 46 regional Internet Crimes Against Children Task Force agencies funded by the US Office of Juvenile Justice and Delinquency Prevention (http://www.icactraining.org/). The Internet Crimes Against Children Training and Technical Assistance Program, in cooperation with Fox Valley Technical College, provides US law enforcement agencies with various training and technical programs and assistance in support of their Internet Crimes Against Children initiatives (Table 26).

**Table 26** Internet Crimes Against Children Task Force training and technical programs

| Program | Content of program |
|---|---|
| ICAC Investigative Techniques Training Program (ICAC-IT) | Designed to provide course participants with a basic understanding of investigative techniques in the area of internet crimes against children |
| ICAC Undercover Chat Investigations Training Program (ICAC-UC) | Designed for experienced ICAC investigators to provide them with the latest tools and techniques necessary to combat online child exploitation |
| ICAC Child Sex Offender Accountability Training Program (ICAC-CSO) | Designed for law enforcement investigators, probation/parole officers and prosecutors responsible for monitoring or investigating the activities of convicted child sexual offenders |
| ICAC Trial Advocacy for Prosecutors Training Program (ICAC-TAP) | A trial advocacy course for experienced prosecutors to examine the distinct phases of a trial and the relevant issues, challenges, tactics, strategies, and the law that enhance the skills and knowledge of prosecutors in these cases. Topics in this course include training on the authentication of technical evidence, how to prepare and organise the case, the selection of jurors, motions practice in computer cases involving crimes against children, the presentation of expert and fact testimony, cross-examination of defendants and their experts as well as how to conduct effective opening statements and closing arguments, among other topics in trial advocacy in such cases |
| ICAC Unit Supervisor Training Program (ICAC-US) | Designed for ICAC unit commanders and supervisors of ICAC Task Force and affiliated law enforcement agencies to provide course participants with an overview of managerial, investigative and early intervention strategies to more effectively protect children in their area of responsibility |
| CyberTips Management Training Program | Designed to provide course participants with the necessary skills to use the CyberTips software application developed for use with the National Center for Missing and Exploited Children Virtual Private Network |
| Peer Precision Training Program | Designed to provide course participants with the necessary skills to investigate the use of the peer-to-peer (P2P) file sharing networks using advanced technology developed as a result of previous peer-to-peer investigations |
| Project Safe Childhood Team Training | Designed to increase the level of investigative collaboration and cooperation among federal, state and local law enforcement agencies and federal prosecutors |

Source: Adapted from http://www.icactraining.org/

These public–private partnerships aim to equip law enforcement agencies with necessary skills to handle electronic evidence in their investigation of online child exploitation matters. Continuation of funding and resources dedicated to these initiatives needs to be undertaken by governments and organisations, as sexual exploitation of children over the internet is not likely to disappear any time soon.

## 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 (e.g. social networking sites) 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. However, some countries have sought to address this educational need.

> [Singapore's] Media Development Authority plans to organise programmes to introduce parents to the wonderful world of Facebook, Twitter, IM, MySpace, Second Life and MMORPGs (massively-multiplayer online role-playing games). Unfortunately, there will be new online fads next year. Keeping up with the latest cyber-trends isn't easy because things change so rapidly and parents have so little free time. And frankly, simply knowing about Facebook, Twitter or Friendster isn't enough. Parents need to monitor what is being said and done online, and with whom. Nothing looks more innocent than children typing away on a computer. Without looking at the screen, you have no idea if they are beavering away at their homework, complaining to their friends about their controlling father, or planning an illicit meeting with someone unsuitable (Yap 2007: unpaginated).

This serves as a reminder to parents that even by closely monitoring what their children are doing online may not be sufficient to prevent some kinds of exploitation from occurring, especially if parents have limited ICT skills. The 2005 Parents' Internet Monitoring Study, for example, conducted a national telephone survey of 503 parents of children aged between 13 and 17 years who had internet access at home (Ketchum Global Research Network 2005). The study found that 51 percent of respondents either did not have, or did not know if they had, software on their computer(s) that monitors where their child goes online and with whom they interact. A surprising 57 percent or more of respondents were reportedly unable to correctly decipher the meanings of several common internet acronyms (Table 1).

In a Finland-based survey directed at children aged between seven and 15 years, 17,848 children answered an online questionnaire available on the Habbo Hotelli, IRC-Galleria, Il2.org, Kavereita.net, Sooda and Suomi24 websites in September 2006 (Pelastakaa Lapset ry 2006). The study found that 97.9 percent of respondents had a mobile phone, 47.4 percent of respondents reported using mobile phones for accessing the internet and 28 percent of respondents said they sent photos (taken using the mobile phones) to the internet. Despite the increasing popularity of mobile phones with the respondents, nearly 27 percent of respondents reported they had never discussed their mobile phone usage with their parents, and 35 percent reported that their parents had no idea or that they did not know if their parents knew what they did with their mobile phones.

In the Ireland-based Survey of Children's Use of the Internet in 2006, 55 percent of the 848 student respondents aged between nine and 16 years indicated that they used the internet at home at least once a week (Webwise 2006):

- more than 50 percent indicated that their parents spoke with them very rarely or not at all about what they did on the internet
- 57 percent reported that their parents never check to see which sites they have visited
- 30 percent reported their mother knew nothing or very little about the internet
- 24 percent reported their father knew nothing or very little about the internet.

The finding from the US-based study carried out by Pew Internet and American Life Project, however, suggested that of the 935 parents with children aged between 12 and 17 years interviewed, 65 percent reported that they checked the websites visited by their child and 74 percent could correctly identify whether or not their child had ever created their own social networking site profile that others could see (Macgill 2007).

The Media and Communications in Australian Families 2007 study, commissioned by the Australian Communications and Media Authority, reported similar findings. Of the 751 Australian households with children aged between eight and 17 years surveyed:

- 57 percent of the parents interviewed reported having rules, understandings and arrangements about duration of internet use by their child
- 48 percent of the parents interviewed reported having rules, understandings and arrangements about limiting or restricting what their child accesses or looks at on the internet
- 81 percent of the parents interviewed reported checking that certain websites or online activities are deemed suitable for their child occasionally, 30 percent most of the time and 32 percent all of the time
- 82 percent of the parents interviewed reported keeping an eye on the computer screen when their child is using the internet occasionally, 36 percent most of the time and 20 percent all of the time
- 97 percent of the parents interviewed reported that they use the internet and are comfortable using the internet, 35 percent are fairly comfortable and 53 percent very comfortable (ACMA 2007a).

The contradictions in findings between these studies could perhaps be due to recruitment biases in terms of non-equivalence of respondents' socioeconomic status. Despite these differences, these studies indicated that children are generally subject, to some degree, to family rules that limit the frequency and their connection time. The studies also emphasised the need for parents to 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.

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 (e.g. 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.

Besides focusing preventive strategies on children, parents should also be included in the educational programs.

> [R]esearch indicates that the most successful sex education programmes require the full participation and cooperation of all parents. Therefore, rather than focusing on the child at the exclusion of the parent, it is important to explore a number of ways in which bridges can be built between all of the interested parties (Cumper 2006: 105).

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. McDaniel noted that:

> the reactions of parents to their child's report of sexual abuse is a matter of much professional concern because parents are reported to have been less than supportive in many cases. Therefore, the education of parents is essential to a successful therapeutic program should abuse have occurred … We can break the cycle of child sexual abuse by creating an environment in which taboo subjects can be discussed openly and accurate information is readily available. Many adults believe that sexual abuse, especially when it involves family and friends, simply will never happen to their children. They might avoid the topic completely to focus on teaching their children general concepts of personal health and safety, especially the avoidance of strangers. This is reinforced by bookstores and libraries, which stock many books about strangers and very few books that specifically discuss child sexual abuse (McDaniel 2001: 2007).

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 encountered online out of a fear of having limits placed on their use of the internet or their mobile phones.

> Paradoxically, when adolescents encounter serious problems on Internet they conceal them from their parents, and it is only when really serious cases arise that they decide to take the step of telling them. They try to resolve the problems themselves, or they consult their peers. They always fear that facing any problem they might raise with their parents, the latter's reaction will be to deny them access to Internet, punish them in some way or inform the parents of the others (Garnacho & Garmendia 2007: 18).

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
- parents about taking a proactive approach in advising their child about online risks without resorting to threatening limiting 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. Websites such as the National Children's Home website on internet security (http://www.nch.org.uk/information/index.php?i=134) serve as a useful information booth for both children and their parents such as a checklist and internet glossary explaining the most frequently used terms (e.g. IRC rooms, blogs, social networking sites).

The community-based Stop It Now! programs (http://www.stopitnow.com/), for example, involve adults (including convicted sexual offenders), victims of sexual abuse, families and communities in their fight against online child exploitation. The programs operate a national toll-free Helpline, which provides adults with an outlet to confidentially voice their concerns such as their own or others' sexualised behaviour towards children. Law enforcement agencies should also work closely with such helplines in offering crime prevention advice. Stop It Now! programs also provide training to professionals who work with children (e.g. daycare providers, foster parents, teachers, clinicians, law enforcement and medical personnel) aiming to help adults to recognise and acknowledge harmful behaviours and offer resources to stop sexual abuse. Focus groups have also been conducted with communities from specified cultures to raise awareness among these groups.

The Cyber Café (http://thinkuknow.co.uk/8_10/cybercafe/), jointly created by Becta, the Department for Children, Schools and Families, the Internet Proficiency Group, GridClub and the Child Protection and Online Protection Centre (UK CEOP 2007d), is one of the recent additions to a list of educational programs designed to educate both parents and children about online dangers. On the Cyber Café 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.

Blogsafety (http://www.childnet-int.org/blogsafety/), launched by Childnet International, is another example of an educational initiative in which parents,

An important part of ensuring the vigilance of both children and parents will be to teach them how they can help prevent such crimes.

educators, industry, children and young people can obtain advice on online safety. The website provides information for:

- parents – terminologies such as blogs and MySpace are explained and the site also allows parents to join a unique forum on Blogsafety by following the link on the site
- educators – the risks and safety issues associated with such online activities are explained, and the need to integrate such issues into the curriculum is also emphasised
- children and young people – advice on how to use blogging sites safely and responsibly
- industry – emphasises the need for privacy settings in the private–public environment, the need to provide relevant safety risks and issues to users, the need to provide effective safety tools to users and the need to protect users' privacy.

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.

# 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. The use of social networking sites is, and will continue to remain, popular with the digital and virtual generations. Children and young people will continue to communicate in ways unfamiliar to adults such as through the use of acronyms and non-linguistic signs in virtual venues. This makes the task of regulation all the more difficult for technologically limited guardians of the internet.

Serious concerns have been expressed about the ways in which new technologies might be exploited for online child grooming and this report provides some indications of the ways in which emerging technological changes may be exploited to facilitate and commit online child grooming. Key risk areas include the use of anonymising protocols (e.g. the Onion Router), password authentication techniques, encryption techniques and steganographic techniques.

Ways in which child sexual offenders can exploit the internet include trafficking child pornography, locating children for the purpose of sexual abuse, engaging in inappropriate sexual communications with children, communicating with other like-minded individuals, locating child-sex tourism operators, making direct contact with child prostitutes and mail ordering children for the purpose of sexual contacts. Another emerging risk relating to online child exploitation is virtual 'rape' of minors perpetrated in online games or virtual worlds. This can potentially cause as real psychological, social and financial harms to individuals as currently occurs in the offline world. Studies have also highlighted the ease with which personal information of children can be obtained online by sexual offenders and fraudsters alike. The need to amend and strengthen the law to address the challenges that new technologies pose will become more pronounced with the rapid advancement and convergence of ICT in the years to come.

Victims of online child exploitation come from all walks of life. The detrimental impact and the potentially long-term effects of living with the consequences of sexual abuse are exacerbated if pornography is involved. Some victims, if left untreated, may become perpetrators of online child grooming in their adulthood. Offenders are a diverse group that include trusted professionals such as lawyers, teachers, police officers, judges and prosecutors. In some cases, offenders are family members or acquaintances who knew their child victims in real life.

Although the actual extent of children being targeted online for sexual purposes can never be accurately

determined, the dangers of online child exploitation have received widespread attention. Online child grooming offences have been introduced in a range of countries including Australia, Canada, Singapore, the United States and the United Kingdom. Internet filtering regimes have also been introduced in several countries to restrict access to potentially objectionable materials online.

It can reasonably be anticipated that online child grooming prosecutions involving multiple jurisdictions will continue to arise in the years ahead along with an increasing demand for new strategies in terms of how law enforcement agencies investigate, prosecute and prevent online multijurisdictional child grooming crimes across state and national borders.

> The roadblocks to many types of international investigations – lack of resources to deal with language barriers and cumbersome bureaucracy – are especially damaging to child pornography investigations, where speed is crucial (Specht 2006: unpaginated).

It will be necessary for the international community to address urgently problems of multiple jurisdictions and for more countries to introduce legislation that criminalises online child exploitation. Issues relating to extradition are also likely to arise and there will continue to be demands placed on Australian law enforcement to work collaboratively with overseas law enforcement agencies in identifying and investigating online child exploitation cases suitable for extradition.

A multidimensional response to combat online child grooming is likely to offer the greatest benefits. This 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. Such partnerships will result in commercial opportunities and perhaps more effective policing avenues for the private sector.

## Future research

Davidson (2007) and other researchers suggested that international law enforcement agencies and academia should, perhaps, consider sharing practices and research information and establishing an information repository for research purposes. This would enable law enforcement agencies and researchers to have better data on child grooming to analyse trends and characteristics. The European Commission Safer Internet and Online Technologies for Children Program summary report also identified the need to have 'more data on types of child abuse incidents, methods and rates, to address the current knowledge gaps' (European Commission Information Society and Media Directorate-General 2007: 37).

The studies noted at the beginning of this report were typically restricted to a particular community or country and the findings rarely compared across different jurisdictions. It is, therefore, difficult to determine whether it is possible to generalise these findings to the international community. The lack of research in the area of online child grooming is also highlighted in the recent EU Kids Online study co-funded by the European Commission Safer Internet Plus Programme. Out of the 235 recent and ongoing empirical studies regarding children, the internet and online technologies in 18 or more countries across Europe identified in the study, it was found that:

- research on content risks (including sexually harmful content such as pornographic materials) and contact risks (including sexually harmful behaviour such as online child grooming) is lacking in some countries, and requires updating and deepening in most or all of the 18 or more countries across Europe
- there is relatively little research on how children 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

- research on the role of parents and teachers in mediating children's internet use is lacking in a number of countries across Europe, particularly research on the effectiveness of parental mediation (Livingstone & Haddon 2007).

## *Studies of victims*

Mitchell, Becker-Blease and Finkelhor (2005: 502) noted that from a victim's perspective, issues can also 'be somewhat different from the classic sexual assault trauma paradigm'. Further studies are necessary to develop insight into the online child grooming offending cycle and to investigate whether victims of online child grooming will eventually progress to become perpetrators of online child grooming in their adulthood. There is some evidence that a history of childhood sexual abuse is one of the many factors associated with sexual offending in adulthood.

The European Commission Safer Internet and Online Technologies for Children Program summary report also identified the need for longitudinal research studies in the following areas:

- the psychosocial impact on children of online situations and how children react to online predators
- who are the vulnerable groups of children and how to support them
- the relationship between the quality of parenting and grooming, and the link between depression and grooming in both the victims and the abuser
- offenders and their grooming behaviour including typology and profiling of online sexual offenders (European Commission Information Society and Media Directorate-General 2007).

## *Internet sex offender treatment programs*

In the various studies cited above, internet offenders are often categorised together with contact child sexual abusers for the purposes of psychological assessment and treatment. Studies of this nature, as pointed out by Middleton et al. (2006), tend to assume that theories of child sexual abuse are 'effective in explaining the behaviour of individuals who access, distribute and create child pornography' when in fact, more studies are required to establish whether '[i]nternet offenders are a separate manifestation within the psychological spectrum of sexual offending or if they share similar profiles to previous typologies' (Middleton et al. 2006: 591). Jewkes and Andrews (2007: 67) have also questioned 'whether people who download child pornography share the same characteristics and behaviours as contact offenders'.

As pointed out by Polizzi, MacKenzie and Hickman 1999 (cited in Howells et al. 2004: 54), 'broad generalisations regarding the efficacy of sex offender treatment programs cannot easily be made due to the lack of homogeneity in the offender group'. Sex offender re-entry into the community programs, for example, seldom distinguish between contact sexual offenders and internet sexual offenders. By way of example, Box 3 is a snapshot of the sex offender re-entry program in Vermont, United States.

As Talbot et al. (2002: 4) suggested, 'no two jurisdictions can or should manage sex offenders in exactly the same manner; local practices must take into account the nature of the local population of sex offenders as well as the resources available to respond to sex offending behaviour'. The same should be said of contact sexual offenders and internet sexual offenders. Traditional supervision practices such as periodic phone contact are unlikely to be effective in today's information age against sexual offenders who exploit cyberspace in their criminal conduct. More coordinated studies would have to be undertaken to understand whether internet sexual offenders will benefit from the same treatment programs as contact sexual offenders.

> [A]lthough some Internet offenders display psychological deficits similar to those of contact sex offenders almost half of this sample did not display any deficits. Consequently, the assumption that Internet offenders will benefit from the same treatment programs as contact sex offenders may need to be reassessed (Middleton et al. 2006: 601).

Quayle and Taylor (2003) also suggested that advances in ICT may be a contributing factor in increased risk-taking behaviour of sexual offenders. For example, there have been suggestions that access to sexually explicit or pornographic magazines, websites and IRC rooms can potentially

**Box 3** The Vermont Treatment Program for Sexual Abusers

The Vermont Treatment Program for Sexual Abusers is often cited as the first to formalise a collaborative and integrated system of in-prison and community-based treatment and supervision for sexual offenders.

Treatment services within the prison include an intensive program for higher-risk offenders, a moderate-intensity program for moderate-risk offenders, and a short-term program for those who are assessed to be at low risk. In the community, 11 sites throughout the state provide varied levels of treatment for sexual offenders released from prison. To ensure consistency and quality, the prison and community-based programs share a common philosophy and approach, and fall under a single coordinated program.

Upon admission to prison, validated assessment tools – the Vermont Assessment of Sex Offender Risk, Rapid Risk Assessment of Sex Offender Recidivism, Static-99, Sex Offender Treatment Needs and Progress Scale, and Level of Service Inventory-revised – are used to identify risk and needs and to triage offenders into programming levels. Although treatment for incarcerated sexual offenders is not mandatory, parole decisions are contingent on program participation.

At least 90 days prior to release from prison, sexual offenders are assigned to a parole officer who meets with the institutional treatment team and offender to begin transition and release planning. They address issues such as housing, employment and community support networks, and identify a community treatment provider prior to release. If the offender has no post-release support, correctional and treatment staff work to develop a team on the offender's behalf, composed of trained volunteers who are recruited and trained explicitly for this purpose.

With respect to community supervision, specially trained officers balance surveillance and monitoring functions with strategies designed to assist offenders with developing a positive, goal-directed lifestyle.

Collaboration among treatment providers, supervision officers, polygraph examiners, and community support networks is the key to the program's ongoing success – multidisciplinary teams meet monthly to coordinate management of these cases.

Source: Bumby, Talbot and Carter (2007)

'undermine the treatment process by exacerbating attitudes supportive of victimization and fuelling deviant fantasies and sexual preoccupations for some offenders' (Bumby, Talbot & Carter 2007: 6).

Future research efforts should also include more population-based studies to better understand the role that ICT may play in online child grooming behaviour.

> Further research is needed to explore the behaviour of online groomers who target children; the link/boundary between non-contact online sexual abuse of children; and internet offender's propensity for contact abuse. Research is also needed to investigate the behaviour and motivations of those using 'extreme sexual pornographic images' depicting adults (Davidson 2007: 12).

One such initiative to better understand how video games and the internet could affect children and young people is the Byron Review. The Byron Review is supported by officials from the UK Department for Children, Schools and Families and the Department for Culture, Media and Sport and will be exploring ways in which government, businesses and families can work together to ensure children and young people can stay safe when using these new technologies (http://www.dfes.gov.uk/consultations/conDetails.cfm?consultationId=1511).

# References


All URLs were correct at 17 April 2008

Abd Rahman Z 2007. 11 sites shut down by MCMC. *The star.com* 22 October. http://star-techcentral.com/tech/story.asp?file=/2007/10/22/technology/20071022143857&sec=technology

Adam A 2002. Cyberstalking and internet pornography: gender and the gaze. *Ethics and information technology* 4(2): 133–142

Albanese J 2007. *Commercial sexual exploitation of children: what do we know and what do we do about it?* Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice. http://www.ojp.usdoj.gov/nij/pubs-sum/215733.htm

Allam H 2007. Middle east seeks to limit web access. *Miamiherald.com* 26 December. http://facthai.wordpress.com/2007/12/26/middle-east-seeks-to-limit-web-access-miami-herald/

Allbon E & Williams P 2002. Nasties in the net: children and censorship on the web. *New library world* 103(1): 30–38

American Psychiatric Association 1994. *Diagnostic and statistical manual of mental disorders*, 4th ed. Washington, DC: American Psychiatric Association

Armagh DS & Battaglia NL 2006. *Use of computers in the sexual exploitation of children*, 2nd ed. Washington, DC: US Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention

Association of Banks in Singapore 2007. Singapore banks join global battle against child pornography. *Media release* 17 January. http://www.abs.org.sg/pdf_files/Final%20Media%20Release%20on%20Singapore%20Banks'%20Battle%20Against%20Child%20Pornography.pdf

Attorney-General's Department (AGD) n.d. Extradition and mutual assistance relationships with other countries. *Fact sheet* 10. Canberra: AGD. http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~Fact+Sheet+~+Extradition+and+Mutual+Assistance+relationships+with+other+countries220207.pdf/$file/Fact+Sheet+~+Extradition+and+Mutual+Assistance+relationships+with+other+countries220207.pdf

Australian Associated Press (AAP) 2007a. Ex-cop jailed over internet sex lure. *News.com.au* 21 November. http://www.news.com.au/story/0,23599,22796771-17001,00.html?from=public_rss

Australian Associated Press (AAP) 2007b. Man acquitted of online sex charges. *News.com.au* 21 May. http://www.news.com.au/story/0,23599,21769226-1248,00.html?from=public_rssc

Australian Associated Press (AAP) 2007c. Child pornography arrests now number 31. *News.com.au* 20 December. http://www.news.com.au/story/0,23599,22952920-2,00.html

Australian Associated Press (AAP) 2007d. Selim cleared over destruction of data. *smh.com.au* 19 April. http://www.smh.com.au/news/national/selim-cleared-over-destruction-of-data/2007/04/18/1176696916796.html#

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

Australian Communications and Media Authority (ACMA) 2007b. New rules for age-restricted internet and mobile content. *Media release* 21 December. http://www.acma.gov.au/WEB/STANDARD/pc=PC_310907

Australian Federal Police (AFP) 2007. Operation Irenic: 24 Australians arrested for child pornography offences. *Media release* 20 December

Australian Institute of Criminology (AIC) 2005. Child exploitation. *High tech crime brief* 2. Canberra: AIC. http://www.aic.gov.au/publications/htcb/htcb002.html

Aytes KE, Olsen SS, Zakrajsek T, Murray P & Ireson R 2001. Cognitive/behavioral treatment for sexual offenders: an examination of recidivism. *Sexual abuse* 13(4): 223–231

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

Berliner L 2002. Introduction: confronting an uncomfortable reality. *American professional society on the abuse of children advisor* 14(2): 2–3

Bertino E, Ferrari E & Perego A 2003. Content-based filtering of web documents: the MaX system and the EUFORBIA project. *International journal of information security* 2(1): 45–58

Blue Coat 2007. *Blue Coat K9 web protection user guide*. http://www1.k9webprotection.com/support/files/K9Manual.pdf

Box D 2007. Pedophiles using abstract symbols to talk. *News.com.au* 29 December. http://www.news.com.au/story/0,23599,22982629-2,00.html

Brenner SW 2001. Is there such a thing as 'virtual crime'? *California criminal law review* 4(1). http://boalt.org/CCLR/v4/v4brenner.htm

Bright M 2004. BT puts block on child porn sites. *The observer* 6 June. http://observer.guardian.co.uk/uk_news/story/0,6903,1232422,00.html

British Telecom 2007. *BT's response to the consultation on Safer Internet and On-line Technologies for Children*. http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_prog/results/bt_a429892.pdf

Bumby K, Talbot T & Carter M 2007. *Managing the challenges of sex offender reentry*. Silver Spring, MD: United States Center for Sex Offender Management

Buttler M 2007. Malvern man among seven arrested in child porn bust. *Herald sun* 17 December. http://www.news.com.au/heraldsun/story/0,21985,22933704-2862,00.html?from=public_rss

Burke P & Craiger P 2007. Forensic analysis of xBox consoles. *IFIP international federation for information processing* 242: 269–280

Camtepe SA, Krishnamoorthy MS & Yener B 2004. A tool for internet chatroom surveillance, in Hsinchun C, Moore R, Zeng DD & Leavitt J (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

Chau M & Xu J 2007. Mining communities and their relationships in blogs: a study of online hate groups. *International journal of human-computer studies* 65(1): 57–70

China tops 20m bloggers 2007. *Australian IT* 12 January. http://australianit.news.com.au/articles/0,7204,21047806%5E15322%5E%5Enbv%5E15306,00.html

Chinese Human Rights Defenders 2007. *China: journey to the heart of internet censorship*. http://www.rsf.org/IMG/pdf/Voyage_au_coeur_de_la_censure_GB.pdf

Choo KKR & Smith RG 2008. Criminal exploitation of online systems by organised crime groups. *Asian journal of criminology*. http://www.springerlink.com/content/l437117571870577/

Choo KKR, 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/rpp/78/

Clayton R 2005. Failures in a hybrid content blocking system, in Danezis G & Martin D (eds), *Proceedings of the 5th international workshop on privacy enhancing technologies*, Cavtat, Croatia, 30 May – 1 June 2005, Springer, Lecture notes in computer science 3856: 78–92

Clayton R, Murdoch SJ & Watson RNM 2006. Ignoring the great firewall of China, in Danezis G & Golle P (eds), *Proceedings of the 6th international workshop on privacy enhancing technologies*, Cambridge, UK, 28–30 June, Springer, Lecture notes in computer science 4258: 20–35

Coen C 2006. Keep kids safe online. *Acadiana parent* October: 12–13

Cohen CL 2007. Growing challenge of computer forensics. *The police chief* 74(3). http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1136&issue_id=32007

Commonwealth Director of Public Prosecutions 2006. *2005–2006 annual report*. Canberra: Commonwealth Director of Public Prosecutions. http://www.cdpp.gov.au/AboutUs/AnnualReports/

Cordonnier V 2006. Cybersex and addiction: is therapy possible? *Sexologies* 15(3): 202–209

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No 201). Strasbourg: Council of Europe. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=1/29/2008&CL=ENG

Cox Communications 2007. *Teen Internet Safety Survey, Wave II*. http://www.cox.com/TakeCharge/includes/docs/survey_results_2007.ppt

Craissati J & McClurg G 1996. The challenge project: perpetrators of child sexual abuse in SE London. *Child abuse and neglect* 20(11): 1067–1077

Craissati J, McClurg G & Browne K 2002. Characteristics of perpetrators of child sexual abuse who have been sexually victimized as children. *Sexual abuse* 14(3): 225–239

Crandall JR, Zinn D, Byrd M, Barr E & East R 2007. ConceptDoppler: a weather tracker for internet censorship, in *Proceedings of the 14th ACM conference on computer and communications security CCS '07*. New York, NY: ACM Press: 352–365

Craven S, Brown S & Gilchrist E 2006. Sexual grooming of children: review of literature and theoretical considerations. *Journal of sexual aggression* 12(3): 287–299

Cumper P 2006. 'Let's talk about sex': balancing children's rights and parental responsibilities. *Legal studies* 26(1): 88–108

Dandurand Y, Colombo G & Passas N 2007. Measures and mechanisms to strengthen international cooperation among prosecution services. *Crime, law and social change* 47(4–5): 261–289

Daneback K, Cooper A & Månsson SA 2005. An internet study of cybersex participants. *Archives of sexual behavior* 34(3): 321–328

Davidson J 2007. *Current practice and research into internet sex offending*. Paisley, UK: Risk Management Authority

Dearne K & Foo F 2008a. Conroy wades into child porn net flood. *Australian IT* 8 January. http://www.australianit.news.com.au/story/0,24897,23021645-15306,00.html

Dearne K & Foo F 2008b. Rudd porn filter fails: experts. *Australian IT* 3 January. http://www.australianit.news.com.au/story/0,24897,23001130-15306,00.html

Deibert RJ 2002. Dark guests and great firewalls: the internet and Chinese security policy. *Journal of social issues* 58(1): 143–159

Denis S 2007. Do you know the lingo? *Gazette magazine* 62(2). http://www.rcmp-grc.gc.ca/gazette/vol69no2/lingo_e.htm

eMarketer 2007. The promise of social network advertising. *Media release* 14 December. http://www.emarketer.com/Article.aspx?id=1005688

Egan V, Kavanagh B & Blair M 2005. Sexual offenders against children: the influence of personality and obsessionality on cognitive distortions. *Sexual abuse* 17(3): 223–240

Ellison C 2000. Oppression net. *Economic affairs* 20(1): 21–28

European Commission Information Society and Media 2007a. Making the internet a safer place. *General fact sheet* 18. Brussels: European Commission Information Society and Media. http://ec.europa.eu/information_society/doc/factsheets/018-saferinternetplus.pdf

European Commission Information Society and Media 2007b. *Safer Internet Plus: a multi-annual community programme on promoting safer use of the internet and new online technologies*. Brussels: European Commission Information Society and Media. http://ec.europa.eu/information_society/activities/sip/docs/call_2007/sip_work_programme_2007.pdf

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. http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_prog/summary_report.pdf

European Parliament and the Council of the European Union 2005. Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual community programme on promoting safer use of the internet and new online technologies. *Official journal of the European Union* L149/1: 1–3. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_149/l_14920050611en00010013.pdf

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

Federal Bureau of Investigation (FBI) n.d. *Investigative programs: critical incident response group*. Washington, DC: FBI. http://www.fbi.gov/hq/isd/cirg/ncavc.htm

Federal Bureau of Investigation (FBI) 2006. *Innocent Images National Initiative*. Washington, DC: FBI. http://www.fbi.gov/publications/innocent.htm

Ferraro MM & Russell A 2004. Current issues confronting well-established computer-assisted child exploitation and computer crime task forces. *Digital investigation* 1(1): 7–15

Fewster S 2007. Man guilty of luring boys. *The advertiser* 28 November. http://www.news.com.au/adelaidenow/story/0,22606,22836272-2682,00.html?from=public_rss

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

Finkelhor D 1994. The international epidemiology of child sexual abuse. *Child abuse and neglect* 18(5): 409–417

Finkelhor D & Ormrod R 2004. Child pornography: patterns from NIBRS. *Juvenile justice bulletin* December. Washington, DC: Office of Juvenile Justice and Delinquency Prevention. http://www.ncjrs.gov/pdffiles1/ojjdp/204911.pdf

Forte M, de Souza WL & do Prado AF 2006. A content classification and filtering server for the internet, in *Proceedings of the 2006 ACM symposium on applied computing*. New York, NY: ACM Press: 1166–1171

Fulda JS 2007. Internet stings directed at pedophiles: a study in philosophy and law. *Sexuality and culture* 11(1): 52–98

Garnacho CG & Garmendia M 2007. *How young people use the internet: habits, risks and parental control*. n.p.: EUKids on Line. http://www.lse.ac.uk/collections/EUKidsOnline/SpanishReport2007English.pdf

Gee DG, Devilly GJ & Ward T 2004. The content of sexual fantasies for sexual offenders. *Sexual abuse* 16(4): 315–331

Gorman GE 2005. China-bashing in the internet censorship wars. *Online information review* 29(5): 453–456

Grabosky P 2007. Requirements of prosecution services to deal with cyber crime. *Crime, law and social change* 47(4–5): 201–223

Grabosky PN & Smith RG 1998. *Crime in the digital age: controlling telecommunications and cyberspace illegalities*. New Brunswick, NJ: Transaction Publishers/Federation Press

Green R 2002. Is pedophilia a mental disorder? *Archives of sexual behavior* 31(6): 467–471

Griffith S 2007. Keep kids e-safe: a community effort in Sugar Land, Texas. *The police chief* 74(4). http://www.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.

Grimes SM 2006. Online multiplayer games: a virtual space for intellectual property debates? *New media and society* 8(6): 969–990

Grunwald Associates LLC 2007. *Creating and connecting: research and guidelines on online social and educational networking*. Bethesda, MD: Grunwald Associates LLC

Hagan K 2007. Judge rebuked by irate lawyer over sex views. *The age* 24 November. http://www.theage.com.au/news/national/judge-rebuked-by-irate-lawyer-over-sex-views/2007/11/23/1195753307239.html

Hagenbuch S 2006. Child pornography subject of house and senate committee hearings. *The source on women's issues in congress* 11(26). http://www.womenspolicy.org/site/News2?news_iv_ctrl=-1&page=NewsArticle&id=6791

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

Havenstein H 2007a. Forget generations X and Y: here comes generation V. *Computerworld* 15 November. http://www.computerworld.com.au/index.php?id=962598741&eid=-255

Havenstein H 2007b. Facebook users look to get disabled accounts reactivated. *Computerworld* 17 December. http://www.computerworld.com.au/index.php?id=2034964649&eid=-180

Hepp R 2007. Tightening online restraints on convicted sex offenders. *The star-ledger* 28 December.

Heywood L 2007. Onus on providers to clean up web content. *News.com.au* 31 December. http://www.news.com.au/story/0,23599,22989028-421,00.html

Hilley S 2007. Trojan horse powers for the police. *Digital investigation* 4(2): 56–58

Hinchcliffe D 2006. Enterprise 2.0: ten predictions for 2007. *ZDNet* 27 December. http://blogs.zdnet.com/Hinchcliffe/?p=76

Hindujaa S & Patchin JW forthcoming. Personal information of adolescents on the internet: a quantitative content analysis of MySpace. *Journal of adolescence*

House of Assembly Hansard 2005. Criminal Code Amendment (Child Exploitation) Bill 2005 (No. 37): Second reading. 14 June. http://www.parliament.tas.gov.au/VPHouse/isysquery/623db782-21ab-4372-a35f-899673fc10b6/1/doc/

Howells K, Watt B, Hall G & Baldwin S 2004. *Correctional offender rehabilitation programs: the national picture in Australia*. Canberra: Criminology Research Council

International Centre for Missing and Exploited Children (ICMEC) 2006. *Child pornography: model legislation and global review*. Alexandria, VA: ICMEC. http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf

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

Internet Watch Foundation (IWF) 2007. IWF response to the government consultation on the possession of non-photographic visual depictions. n.p.: IWF. *Consultation response* 19 June. http://www.iwf.org.uk/public/page.113.442.htm

Jewkes Y & Andrews C 2007. Internet child pornography: international responses, in Jewkes Y (ed.), *Crime online*. Cullompton: Willan: 60–80

Jones KC 2007. New Jersey bars some sex offenders from internet. *Informationweek* 28 December. http://www.informationweek.com/news/showArticle.jhtml?articleID=205204285

Jones V & Skogrand E 2005. *Position paper regarding online images of sexual abuse and other internet-related sexual exploitation of children*. Copenhagen and Oslo: Save the Children Europe Group. http://www.savethechildren.net/alliance/get_involved/report/position_internet_abuse.pdf

Kanable R 2007. Organizing child pornography evidence. *Law enforcement technology* August. http://www.officer.com/print/Law-Enforcement-Technology/Organizing-child-pornography-evidence/1$37938

Keizer G 2007. FBI planted spyware on teen's PC to trace bomb threats. *Computerworld* 20 July. http://www.computerworld.com.au/index.php?id=1156859833&eid=-255

Kerlikowske RG 2007. NetSmartz: a comprehensive approach to internet safety and awareness. *The police chief* 74(4). http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1157&issue_id=42007

Ketchum Global Research Network 2005. *Parents' internet monitoring study*. n.p.: Cox Communications; National Center for Missing & Exploited Children; NetSmartz. http://www.cox.com/takecharge/includes/docs/results.pdf

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

Kingston DA, Firestone P, Moulden HM & Bradford JM 2007. The utility of the diagnosis of pedophilia: a comparison of various classification procedures. *Archives of sexual behavior* 36(3): 423–436

Kirk J 2007. Facebook sues Canadian porn company over hacking. *Computerworld* 18 December. http://www.computerworld.com.au/index.php?id=1056262081&eid=-255

Klang M 2006. Virtual censorship: controlling the public sphere. *IFIP international federation for information processing* 223: 185–194

Klerks P 2001. The network paradigm applied to criminal organizations: theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. *Connections* 24(3): 53–65

Koschade S 2006. A social network analysis of Jemaah Islamiyah: the applications to counterterrorism and intelligence. *Studies in conflict and terrorism* 29(6): 559–575

Lamb ME & Brown DA 2006. Conversational apprentices: helping children become competent informants about their own experiences. *British journal of development psychology* 24(1): 215–234

Lang RA & Frenzel RR 1988. How sex offenders lure children. *Annals of sex research* 1(2): 303–317

Langbein S 2007. Hacker gets 110 years for threats on MySpace. *Orlando sentinel* 1 December

Langevin R, Lang RA & Curnoe S 1998. The prevalence of sex offenders with deviant fantasies. *Journal of interpersonal violence* 13(3): 315–327

Lanning KV 2002. Law enforcement perspective on the compliant child victim. *American professional society on the abuse of children advisor* 14(2): 4–9

Lenhart A & Madden M 2007. *Social networking websites and teens: an overview*. Washington, DC: Pew Internet and American Life Project. http://www.pewinternet.org/pdfs/PIP_SNS_Data_Memo_Jan_2007.pdf

Levenson JS, Brannon YN, Fortney T & Baker J 2007. Public perceptions about sex offenders and community protection policies. *Analyses of social issues and public policy* 7(1): 1–25

LexisNexis 2007. LexisNexis risk and information analytics group launches solution to help tackle national sex predator problem. *Media release* 11 April. http://risk.lexisnexis.com/Article.aspx?id=33

Leyden J 2007a. Germany floats Trojan for terror suspects. *The register.com* 3 September. http://www.theregister.co.uk/2007/09/03/german_trojan_plan/

Leyden J 2007b. Net censorship growing worldwide. *The register.com* 18 May. http://www.theregister.co.uk/2007/05/18/net_censorship/

Lim J 2007a. Teens playing rape games on net. *The electric new paper* 11 March.

Lim J 2007b. Shocked psychiatrist says: it's worse than porn. *The electric new paper* 11 March.

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

Losel F & Schmucker M 2005. The effectiveness of treatment for sexual offenders: a comprehensive meta-analysis. *Journal of experimental criminology* 1(1): 117–146

Lower G 2007. Call to jail ex-cop internet child sex predator. *The advertiser* 31 October. http://www.news.com.au/adelaidenow/story/0,22606,22678991-2682,00.html?from=public_rss

MacKinnon R 2008. Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public choice* 134(1–2): 31–46

Macgill AR 2007. *Parent and teenager internet use*. Washington, DC: Pew Internet and American Life Project. http://www.pewinternet.org/pdfs/PIP_Teen_Parents_data_memo_Oct2007.pdf

Marks P 2007. How to leak a secret and not get caught. *New scientist* 2586: 13

Marshall B & Chen H 2006. Using importance flooding to identify interesting networks of criminal activity, in Mehrotra S, Zeng DD, Hsinchun C, Thuraisingham BM & Wang F-Y (eds), *Proceedings of the IEEE international conference on intelligence and security informatics*, San Diego, CA, 23–24 May, Lecture notes in computer science 3975: 14–25

McAlinden AM 2006. Managing risk: from regulation to the reintegration of sexual offenders. *Criminology and criminal justice* 6(2): 197–218

McDaniel C 2001. Children's literature as prevention of child sexual abuse. *Children's literature in education* 32(3): 203–224

McMenamin B 2008. Filters needed to battle child porn. *Australian IT* 8 January. http://www.australianit.news.com.au/story/0,24897,23021828-15306,00.html

McNulty PJ 2007. Project safe childhood. *The police chief* 74(3). http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1138&issue_id=32007

Men refused bail over alleged child porn ring 2007. *ABC.net.au* 17 December. http://www.abc.net.au/news/stories/2007/12/17/2121104.htm

Microsoft 2004a. Global campaign against child pornography is launched by International Centre for Missing and Exploited Children. *Media release* 22 April. http://www.microsoft.com/presspass/press/2004/apr04/04-22icmecglobalpr.mspx

Microsoft 2004b. Purging the internet of child predators. *Media release* 22 April. http://www.microsoft.com/presspass/features/2004/apr04/04-22ICMEC.mspx

Middleton D, Elliott IA, Mandeville-Norden R & Beech AR 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

Mitchell K, Becker-Blease KA & Finkelhor D 2005. Inventory of problematic internet experiences encountered in clinical practice. *Professional psychology: research and practice* 36(5): 498–509

Mitchell K, Finkelhor D & Wolak J 2007. Online requests for sexual pictures from youth: risk factors and incident characteristics. *Journal of adolescent health* 41(2): 196–203

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

Müller VC 2006. Some information is too dangerous to be on the internet. *ACM SIGCAS computers and society* 36(1): 1–11

National Center for Missing and Exploited Children (NCMEC) 2006. *The child victim identification program*. Alexandria, VA: NCMEC. http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=2358

National Center for Missing and Exploited Children (NCMEC) 2007a. *2006 annual report*. Alexandria, VA: NCMEC. http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=845

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

National Center for Missing and Exploited Children (NCMEC) n.d. *What is online enticement of children for sexual acts*. Alexandria, VA: NCMEC. http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=1503

National Child Exploitation Coordination Centre (NCECC) 2007. International and multi-jurisdictional child sexual exploitation investigations standard practice for the NCECC. *Media release* 2 November. http://ncecc.ca/st_2007-11-02_e.htm

New Jersey Senate Democrats 2007. Full senate finalizes Codey Bill cracking down on internet predators. *Media release* 17 December. http://www.njsendems.com/release.asp?rid=1712

New South Wales Police 2007. Man charged with child grooming offences: child exploitation internet unit. *Media release* 28 March

Newman GR 2007. Sting operations. *Problem-oriented guides for police response guides series* no. 6. Washington, DC: US Department of Justice, Office of Community Oriented Policing Services

Nicholas S, Kershaw C & Walker A 2007. *Crime in England and Wales 2006/07*. London: Home Office. http://uk.sitestat.com/homeoffice/homeoffice/s?rds.hosb1107pdf&ns_type=pdf&ns_url=%5Bhttp://www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf%5D

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

Nijboer J 2004. Big Brother versus anonymity on the internet: implications for internet service providers, libraries and individuals since 9/11. *New library world* 105(1202/1203): 256–261

O'Connell R 2003. A typology of child cybersexploitation and online grooming practices. Paper to Netsafe conference 2003, Auckland, July: 16

O'Donohue W, Regev LG & Hagstrom A 2000. Problems with the DSM-IV diagnosis of pedophilia. *Sexual abuse: a journal of research and treatment* 12(2): 95–105

Olson LN, Daggs JL, Ellevold BL & Rogers TKK 2007. Entrapping the innocent: toward a theory of child sexual predators' luring communication. *Communication theory* 17(3): 231–251

Online porn merchants dodge internet dragnet 2007. *Reuters* 4 June. http://www.reuters.com/article/internetNews/idUSPEK31477620070605

Palczewski CH 2001. Contesting pornography: terministic catharsis and definitional argument. *Argumentation and advocacy* 38(1): 1–17

Pan-European Game Information (PEGI) 2007. *Annual report 2006–2007*. Brussels: PEGI. http://www.pegi.info/en/index/id/178/nid/media/pdf/211.pdf

Pelastakaa Lapset ry 2006. *By cell phone: sure! Report on children's cell phone use*. Helsinki: 165Pelastakaa Lapset ry. http://www.pelastakaalapset.fi/nettivihje/english/Cell%20phone%20use%20Eng.pdf

Power out on bail: and now DPP faces questions 2007. *smh.com.au* 10 May. http://www.smh.com.au/news/national/power-out-on-bail--and-now-dpp-faces-questions/2007/05/10/1178390396207.html#

Prentice S 2007. *The five laws of virtual worlds*. Stamford CT: Gartner

Province of Manitoba 2007. Bill proposes mandatory reporting of child pornography. *Media release* 28 November. http://news.gov.mb.ca/news/index.html?archive=&item=2704

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

Quayle E & Taylor M 2003. Model of problematic internet use in people with a sexual interest in children. *Cyberpsychology and behavior* 6(1): 93–106

Queensland Crime and Misconduct Commission 2007. Sunshine Coast paedophile sentenced. *Media release* 2 April. http://www.cmc.qld.gov.au/asp/index.asp?pgid=10814&cid=5201&id=992

Rink E, Tricker R & Harvey SM 2007. Onset of sexual intercourse among female adolescents: the influence of perceptions, depression, and ecological factors. *Journal of adolescent health* 41(4): 398–406

Robertiello G & Terry KJ 2007. Can we profile sex offenders? A review of sex offender typologies. *Aggression and violent behavior* 12(5): 508–518

Rogers M, Scarborough K, Frakes K & San Martin C 2007. Survey of law enforcement perceptions regarding digital evidence. *IFIP international federation for information processing* 242: 41–52

Ropelato J 2007. *Internet pornography statistics*. Top Ten Reviews. http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html

Rosenberg RS 2001. Controlling access to the internet: the role of filtering. *Ethics and information technology* 3(1): 35–54

Rosenbloom A 2004. The blogosphere. *Communications of the ACM* 47(12): 31–33

Rye BJ & Meaney GJ 2007. The pursuit of sexual pleasure. *Sexuality and culture* 11(1): 28–51

SA police officer charged with internet grooming 2007. *IBN news* 4 September

Sandy GA 2000. The online services bill: theories and evidence of pornographic harm. *ACM international conference proceeding series* 7: 46–55

Save the Children Denmark 2005. *Save the children Denmark working to prevent the IT-related sexual exploitation of children*. Copenhagen: Save the children Denmark. http://www.redbarnet.dk/Admin/Public/DWSDownload.aspx?File=Files%2FFiler%2FSeksuelt_misbrug%2FAarsberetningHotline05_ENG.pdf

Schell BH, Martin MV, Hung PCK & Rueda L 2007. Cyber child pornography: a review paper of the social and legal issues and remedies and a proposed technological solution. *Aggression and violent behavior* 12(1): 45–63

Seto MC & Eke AW 2005. The criminal histories and later offending of child pornography offenders. *Sexual abuse: a journal of research and treatment* 17(2): 201–210

Sex offenders explain how and why 2007. *BBC news* 30 October. http://news.bbc.co.uk/1/hi/uk/7069022.stm

Shelby RC 2006. Shelby leads fight against child pornography. *Media release* 15 March http://shelby.senate.gov/news/record.cfm?id=252687

Sibley CG & Heath SO 2004. A quantitative analysis of the content and structure of public requests for private interaction posted in online public chatrooms. *Cyberpsychology and behavior* 7(2): 231–239

Singapore Ministry of Home Affairs 2007a. Summary of the key amendments to the Penal Code. *Media release* 17 September. http://www.mha.gov.sg/news_details.aspx?nid=1115

Singapore Ministry of Home Affairs 2007b. Second reading speech of the Penal Code (Amendment) Bill, by Senior Minister of State A/P Ho Peng Kee on 22 October 2007. *Media release* 22 October. http://www.mha.gov.sg/news_details.aspx?nid=1131

Smith A 2007. *Teens and online stranger contact*. Washington, DC: Pew Internet and American Life Project. http://www.pewinternet.org/PPF/r/223/report_display.asp

Smith RG, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Sophos 2007. Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. *Media release* 14 August. http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html

Specht M 2006. More global effort needed to fight sex crimes against children. *USINFO current issues* 28 September. http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2006&m=September&x=20060928155708lmthceps7.723635e-02

Standards Australia International 2003. *Guidelines for the management of IT evidence: handbook HB 171–2003*. Sydney: Standards Australia International

Stop It Now! 2007. *Annual report 2005–2006*. Northampton, MA: Stop It Now. http://www.stopitnow.org/downloads/StopItNow!AnnRep05-06.pdf

Subrahmanyam K, Smahel D & Greenfield P 2006. Connecting developmental constructions to the internet: identity presentation and sexual exploration in online teen chat rooms. *Developmental psychology* 42(3): 395–406

Swenson C, Phillips R & Shenoi S 2007. File system journal forensics. *IFIP international federation for information processing* 242: 231–244

Syria blocks public access to Facebook 2007. *Todayonline* 29 November. http://www.todayonline.com/articles/224641.asp

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

Tan C 2007. You're 13? What's your bust size? *The straits times* 6 May. http://sporecowboy.blogspot.com/2007/05/youre-13-whats-your-bust-size.html

Telenor 2004. Telenor and KRIPOS introduce internet child pornography filter. *Media release* 21 September. http://press.telenor.com/PR/200409/961319_5.html

Terry KJ & Tallon J 2004. Child sexual abuse: a review of the literature, in *Study of the causes and context of the crisis of sexual abuse of minors in the Catholic Church in the US*. Washington, DC: United States Conference of Catholic Bishops

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 man jailed for child grooming 2007. *Reuters* 26 October. http://www.reuters.com/article/technologyNews/idUSL2629806220071026

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

United Kingdom Child Exploitation and Online Protection (UK CEOP) 2007b. Global online child abuse network smashed: CEOP lead international operation into UK based paedophile ring. *Media release* 18 June. http://www.ceop.gov.uk

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

United Kingdom Child Exploitation and Online Protection (UK CEOP) 2007d. IWF welcomes CEOP's online safety programme for 8–11 year olds. *Media release* 25 October. http://www.iwf.org.uk

United Kingdom Crown Prosecution Services (UK CPS) n.d. *Sexual Offences Act 2003*. http://www.cps.gov.uk/legal/section7/chapter_a.html#73

United Kingdom Home Office 2006. *Sexual Offences Act 2003: a stocktake of the effectiveness of the Act since its implementation*. London: Home Office. http://www.crimereduction.homeoffice.gov.uk/sexual/sexual24.pdf

United Kingdom Office of Public Sector Information (UK OPSI) 2004. *Explanatory notes to Sexual Offences Act 2003*. London: Queen's Printer of Acts of Parliament. http://www.opsi.gov.uk/ACTS/acts2003/en/ukpgaen_20030042_en_1

United States Centers for Disease Control and Prevention (US CDC) 2007. *Sexually transmitted disease surveillance, 2006*. Atlanta, GA: US Department of Health and Human Services

United States Department of Justice (US DoJ) 2007a. Georgia man arrested for sending child pornography to a minor and traveling to New York to engage in sexual acts with a twelve-year-old girl. *Media release* 17 July. http://www.usdoj.gov/usao/nys/pressreleases/July07/harrisarrestpr.pdf

United States Department of Justice (US DoJ) 2007b. US arrests Manhattan consultant for traveling between states to engage in sexual activities with a minor under the age of 12. *Media release* 17 July. http://www.usdoj.gov/usao/nys/pressreleases/July07/hinkleyarrestpr.pdf

United States Department of Justice (US DoJ) 2007c. Project safe childhood: Springfield man sentenced to federal prison for victimizing Connecticut girl he met on myspace.com. *Media release* 17 September. http://newhaven.fbi.gov/dojpressrel/2007/nh091707.htm

United States Department of Justice (US DoJ) 2007d. Former Holly Springs man sentenced to ten years in western NC for coercion and enticement of a minor by computer via the internet. *Media release* 10 October. http://charlotte.fbi.gov/dojpressrel/2007/ce101007a.htm

United States Department of Justice (US DoJ) 2007e. Repeat sex offender indicted on child exploitation charges in Mississippi. *Media release* 17 May. http://www.usdoj.gov/criminal/ceos/Press%20Releases/SDMS%20Ramey%20indict%20PR_051707.pdf

United States Department of Justice (US DoJ) 2007f. Repeat sex offender sentenced to 20 years in prison in Mississippi for possessing child pornography. *Media release* 14 December. http://jackson.fbi.gov/dojpressrel/pressrel07/jacksonchildporn121407.htm

United States Department of Justice (US DoJ) 2008a. Florida man sentenced to 188 months in prison for child exploitation. *Media release* 7 January. http://richmond.fbi.gov/dojpressrel/pressrel08/childexploitation010708.htm

United States Department of Justice (US DoJ) 2008b. Project Safe Childhood: Enfield man who used internet to attempt to engage in sex with minor sentenced to more than 10 years. *Media release* 7 January. http://newhaven.fbi.gov/dojpressrel/2008/nh010708.htm

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 California, Los Angeles (UCLA) 2005. Teenagers find information about sex on the internet when they look for it: and when they don't, UCLA's Children's Digital Media Center reports. *Media release* 27 January. http://newsroom.ucla.edu/portal/ucla/Teenagers-Find-Information-About-5876.aspx?RelNum=5876

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

US sailor walks free after grooming 'girl' 2007. *ABC news* 2 October. http://www.abc.net.au/news/stories/2007/10/02/2048787.htm

Valdes R 2007. *Facebook and the emerging social platform wars*. Stamford, CT: Gartner

Vizard E 2007. Adolescent sexual offenders. *Adolescents* 6(10): 433–437

Vogelstein F, Kirkpatrick D, Roth D, Lashinsky A, Schlender B et al. 2005. 10 tech trends to watch in 2005. *Fortune* 151(1): 43–55

Wagner L 2007. *Using the MySpace friend mapper to build connections for an investigation*. Sacramento, CA: SEARCH, The National Consortium for Justice Information and Statistics

Waite D et al. 2005. Juvenile sex offender re-arrest rates for sexual, violent nonsexual and property crimes: a 10-year follow-up. *Sexual abuse* 17(3): 313–331

Walsh M 2007. Ad spending on social networks will continue to grow in '08. *Mediapost* 17 December. http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=72830

Walsh WA 2005. Nonforcible internet-related sex crimes with adolescent victims: prosecution issues and outcomes. *Child maltreatment* 10(3): 260–271

Websense Security Labs 2006. Malicious website/malicious code: fradulent YouTube video on MySpace installing Zango Cash. *Media release* 6 November. http://www.websense.com/securitylabs/alerts/alert.php?AlertID=689

Webwise 2006. *Survey of children's use of the internet*. n.p.: Webwise. http://www.webwise.ie/GenPDF.aspx?id=1389

Wells M & Mitchell KJ 2007. Youth sexual exploitation on the internet: DSM-IV diagnoses and gender differences in co-occurring mental health issues. *Child and adolescent social work journal* 24(3): 235–260

Westenberg EAM & Garnefski N 2003. Depressive symptomatology and child abuse in adolescents with behavioral problems. *Child and adolescent social work journal* 20(3): 197–210

Whitfield E n.d. Whitfield investigates sexual exploitation of children on the internet. *Media release* 4 April. http://whitfield.house.gov/news/press.aspx?id=32

Williams KR & Guerra NG 2007. Prevalence and predictors of internet bullying. *Journal of adolescent health* 41(6) Supplement 1: S14–S21

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. http://www.missingkids.com/en_US/publications/NC144.pdf

Wolak J, Mitchell K & Finkelhor D 2003. *Internet sex crimes against minors: the response of law enforcement*. Alexandria, VA: National Center for Missing and Exploited Children. http://www.missingkids.com/en_US/publications/NC132.pdf

Wolak J, Mitchell K & Finkelhor D 2006. *Online victimization of youth: five years later*. Alexandria, VA: National Center for Missing and Exploited Children. http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=2530

Would-be pedophile uses net 2007, *The advertiser* 6 November, http://www.news.com.au/adelaidenow/story/0,22606,22708269-2682,00.html?from=public_rss

Yang CC, Liu N & Sageman M 2006. Analyzing the terrorist social networks with visualization tools, in Mehrotra S, Zeng DD, Hsinchun C, Thuraisingham BM & Wang F-Y (eds), *Proceedings of the IEEE international conference on intelligence and security informatics*, San Diego, CA, 23–24 May, Lecture notes in computer science 3975: 331–342

Yap J 2007. Should your kids be on the net? *Todayonline* 29 December. http://www.todayonline.com/articles/229615.asp

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

Zaharia 2007. Romania tackles child porn with software. *Reuters* 25 October. http://www.reuters.com/article/latestCrisis/idUSL25810282

Zittrain J & Edelman B 2003. *Documentation of internet filtering worldwide*. http://cyber.law.harvard.edu/filtering/

# Appendixes

# Appendix A: Sex offender registry websites in the United States [a]

| Sex offender registry websites in the United States | |
|---|---|
| **National** | |
| Dru Sjodin National Sex Offender Public Registry | http://www.nsopr.gov/ |
| **State** | |
| Alabama (Alabama Department of Public Safety Community Information Center) | http://community.dps.state.al.us/ |
| Alaska Sex Offender/Child Kidnapper Registration Central Registry | http://www.dps.state.ak.us/Sorweb/sorweb.aspx |
| Arizona Sex Offender InfoCenter | https://az.gov/webapp/offender/main.do |
| Arkansas Sex Offender Registry | http://www.acic.org/Registration/index.htm |
| California Department of Justice (Megan's Law Home) | http://meganslaw.ca.gov/ |
| Colorado Convicted Sex Offender Site | http://sor.state.co.us/index.cfm?SOR=home.home |
| Connecticut Sex Offender Registry | http://www.ct.gov/dps/cwp/view.asp?a=2157&Q=294474&dpsNav=\| |
| Delaware Sex Offender Central Registry | http://sexoffender.dsp.delaware.gov/ |
| District of Columbia Metropolitan Police Department Sex Offender Registry | http://mpdc.dc.gov/mpdc/cwp/view,a,1241,Q,540704,mpdcNav_GID,1523,mpdcNav,%7C,.asp |
| Florida Sexual Offenders and Predators Registry | http://offender.fdle.state.fl.us/offender/homepage.do;jsessionid=HD6LdLRvQNYhyGBTslvsZVRhhynWZxv1ShQGJXFfnJNn5Xtgg5F6!-1149069608 |
| Georgia Sex Offender Registry | http://gbi.georgia.gov/00/channel_modifieddate/0,2096,67862954_87983024,00.html |
| Guam Sex Offender Registry | http://www.guamcourts.org/sor/ |
| Hawaii Criminal Justice Data Center Sex Offender and Offender Against Minors | http://sexoffenders.hawaii.gov/ |
| Idaho State Police Central Sex Offender Registry | http://www.isp.state.id.us/identification/sex_offender/ |
| Illinois Sex Offender Registration Information Website | http://www.isp.state.il.us/sor/ |
| Indiana Sheriff's Sex and Violent Offender Registry | http://www.insor.org/insasoweb/ |
| Iowa Sex Offender Registry | http://www.iowasexoffender.com/ |
| KBI Registered Offender Website | http://www.accesskansas.org/kbi/ro.shtml |
| Kentucky Sex Offender Registry [b] | http://kspsor.state.ky.us/ |
| Louisiana State Police, State Sex Offender and Child Predator Registry Site | http://lasocpr1.lsp.org/ |
| Maine Sex Offender Registry | http://sor.informe.org/sor/ |
| Maryland Sex Offender Registry | http://www.dpscs.state.md.us/onlineservs/sor/ |
| Massachusetts Sex Offender Registry Board | http://www.mass.gov/?pageID=eopsagencylanding&L=3&L0=Home&L1=Public+Safety+Agencies&L2=Sex+Offender+Registry+Board+(SORB)&sid=Eeops |
| Michigan Public Sex Offender Registry | http://www.mipsor.state.mi.us/ |
| Minnesota Predatory Offender Registry | https://por.state.mn.us/ |
| Missouri Sex Offender Registry | http://www.mshp.dps.missouri.gov/MSHPWeb/PatrolDivisions/CRID/SOR/SORPage.html |
| Montana Sexual or Violent Offender Registry | http://doj.mt.gov/svor/ |
| Nebraska Sex Offender Registry | http://www.nsp.state.ne.us/sor/ |
| Nevada Sexual Offenders Registry | http://www.nvsexoffenders.gov/ |
| New Hampshire Department of Safety, Registered Offenders Against Children | http://www.egov.nh.gov/nsor/ |
| New Jersey State Police Sex Offender Internet Registry | http://www.state.nj.us/njsp/info/reg_sexoffend.html |
| New Mexico Sex Offender | http://www.nmsexoffender.dps.state.nm.us/ |

| Sex offender registry websites in the United States continued | |
|---|---|
| **State** | |
| New York State Sex Offender Registry | http://criminaljustice.state.ny.us/nsor/ |
| North Carolina Sex Offender and Public Protection Registry | http://ncfindoffender.com/disclaimer.aspx |
| Ohio Electronic Sex Offender Registration and Notification | http://www.esorn.ag.state.oh.us/Secured/p1.aspx |
| Oklahoma Sex and Violent Crime Offender Registry | http://docapp8.doc.state.ok.us/servlet/page?_pageid=190&_dad=portal30&_schema=PORTAL30 |
| Oregon Sex Offender Inquiry System | http://sexoffenders.oregon.gov/ |
| Pennsylvania State Police Megan's Law Website | http://www.pameganslaw.state.pa.us/ |
| Puerto Rico Sex Offender and Child Abuse Registry | http://sijc.gobierno.pr/CJISPortal/SexualOffenders/search.aspx |
| Rhode Island Parole Board and Sex Offender Community Notification Unit | http://www.paroleboard.ri.gov/sexoffender/agree.php |
| South Carolina Sex Offender Registry | http://services.sled.sc.gov/Sor/ |
| South Dakota Sex Offender Registry | http://sor.sd.gov/disclaimer.asp?page=search&nav=2 |
| Tennessee Sexual Offender Registry | http://www.ticic.state.tn.us/sorinternet/sosearch.aspx |
| Texas Sex Offender Registry | https://records.txdps.state.tx.us/DPS_WEB/Sor/index.aspx |
| Utah Sex Offender Registry | http://corrections.utah.gov/asp-bin/sexoffendersearchform.asp |
| Vermont Sex Offender Registry | http://170.222.137.2:8080/sor/ |
| Virginia Sex Offender and Crimes Against Minors Registry | http://sex-offender.vsp.virginia.gov/sor/index.htm |
| Washington State Sex Offender Information Center | http://ml.waspc.org/ |
| West Virginia State Police Sex Offender Registry | http://www.wvstatepolice.com/sexoff/ |
| Wisconsin Sex Offender Registry | http://offender.doc.state.wi.us/public/ |
| Wyoming Sex Offender Registry | http://wysors.dci.wyo.gov/ |

a: Several of the URLs provided on SEARCH are outdated. The above URLs were correct as of 21 November 2007.

b: Kentucky Sex Offender Registry explicitly states that the use of information from the website to harass a sex offender is criminalised under KRS 525.070 and 525.080 and is punishable by up to 90 days in the county jail. Similar warnings are on other sites such as the Nebraska Sex Offender Registry, and the Rhode Island Parole Board and Sex Offender Community Notification Unit.

Source: Adapted from SEARCH (http://www.search.org/programs/policy/states.asp)

# Appendix B: Examples of countries with and without legislation to criminalise child pornography

| Examples of countries with and without legislation to criminalise child pornography | | | |
|---|---|---|---|
| **Country** | **Legislation criminalising child pornography offences?** | **Computer-facilitated child exploitation offences?** | **Mandatory for ISPs to report suspected child pornography to law enforcement or other authorities?** |
| Afghanistan | No | No | No |
| Albania | No | No | No |
| Algeria | No | No | No |
| Andorra | Yes | No | No |
| Angola | No | No | No |
| Antigua and Barbuda | No | No | No |
| Argentina | Yes | No | No |
| Armenia | Yes | Yes | No |
| Aruba | Yes | Yes | No |

| Examples of countries with and without legislation to criminalise child pornography continued | | | |
|---|---|---|---|
| Country | Legislation criminalising child pornography offences? | Computer-facilitated child exploitation offences? | Mandatory for ISPs to report suspected child pornography to law enforcement or other authorities? |
| Australia | Yes | Yes | Yes |
| Austria | Yes | Yes | No |
| Azerbaijan | No | No | No |
| Bahamas | No | No | No |
| Bahrain | No | No | No |
| Bangladesh | No | No | No |
| Barbados | Yes | No | No |
| Belarus | Yes | No | No |
| Belgium | Yes | Yes | Yes |
| Belize | No | No | No |
| Benin | No | No | No |
| Bhutan | Yes | Yes | No |
| Bolivia | No | No | No |
| Bosnia–Herzegovina | Yes | Yes | No |
| Botswana | No | No | No |
| Brazil | Yes | Yes | No |
| Brunei | Yes | Yes | No |
| Bulgaria | Yes | Yes | No |
| Burkina–Faso | No | No | No |
| Burundi | No | No | No |
| Cambodia | No | No | No |
| Cameroon | No | No | No |
| Canada | Yes | Yes | No |
| Cape Verde | Yes | No | No |
| Central African Republic | No | No | No |
| Chad | No | No | No |
| Chile | Yes | Yes | No |
| China | Yes | Yes | No |
| Colombia | Yes | Yes | Yes |
| Comoros | No | No | No |
| Congo | No | No | No |
| Costa Rica | Yes | No | No |
| Côte d'Ivoire | No | No | No |
| Croatia | Yes | Yes | No |
| Cuba | No | No | No |
| Cyprus | Yes | Yes | No |
| Czech Republic | Yes | Yes | No |
| Democratic Republic of Congo | No | No | No |
| Denmark | Yes | Yes | No |
| Djibouti | No | No | No |
| Dominica | No | No | No |
| Dominican Republic | Yes | No | No |
| Ecuador | Yes | No | No |
| Egypt | No | No | No |
| El Salvador | Yes | Yes | No |

| Examples of countries with and without legislation to criminalise child pornography continued | | | |
|---|---|---|---|
| Country | Legislation criminalising child pornography offences? | Computer-facilitated child exploitation offences? | Mandatory for ISPs to report suspected child pornography to law enforcement or other authorities? |
| Equatorial Guinea | No | No | No |
| Eritrea | No | No | No |
| Estonia | Yes | Yes | No |
| Ethiopia | No | No | No |
| Fiji | No | No | No |
| Finland | Yes | Yes | No |
| France | Yes | Yes | Yes |
| Gabon | No | No | No |
| Gambia | Yes | No | No |
| Georgia | Yes | No | No |
| Germany | Yes | Yes | No |
| Ghana | No | No | No |
| Greece | Yes | Yes | No |
| Grenada | No | No | No |
| Guatemala | Yes | No | No |
| Guinea | No | No | No |
| Guinea Bissau | No | No | No |
| Guyana | No | No | No |
| Haiti | No | No | No |
| Honduras | Yes | Yes | No |
| Hong Kong | Yes | Yes | No |
| Hungary | Yes | Yes | No |
| Iceland | Yes | Yes | No |
| India | No | No | No |
| Indonesia | No | No | No |
| Iran | No | No | No |
| Iraq | No | No | No |
| Ireland | Yes | Yes | No |
| Israel | Yes | Yes | No |
| Italy | Yes | Yes | No |
| Jamaica | No | No | No |
| Japan | Yes | Yes | No |
| Jordan | No | No | No |
| Kazakhstan | Yes | No | No |
| Kenya | No | No | No |
| Korea | Yes | Yes | No |
| Kuwait | No | No | No |
| Kyrgyzstan | Yes | No | No |
| Laos | No | No | No |
| Latvia | Yes | Yes | No |
| Lebanon | No | No | No |
| Lesotho | No | No | No |
| Liberia | No | No | No |
| Libya | No | No | No |
| Liechtenstein | Yes | Yes | No |

| Examples of countries with and without legislation to criminalise child pornography continued | | | |
|---|---|---|---|
| Country | Legislation criminalising child pornography offences? | Computer-facilitated child exploitation offences? | Mandatory for ISPs to report suspected child pornography to law enforcement or other authorities? |
| Lithuania | Yes | No | No |
| Luxembourg | Yes | Yes | No |
| Macedonia | Yes | Yes | No |
| Madagascar | Yes | Yes | No |
| Malawi | No | No | No |
| Malaysia | No | No | No |
| Maldives | No | No | No |
| Mali | Yes | No | No |
| Malta | Yes | Yes | No |
| Marshall Islands | No | No | No |
| Mauritania | No | No | No |
| Mauritius | Yes | Yes | No |
| Mexico | Yes | Yes | No |
| Moldova | No | No | No |
| Monaco | No | No | No |
| Mongolia | No | No | No |
| Morocco | Yes | No | No |
| Mozambique | No | No | No |
| Myanmar | Yes | No | No |
| Namibia | No | No | No |
| Nauru | No | No | No |
| Nepal | Yes | No | No |
| Netherlands | Yes | Yes | No |
| Netherlands Antilles | No | No | No |
| New Zealand | Yes | Yes | No |
| Nicaragua | No | No | No |
| Niger | No | No | No |
| Nigeria | No | No | No |
| Norway | Yes | Yes | No |
| Oman | No | No | No |
| Pakistan | No | No | No |
| Panama | Yes | Yes | No |
| Papua New Guinea | Yes | No | No |
| Paraguay | Yes | No | No |
| Peru | Yes | Yes | No |
| Philippines | Yes | No | No |
| Poland | Yes | No | No |
| Portugal | Yes | Yes | No |
| Qatar | Yes | Yes | No |
| Romania | Yes | Yes | No |
| Russia | Yes | No | No |
| Rwanda | No | No | No |
| St. Kitts and Nevis | No | No | No |
| St. Lucia | No | No | No |
| St. Vincent and the Grenadines | No | No | No |

| Examples of countries with and without legislation to criminalise child pornography continued | | | |
|---|---|---|---|
| Country | Legislation criminalising child pornography offences? | Computer-facilitated child exploitation offences? | Mandatory for ISPs to report suspected child pornography to law enforcement or other authorities? |
| São Tomé and Príncipe | No | No | No |
| Saudi Arabia | No | No | No |
| Senegal | No | No | No |
| Serbia and Montenegro | Yes | Yes | No |
| Seychelles | No | No | No |
| Sierra Leone | No | No | No |
| Singapore [a] | Yes | Yes | No |
| Slovak Republic | Yes | Yes | No |
| Slovenia | Yes | Yes | No |
| Somalia | No | No | No |
| South Africa | Yes | Yes | Yes |
| Spain | Yes | Yes | No |
| Sri Lanka | Yes | No | No |
| Sudan | No | No | No |
| Suriname | No | No | No |
| Swaziland | No | No | No |
| Sweden | Yes | Yes | No |
| Switzerland | Yes | Yes | No |
| Syria | No | No | No |
| Tajikistan | Yes | No | No |
| Tanzania | Yes | No | No |
| Thailand | No | No | No |
| Timor Leste | No | No | No |
| Togo | No | No | No |
| Tonga | Yes | Yes | No |
| Trinidad and Tobago | No | No | No |
| Tunisia | Yes | Yes | No |
| Turkey | Yes | No | No |
| Turkmenistan | No | No | No |
| Uganda | No | No | No |
| Ukraine | Yes | Yes | No |
| United Arab Emirates | No | No | No |
| United Kingdom | Yes | Yes | No |
| United States | Yes | Yes | Yes |
| Uruguay | Yes | Yes | No |
| Uzbekistan | No | No | No |
| Venezuela | Yes | Yes | No |
| Vietnam | No | No | No |
| Yemen | No | No | No |
| Zambia | No | No | No |
| Zimbabwe | No | No | No |

a: Legislation in Singapore has been updated to criminalise the meeting or travelling to meet a minor under 16 years of age after sexual grooming (Table 22)

Source: Adapted from ICMEC (2006)

**AIC** Reports
Research and Public Policy Series 103

The grooming of children for sexual purposes has been facilitated by online technologies, particularly social networking sites. This report describes the nature and extent of how new technologies are being exploited by offenders and the legislative and non-legislative responses being used to combat this growing problem.

Australia's national research and
knowledge centre on crime and justice

**www.aic.gov.au**