NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

Protecting Children From Online Sexual Predators

by

Gareth Griffith and Lenny Roth

Briefing Paper No 10/07

RELATED PUBLICATIONS

- Child Sexual Offences: An Update on Initiatives in the Criminal Justice System by Rowena Johns, NSW Parliamentary Library Briefing Paper No 20/2003

ISSN 1325-5142
ISBN 978 0 7313 18261

September 2007

Protecting Children From Online Sexual Predators

by

Gareth Griffith and Lenny Roth

NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

David Clune (MA, PhD, Dip Lib), Manager.....(02) 9230 2484

Gareth Griffith (BSc (Econ) (Hons), LLB (Hons), PhD),
Senior Research Officer, Politics and Government / Law .....(02) 9230 2356

Stephanie Baldwin (BSc (Hons), PhD), Research Officer, Environment ..(02) 9230 2798

Lenny Roth (BCom, LLB), Research Officer, Law .....(02) 9230 3085

John Wilkinson (MA, PhD), Research Officer, Economics.....(02) 9230 2006

Should Members or their staff require further information about this publication please contact the author.

Information about Research Publications can be found on the Internet at:

www.parliament.nsw.gov.au/WEB_FEED/PHWebContent.nsf/PHPages/LibraryPublications

CONTENTS

EXECUTIVE SUMMARY

Online grooming: Issues concerning the protection of children from online sexual predators have been prominent in political and media debates in recent times. The focus of this paper is on the use of the Internet for the sexual solicitation of children, which is known as 'online grooming'. Typically, this relates to the use of the Internet with the intention to 'procure' a child to engage in sexual activity, either online or by means of a physical encounter offline. It can also refer to more preparatory online communications that are designed to make children more amenable to sexual advances. **[1]**

Recent proposals and initiatives: In recent weeks attention has focused on the deletion in the United States of the profiles of 29,000 convicted sex offenders from the social networking site MySpace. In Australia MySpace has proposed that the email addresses of convicted child sex offenders be compulsorily registered for the purpose of removing known sex offenders from the site. To date, the Commonwealth Government has not endorsed this proposal. On 10 August 2007 it was reported that the NSW Police Minister plans to refer to Cabinet a proposal to require sex offenders to register their email addresses. If Cabinet agrees, the requirement will be incorporated into the *Child Protection (Offenders Registration) Act 2000* (NSW) **[2.1].** On the same day, the Federal Government announced a $189 million package of reforms to 'protect Australian families from online dangers in the increasingly complex internet environment'. **[2.3]**

Research findings: Since the dangers of online usage were identified in the 1990s many jurisdictions, including Australia, have engaged in research projects to identify the scope and nature of the problems at issue. The research suggests that the world of online grooming is a complex place. A US study in 2007 found that 8% of children reported they'd actually met someone they knew online, while a 2006 study found that one in seven children aged 10-17 received unwanted online sexual solicitations. On the other hand, not all these come from strangers. It also seems that many 'groomers' do not lie at all about themselves and what their intentions are. This research suggests that most at risk from online grooming are teenage girls who become 'romantically' involved with those they meet on social networking systems. However, more research needs to be undertaken in this field, across jurisdictions, to gain a broader and truer picture of the risks involved to all minors. **[5.2]** When the online practices and perceptions of parents and children are compared there is a sense in which they are reporting on parallel realities. It has been suggested that 'Directing more safety awareness at children themselves may be the best way forward, since parents often don't know what their children are doing online'. **[5.4]**

Online grooming laws in Australia: Laws specifically designed to counter the online sexual solicitation of minors have been passed in several Australian and other comparable jurisdictions, but not in NSW. In 2001, the ACT created a new offence of 'Using the Internet etc to deprave young people'. Two years later Queensland created a new offence of using the Internet with the intent of procuring a child under the age of 16 to engage in a sexual act or providing indecent matter to a child under 16. The law allows police to catch cyber-predators by providing that it is irrelevant to the offence that the child is a fictitious person represented by an adult. Express provision is therefore made for police 'stings' against online predators. Similar reforms followed in Tasmania, Western Australia and at the Commonwealth level. South Australia and Victoria have also made relevant

amendments to their criminal laws. In summary, the main Australian laws expressly targeting online sexual predators are directed towards some or all of the following acts:

- using the Internet (or other form of communication) with the intention of 'procuring' a child to engage is sexual activity (Commonwealth, Queensland, South Australia, Tasmania and Western Australia);
- 'grooming' a child, by sending indecent material to a child or otherwise engaging in prurient communication with a child, with the intention of making it easier to procure a child to engage in sexual activity (Commonwealth, South Australia);
- 'exposing' a child to indecent or pornographic material (Queensland, Tasmania, Western Australia, ACT, NT). **[6.6]**

To some extent the introduction of the Commonwealth Internet procuring and 'grooming' offences has overtaken the need for parallel reforms in the States. In the absence of a specific NSW online grooming offence, NSW Police can (and does) refer cases to the Commonwealth Director of Public Prosecutions. **[6.5]**

Online grooming laws in other jurisdictions: Online grooming laws have also been passed in other jurisdictions, including the United States **[6.11]**, Canada **[6.16]**, England and Wales **[6.17]**, and New Zealand. **[6.18]**

Police operations targeting online child exploitation: Specialist police units have been formed in Australia to combat online child exploitation. In 1999, NSW police set up the Child Exploitation Internet Unit and in March 2005 the Australian Federal Police established the Online Child Sex Exploitation Team (OCSET). In August 2005, it was reported that, as part of a joint operation with the Federal police, NSW police would rely on the Commonwealth laws to launch an undercover operation to catch online predators targeting children in chat rooms. In August 2007, Federal Government committed additional funds to OCSET. Australia is also part of an international effort to combat online child abuse through the Virtual Global Taskforce, which was set up in 2003. **[7.1]-[7.5]**

Prosecutions for offences in Australia: There have been over 130 completed prosecutions for online procuring, grooming and exposure offences in Australia. Most of these have been for offences under the Queensland provision (118 cases) with prosecutions also occurring under the Commonwealth provision (4 cases), the West Australian provision (8 cases) and the Northern Territory provision (at least one case). No data is available about sentencing outcomes in Queensland but in five appeal cases a 3-month custodial sentence was typical. Commonwealth prosecutions have resulted in custodial sentences ranging from 3 months up to almost the maximum of 12 years. In Western Australia, custodial sentences have usually been imposed, with the maximum being 27 months. **[8.1]-[8.6]**

Industry measures to protect children: Social networking sites, MySpace and Facebook, have taken some measures to protect children including setting a minimum age (although neither site can verify a person's age), creating special privacy controls for children, posting safety tips for parents and children on their websites, and allowing users to report misconduct. As noted above, MySpace has also checked its members' names against a national database of sex offenders in the US and has deleted 29,000 profiles. In the US, State Attorneys General have criticised social networking sites for not doing enough to protect children and they have called for the sites to introduce age verification and to obtain parental permission before allowing children under the age of 18 to sign up. **[9.1]-[9.4]**

Educating children and parents about online safety: NetAlert (the Federal Government's Internet safety advisory body) educates children and parents about online safety. Its website contains a range of information and safety tips and people can now contact its new Internet safety hotline. NetAlert also runs educational programs in primary and secondary schools including CyberSafe Schools, and the Think U Know program (commencing in 2008). The Australian Communications and Media Authority has also contributed to this effort by launching the Cybersmart kids website, publishing the Cybersmart guide and running the Cybersmart detectives online activity in some schools. In August 2007, the NSW Government announced that it would distribute a new technology guide for parents in schools across NSW. The Federal Government also announced in August that it would be launching a new public awareness and education program. **[10.1]-[10.3]**

Use of filtering software to protect children: Internet filtering software can block children from using a computer to access inappropriate content on the Internet. In addition to blocking access to websites (and of more relevance to the issue of online predators), some filtering programs can block chat, instant messaging and email communications. Some programs can also prevent children from giving out personal information and some allow parents to monitor activities such as the use of computer programs, websites visited, chat room activity and social network sites accessed. In August 2007, the Federal Government announced that it would introduce a National Filter Scheme that will provide every family with free access to the best available Internet filtering technology. Under this scheme, which commenced on 20 August 2007, parents can download accredited filtering programs from the NetAlert website or have them delivered by post. **[11.1]-[11.5]**

1. INTRODUCTION

Issues concerning the protection of children from online sexual predators have been prominent in political and media debates in recent times. For paedophiles the new online technologies have presented alternative avenues of operation, including the opportunity to organise informal networks on a global scale. The dangers posed by online communications technologies for unsuspecting youngsters have been the subject of policy and legislative initiatives, as governments, police forces and others have sought to protect the vulnerable from falling into the traps set by those seeking to gain access to their lives. The prevailing debate concerns the formulation of practical laws and polices for the protection of children from harm in an environment that is constantly evolving, producing ever more opportunities for communication, education and entertainment. Within this environment the focal points for potential legal and administrative initiatives are many and varied, some looking to prevention, others to the apprehension and prosecution of offenders.

The focus of this paper is on the use of the Internet for the sexual solicitation of children, which is known as 'online grooming'. Typically, this relates to the use of the Internet with the intention to 'procure' a child to engage in sexual activity, either online or by means of a physical encounter offline. It also refers to more preparatory online communications that are designed to make children more amenable to sexual advances.

Laws specifically designed to counter the online sexual solicitation of minors have been passed in several Australian and other comparable jurisdictions, but not in NSW. This is despite the fact that during the campaign for the March 2003 State election Premier Carr proposed the introduction of a new offence of using electronic communication devices, such emails and SMS text messages sent by mobile phones, to entice a child into illegal sexual activity.[1] As far back as 1997 the Wood Royal Commission recommended the introduction into the *Crimes Act 1900* (NSW) of an offence to proscribe:

> the use of an on-line service to make any request, suggestion, or proposal constituting an invitation or encouragement to a person under the age of 16 years to engage in sexual activity (with the maker of that communication, or anyone else) knowing the recipient to be under 16 years of age, or recklessly careless as to whether the recipient is under that age.[2]

To some extent the introduction of the Commonwealth Internet procuring and 'grooming' offences has overtaken the need for parallel reforms in the States. In the absence of a specific NSW online grooming offence, NSW Police can (and does) refer cases to the Commonwealth Director of Public Prosecutions.

The paper concentrates on three questions: What are the dangers posed by the online sexual

---

1 NSW Attorney General, 'Government questions timing of Coalition's child protection announcement', *Media Release*, 14 March 2003.

2 Royal Commission into the NSW Police Service, *Final Report,* Vol. 1V: *The Paedophile Inquiry*, August 1997, p1148.

solicitation of children? what has been done to address and combat these? what other legal, administrative and other initiatives have been proposed? The paper begins with a brief overview of recent developments and an outline of Internet communication technology.

Unless otherwise stated, the information in this paper is current as at 31 August 2007.

2. OVERVIEW OF RECENT DEVELOPMENTS

2.1 Proposal to require sex offenders to register their email addresses

In recent weeks attention has focused on the deletion in the United States of the profiles of 29,000 convicted sex offenders from the social networking site MySpace. This occurred as a result of cooperation between MySpace and State and federal law enforcement authorities. Several State Attorneys-General had been pressuring MySpace to release data on how many registered sex offenders were using the social networking site. After initially withholding the information, citing federal privacy laws, by matching member names with child offender registers MySpace began sharing the information in May 2007, this after the States filed formal legal requests. At that initial stage, MySpace deleted 7,000 profiles of sex offenders, out of an estimated 180 million profiles on the site.[3]

In Australia MySpace has proposed that the email addresses of convicted child sex offenders be compulsorily registered for the purpose of removing known sex offenders from the site. To date, the Commonwealth Government has not endorsed this proposal, indicating on 28 June 2007 that there were 'practical limitations' that would need to be addressed before it could be further considered.[4] On 27 July 2007, following news of developments in the United States, an editorial in the *Sydney Morning Herald* lent its support to the MySpace proposal, stating:

> We must be more proactive in keeping predators off the websites that attract the young. In this regard, proposals from the MySpace website are moderate and worth exploring. MySpace does not want a public list of offenders or even access to such a list. It wants to be able to supply email addresses of its members to the Federal Government agency CrimTrac to see if they match any on the Australian National Child Offence Register. The risk is seeks to address is clear.[5]

On 26 July 2007, the Federal Government is reported to have said it would 'not be updating' the Australian National Child Offenders Register [ANCOR] to include current email addresses.[6] However, as part of online safety reforms announced on 10 August 2007 (see below), the Federal Government stated that it would investigate how ANCOR 'could

---

3 GD Robertson, 'MySpace: 29,000 sex offenders have profiles', *MSNBC*, 24 July 2007 - http://www.msnbc.msn.com/id/19936355/

4 AFP document provided to the authors and held in the NSW Parliamentary Library.

5 'Tracking predators on the web', *SMH*, 27 July 2007 p 10.

6 A Moses, 'Online sex pests unwatched', *SMH*, 26 July 2007, p 1.

be better used to keep paedophiles away from children online'.[7]

The NSW Police Minister, David Campbell, said he would consider any proposals to improve Internet safety, saying 'In an era where this type of social interaction is increasing, there are clear risks for children and young people from online sexual predators'.[8] Taking independent action, on 10 August it was reported that Mr Campbell plans to refer to Cabinet a proposal to require sex offenders to register their email addresses. If Cabinet agrees, the requirement will be incorporated into the *Child Protection (Offenders Registration) Act 2000* (NSW).[9]

In the United Kingdom, recent developments have prompted a leading children's charity, the NSPCC, to call for social networking websites to be given access to the register of sex offenders so that sex offenders can be blocked from targeting children on these sites. Zoe Hilton, policy advisor at the NSPCC, said 'As long as the information is handled safely and it is encrypted it would be a no-brainer. It would be a useful tool to block sex offenders'. The same report noted that in June 2007 the then Home Secretary, John Reid, announced that all convicted sex offenders would have to supply their email addresses to the police.[10] The proposal had in fact been announced as far back as February 2007, for child sex offenders to supply both their email addresses and 'any screen names they use in Internet chat rooms'.[11]

2.2 NSW and Federal Government initiatives announced in August 2007

On 9 August 2007, it was announced that a guide for parents on protecting children from the risks involved with the Internet would be distributed in schools throughout NSW.[12]On 10 August 2007, the Federal Government announced a $189 million package of reforms to 'protect Australian families from online dangers in the increasingly complex internet environment'.[13] These reforms include:

---

7 Senator Helen Coonan, 'NetAlert: Protecting Australian Families Online', *Media Release,* 10/8/07.

8 A Moses, 'Online sex pests unwatched', *SMH*, 26 July 2007, p 1. Mr Campbell is further reported to have said: 'The Commonwealth doesn't have any work in place to try and identify [the problem]…That's why the NSW Government stands ready to work with the Commonwealth, to look at any means of limiting, or eliminating would be a preferable way, the use of the Internet for this purpose' - 'Internet paedophiles should be deleted: NSW Government', *ABC News*, 26 July 2007 – http://www.abc.net.au/news/stories/2007/07/26/1988845.htm

9 P Coorey, 'Veto for parents on web content', *SMH*, 10 August 2007, p 1; M Farr, 'Porn-proof web pledge', *Daily Telegraph*, 10 August 2007, p 5.

10 H Wallop, 'MySpace should seek UK sex offenders list', *Telegraph.co.uk*, 27 July 2007 - http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/07/27/nmyspace127.xml

11 http://police.homeoffice.gov.uk/news-and-publications/news/children-internet

12 B McDougall, 'School manual fights the cyber predators', *Daily Telegraph*, 9 August 2007, p 7.

13 Coonan, n 7. Note that a package containing some of these measures had previously been

- Free access to Internet filtering technology for every Australian family;
- Additional resources for the Australian Federal Police's Online Child Sex Exploitation Unit and its high-tech crime units;
- Additional resources for the Commonwealth DPP;
- A national Internet safety hotline for parents;
- A public awareness and education campaign about online safety issues;
- Additional resources to expand NetAlert's outreach education program;
- A Consultative Working Group concerning social networking websites.[14]

3. INTERNET COMMUNICATION TECHNOLOGY

Children use various forms of Internet communication technology including:

- ***Blogs:*** A blog (short for web log) is a page on the Internet where a person posts information, usually in the form of a personal journal.[15] A typical blog combines text, images, and links to other pages.[16] Blogs can usually be viewed by anyone but they can be also restricted to friends. Readers can post comments on blogs.

- ***Chat rooms:***[17] A chat room is a place on the Internet where several people can communicate in real time by typing text messages. Messages appear instantly to everybody who is present in the virtual room. Chat rooms are open to everyone on the Internet and people can join a chat room without verification of who they are. Many chat rooms are devoted to a topic (eg movies), while others are intended for a particular age group (eg teens). Many chat rooms have a function that allows two people to leave the virtual room and write private messages to each other. Some chat rooms have moderators that monitor conversations.

- ***E-mail:*** E-mail is a tool that allows someone to send a text message over the Internet to the electronic mailbox of another user.[18] In order to send an e-mail, the sender must know the recipient's electronic mailbox address.

- ***Online games:***[19] These are video games and other interactive games (eg chess) that

---

announced in June 2006: see Senator Helen Coonan, '$116.6 million to Protect Australian Families Online', *Media Release,* 21/6/06.

14 Coonan, n 7.

15 ECPAT International, *Violence Against Children in Cyberspace,* September 2005, p86. Accessed at http://www.ecpat.net/eng/publications/Cyberspace/

16 *Wikipedia,* 'Blog', accessed at: http://en.wikipedia.org/wiki/Blog

17 This information was, in part, sourced from NetAlert, 'What is a chat room', accessed at: http://www.netalert.gov.au/advice/services/chat/what_is_a_chat_room.html

18 ECPAT International, n15, p87.

19 This information was sourced from the Chatdanger website: http://www.chatdanger.com/games/facts.aspx and the Los Angeles District Attorney's

are played over the Internet. People often play with or compete against people from all over the world who they do not know. Most online game websites allow the players to chat with each other using instant messaging (see below).

- ***Instant messaging:*** Instant messaging (IM) programs allow two people who use the same program to communicate with each other in real time by typing text messages that appear instantly.[20] IM 'can be a very private form of communication between known friends where the user builds up a list of contacts and is alerted when they are online'.[21] However, some IM programs allow all users to view personal information about other users and to contact them (but users may have the option of not receiving messages from unknown users).[22] In addition to text-based chat, IM programs also allow users to send files and photographs.[23] Webcams can now be used with some programs to enable real-time online video communication.[24] Popular IM programs include *ICQ* and *MSN Messenger*.

- ***Skype:***[25] Skype allows people to use the Internet to make free telephone calls – and with the use of webcams, free video calls - to other users anywhere in the world. Skype also facilitates instant messaging and chat rooms. In addition, Skype users can create a personal profile. Other users can view these profiles and – subject to privacy controls - can communicate with the person either by voice or video call or by instant messaging. Skype has around 200 million users worldwide.[26] Some relevant features of Skype are outlined in **Appendix 1.**

- ***Social networking websites*:** These websites – two popular ones are **MySpace** and **Facebook –** are designed to enable members to communicate online with friends and make new friends. Members create online profiles and they can upload photos and videos and create blogs. Subject to privacy controls, other members can view this content and can communicate with them. MySpace has more than 175 million

---

website http://da.co.la.ca.us/pok/onlgames.htm

20 NetAlert, 'What is instant messaging', accessed at: http://www.netalert.gov.au/advice/services/im/What_is_instant_messaging.html

21 UK Home Office Task Force on Child Protection on the Internet, *Good Practice Models and Guidance for the Internet Industry on Chat Services, Instant Messaging and Web-based services,* Home Office Communication Directorate, January 2003, p16

22 UK Home Office Task Force, n 21, p16-17.

23 NetAlert, 'What are the benefits of instant messaging', accessed at: http://www.netalert.gov.au/advice/services/im/What_are_the_benefits_of_instant_messaging.html

24 *Wikipedia,* 'Webcam', accessed at http://en.wikipedia.org/wiki/Webcam

25 This information was sourced from the Skype website: www.skype.com

26 'Paedophiles use Skype 'loophole' to woo children', *Times Online,* 6/5/07.

members worldwide.[27] In Australia, there are 3.8 million members, a quarter of which are under 18.[28] Facebook has around 25 million members worldwide.[29] Some relevant features of these two sites are outlined in **Appendix 2.**

It is important to note that the new **3G mobile phones** allow users to connect to the Internet. Children who have these new phones can therefore access the various forms of Internet communication technology directly from their phone.

4. THE DANGERS POSED BY ONLINE PREDATORS

4.1 The problem stated

Many of the concerns in the debate about online predators were encapsulated in the March 2000 report of the US President's Working Group on Unlawful Conduct on the Internet, which stated:

> The Internet, despite its many benefits, has unfortunately provided pedophiles with a new tool. Offering relative anonymity for sophisticated users and continuous access, the Internet has made it easy for child pornographers to distribute their materials and for pedophiles to lure and prey on children…pedophiles can lurk around chat channels and rooms and message boards and use e-mail to lure children for sex.[30]

A similar scenario was presented in the Second Reading speech for the ACT's anti-grooming legislation, with the Minister stating:

> Instead of hanging around schools and playgrounds, as they used to, many paedophiles now contact their intended victims through the relative safety of anonymous chat rooms. They seek out lonely and troubled kids, befriend them and then work clever schemes to trick them into a meeting. There have been horrific instances of such activity. Unfortunately, as is occasionally reported in the media, we are not immune to these types of people in Australia...[31]

In a brief on high tech crime published by the Australian Institute of Criminology in 2005 Tony Krone wrote:

> ICT [information and communication technologies] enables offenders to target

---

27 'MySpace calls for Australian sex-offender database', *The Age,* 24/5/07.

28 'Online sex pests unwatched', *The Sydney Morning Herald,* 26/7/07.

29 'Popularity of Facebook soars', *ABC News,* 19/6/07.

30 The President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, Appendix C, March 2000 - http://www.usdoj.gov/criminal/cybercrime/unlawful.htm

31 *ACT Parliamentary Debates*, 9 August 2001, p 2651 (Mr Osborne).

> children individually or collectively…Children are particularly vulnerable to exploitation via ICT because the medium is attractive, they often use the internet unsupervised and increasingly have access to portable devices with the capacity for data storage, digital photography and communications such as third generation mobile phones. Electronic communications allow offenders to exploit the curiosity and interests of children for a number of purposes.

The briefing paper continued:

> Sexual exploitation may commence using seemingly innocent facilities such as internet chat rooms. Initial contact may be part of 'grooming' the child, whereby the child begins to trust the perpetrator and is desensitised to sexually explicit material including child pornography. Possible motives for grooming a child are: to engage in cyber sex or simulated sex online, to distribute pornographic material to the child or to induce the child to submit pornographic images of themselves online. In some cases, grooming leads to a physical meeting in which the perpetrator sexually assaults the child.[32]

4.2 Media reports and other developments

Australia: Media reports of such predatory activity are now commonplace, as are reports of police operations and journalistic 'stings' directed against online predators. On 26 June 2007 the *Sydney Morning Herald* carried three related stories. One headed 'I'm a family man: accused' told of a US serviceman who was arrested at Sydney Airport and charged with allegedly grooming a child over the Internet for sexual intercourse.[33] The second story, which carried the by-line 'Gothic fan groomed teen for sex, court told' told of man who set up an online Gothic appreciation club on his MySpace web page and, by way of a membership fee, allegedly required under-age teenage girls either to agree to sexual intercourse or to email naked photographs of themselves to him. The man, who was charged with using a telecommunications carriage service to groom a 13-year old girl for sex, was remanded in custody to reappear before Central Local Court on 22 August. A third story, headed 'Virtual girl traps predators', reported a 'sting' arranged by journalist in Britain who used the Skype internet chat room to pose as a 14-year old Sydney schoolgirl. It was reported that, within an hour, contact had been made with 15 Skype users wanting sex with the 'virtual girl'. The article concluded, 'British police are investigating the possibility that an organised pedophile ring operates on Skype'.[34]

---

32 T Krone, *High Tech Crime Brief – No 2 Child Exploitation*, AIC 2005 - http://www.aic.gov.au/publications/htcb/htcb002.html

33 The man later pleaded guilty to 'using the internet to groom a 14-year old Australian girl for sex in a police sting operation'. He was released on bail ahead of a sentencing hearing in the District Court on 31 August 2007. Under his bail conditions, he has been banned from using the Internet except for work or to contact his immediate family – D Braithwaite, 'Sailor guilty of net grooming', *SMH*, 20 August 2007 - http://www.smh.com.au/news/national/sailor-guilty-of-net-grooming/2007/08/20/1187462141758.html See also E Yamine, 'Sailor's child-sex guilt', *Daily Telegraph*, 21 August 2007, p 14.

34 M Foley and B Cubby, 'Virtual girl traps predators', *SMH*, 26 June 2007, p 2.

United States: Of course reports of this kind are not confined to Australia. In the United States in 2005 the Center for Missing and Exploited Children reported more than 2,600 incidents of adults using the Internet to entice children.[35] In January 2007 the US House of Representatives Committee on Energy and Commerce reported that it had received testimony from television news journalist Chris Hansen, who led a multi-part investigative series that aired on Dateline NBC, entitled 'To Catch a Predator'. The series focused on the activities of predators on the Internet and showed how actual predators contacted and groomed individuals they believed were potential child victims. The individuals that the predators communicated with online were actually adult volunteers for an online watchdog group, Perverted Justice. The adult volunteers posed online as 13 or 14-year old children who were home alone and receptive to an in-person meeting with an adult whom they had met on the Internet. In his testimony to the Committee, Hansen described the online grooming process he observed and noted how quickly the predator would turn the conversation into one overtly sexual in nature. He also noted that the persons who were identified and arrested as a result of the series – at the time of the Committee hearing, 98 of whom had been charged criminally – defied characterisation. Concluding, Hansen told the Committee, 'They came from all walks of life and, upon meeting them, many did not seem particularly dangerous or suspicious'.[36]

The deletion of 29,000 sex offender profiles in recent weeks by MySpace was one development on several fronts. In January 2007 it was reported that the parents of five teenage girls who were sexually assaulted by men that had met on MySpace were suing the company, Rupert Murdoch's News Corporation, claiming compensation over allegations of negligence, fraud and misrepresentation.[37]

United Kingdom: In the United Kingdom, BBC News reported in May this year that an NSPCC poll found that '50.4% of 2,053 children had experienced problems such as bullying, being threatened or sexually harassed while online'. The child protection organisation was said to be concerned about the popularity of social networking sites such as Bebo or MySpace, which it said '52% of children aged 11-16 use once a day'. NSPCC director and chief executive Dame Mary Marsh commented that 'Children face real threats on the internet such as sexual grooming, cyber-bullying, exposure to violent, pornographic and other unsuitable material'.[38]

Around the same time an investigation undertaken by the *Sunday Times* in the UK reported that, 'Internet chatrooms run by Skype…have become a magnet for paedophiles and sexual

---

35 'MySpace: your kids' danger?' *CBS News*, 6 February 2006 - http://www.cbsnews.com/stories/2006/02/06/eveningnews/main1286130.shtml

36 US House of Representatives, A Staff Report prepared for the use of the Committee on Energy and Commerce, *Sexual Exploitation of Children over the Internet*, January 2007, p 21 - http://republicans.energycommerce.house.gov/108/News/01032007_Report.pdf

37 T Leonard, 'US parents sue MySpace over sex abuse cases', *Telegraph.co.uk*, 21 January 2007 -http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/01/20/wmyspace20.xml

38 'Web safety warning for children', *BBC News* 14 May 2007 - http://news.bbc.co.uk/1/hi/uk/6652585.stm

predators who want to groom children as young as 10 for sex'. The report went on to say that, during a two-week investigation, undercover investigative journalists

> posed online as children aged between 10 and 14. They were bombarded with sexually overt messages from adult men in Britain and overseas who wanted to meet children and asked them for pornographic images of themselves.[39]

Commenting on these findings, an article posted by Phil Wolff on *Skype Journal* observed 'The problems aren't simple. The solutions aren't obvious'. He explained:

> Skype isn't a bulletin board where moderators can watch for bad behavior. It's a private, encrypted, person-to-person phone system. So Skype's ability to intervene before something bad happens, or even to detect that something bad has already happened, are very limited. As Kurt Sauer, Skype's chief security officer, told the *Times*: 'This raises some very practical issues. However, we have not found a way to address each of the issues'.

The same article continued:

> The very efficiency of Skype's directory is what enabled the bad actors to locate their targets. Millions of people use that efficient white pages to find and talk with each other daily, allowing Skype Journal and other reporters (like the ones at the *Times*) to investigate stories all over the world. You don't want to cripple an entire network as a response. What can you do? What are your options? There are matters of call content. What do you do when the age of consent in one jurisdiction is 18 years' old and is 14 in another? When the definitions of predatory behavior, fraud, or snooping are different?[40]

4.3 How is grooming different online?

The grooming of minors for child sexual abuse purposes is nothing new. For example, the June 2000 report on Project AXIS by the Queensland Crime Commission and the Queensland Police Service contained detailed accounts of the offline grooming of minors for sexual contact.[41] However the Internet has opened new possibilities in this context, providing another means of targeting minors for the purposes of sexual exploitation. Some of the distinctive features of online grooming have been identified by Netsafe, the programme of New Zealand's Internet Safety Group as follows:

---

39 D Foggo, C Newell and M Foley, 'Paedophiles use Skype "loophole" to woo children', *Times Online* 6 May 2007 - http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article1752240.ece

40 P Wolff, 'UK: Paedophiles use Skype to find and pursue likely targets', *Skype Journal* 13 May 2007 - http://skypejournal.com/blog/2007/05/uk_paedophiles_use_skype_to_fi.html

41 Queensland Crime Commission and Queensland Police Service, *Project AXIS: Child Sexual Abuse in Queensland – the Nature and Extent*, June 2000, Chapter 5 - http://www.cmc.qld.gov.au/data/portal/00000005/content/67709001131403329213.pdf

- Online grooming can be faster. Many people mistakenly believe that they are anonymous online, and take greater and more frequent risks. People online often come to trust an online acquaintance more quickly than they would a person they have met face-to-face (offline). In addition, as online technologies speed up communication (especially emailing and texting), groomers have many more opportunities to interact with their victims.
- Groomers can combine their efforts to gain more information about their victims with searches of online databases, such as online phone books, profile searchers etc. Often victims of online grooming do not realise that the groomer already knows a lot of personal information about them that they found elsewhere online.
- Groomers can use online technologies such as images (pictures), videos, texts, email, voice transmission, viruses and Trojan programs to aid them in the grooming and abusing processes.
- It is very easy for an online groomer to mask their real identity, especially their age and gender. They can lie in what they type (or say) and also use pictures of other people and say they are images of themselves.
- Online grooming is usually a private interaction between the groomer and their victims, and is usually very secretive and hidden from other people. For example, if the groomer has the victim's mobile phone number they can easily communicate with the victim from a distance, with no one else ever seeing the victim and the groomer together. The groomer might even be in a different country to the victim.
- Online grooming does not have to adhere to the usual limitations of time and access. Victims can be groomed at all hours of the day and night, at home and at school. For lonely or isolated young people this perceived company/friendship might be very attractive.
- Online grooming allows groomers to be very specific and selective in the kind of person they want as a victim. For example, a groomer can select a victim by the way they look, or by their age, from a vast number of potential victims.
- Online groomers can groom a number of victims at the same time. In addition, if the victim rejects their advances, they can 'disappear', change their identity and reappear as 'someone else', and approach the same victim, but this time wiser to what that victim's limits and preferences are.

4.4 How do groomers find online victims?

Groomers can use many aspects of online technologies to find and choose their victims. The following is a list of *some* of the ways groomers select victims online, again as identified by NetSafe, the programme of new Zealand's Internet Safety Group:

- Groomers often search for victims in chatrooms, especially those 'chats' that are specifically focused around young people's interests (e.g. a teen chatroom, gaming forum, or music-themed chatroom).
- Groomers might pretend to be younger than they actually are, or of a different gender, especially if they want their victims to think that they might be a good potential friend or girl/boy friend. However, many groomers do not lie about their real age or gender at all, and still manage to find victims.
- Groomers might manipulate victims to contact them in the first instance. This can

sometimes make them look more innocent and trustworthy, and the victim as being more complicit in the grooming, for example:

'any girls out there who can tell me where to buy pink lip-gloss cheap?'

- Groomers might have online profiles on dating sites and other sites where people meet each other (e.g. penpal sites, newsgroups, gaming sites etc). These might be real or fictitious. Photos of other people can be easily used in place of their own.
- Groomers can hunt for potential victims by looking through personal websites. Examples of such sites include: blogs (online diaries), pictures, and sites that 'give out' personal information and pictures about young people, and some school and sporting club websites
- People with an interest in grooming victims online sometimes work together with other groomers and sex-offenders to help each other find and groom victims.
- Groomers often move between different cyber-technologies as they position themselves for abuse. For example, they might select a victim from a picture and profile they found online from a school website. They then might meet the victim in an open chatroom and then go into a private chatroom, where they start exchanging emails, messages, pictures and videos. After this, they might even send the victim a prepaid mobile phone that they can keep in secret to talk with the groomer.

4.5 A typology of online grooming practices

It is said that the basic technique adopted by online predators is to hang around in a public Internet chat room, on the look out for a child that seems 'vulnerable'. Ruben Rodriguez, director of the US National Centre for Missing and Exploited Children's Exploited Child Unit says that 'Predators like to go after kids who tend to express agreement in Chat Rooms but not say a lot because they know these kids are vulnerable', children that would perhaps really value attention, understanding and friendship. It is said that when the predator finds such a child they invite them into a private area of the chat room to get to know them better. In its submission to the UK Home Office, Childnet International went on to explain:

> Next in the grooming sequence comes private chat via an instant messaging service, and then email, phone conversations (often mobile phones) and finally a face-to-face meeting. The grooming process can go on for weeks and months, as it may take this long for the child to feel truly comfortable.[42]

Rachel O'Connell, who is Director of Research in the Cyberspace Research Unit at the University of Central Lancashire, has produced a typology of cybersexploitation and online grooming practices. The stages identified by O'Connell are as follows:

- victim selection stage;
- friendship forming stage;
- relationship forming stage;
- risk assessment stage;
- exclusivity stage; and

[42] Childnet International, *Online grooming and UK law* - http://www.childnet-int.org/downloads/online-grooming.pdf

- sexual stage.[43]

Basically, the picture to emerge is one where the online predator forms a relationship with a minor, a process that typically involves deception, with O'Connell observing that 'The level of duplicity engaged in by the adult means it is very difficult for a child to detect that firstly, they are not in fact talking to a child, and secondly to discover the true intentions of the adult'. This friendship and relationship forming stage will be interspersed with questions where the online predator tries to assess the likelihood of his activities being detected by the child's parents or older siblings. According to O'Connell the risk assessment stage is typically followed by the exclusivity stage where 'the tempo of the conversation changes so that the idea of "best friends" or "I understand what you're going through" and so you can speak to me about anything ideas are introduced into the conversation by the adult'. The idea of trust is introduced which 'often provides a useful means to introduce the next stage of the conversation, which focuses on issues of a more intimate and sexual nature'. While differences in conversational patterns occur at this sexual stage, O'Connell states that many revolve around masturbation. She concludes:

> Research findings indicate that this pattern of conversation is characteristic of an online relationship that may progress to a request for a face-to-face meeting and arguably most closely resembles the conduct the 'anti-grooming' legislation is designed to combat.[44]

4.6 Child pornography and grooming

A concern that is often expressed relates to the use of the Internet by paedophiles, to network[45] and for the exchange, selling and production of various forms of child pornography.[46] The dangers are real enough. In NSW, the Wood Royal Commission regarded the problem as of such potential importance that it dealt separately with it in its

---

43 For a discussion of this typology in the context of Queensland police sting operations see – T Krone, *Trends and Issues in Crime and Criminal Justice: No 301 – Queensland Police Sting Operations in Online Chat Rooms*, AIC, July 2005.

44 This overview is based on the submission of R O'Connell to the Justice 1 Committee of the Scottish Parliament, dated 26 January 2005 - http://www.scottish.parliament.uk/business/committees/justice1/reports-05/j1r05-05-vol02-01.htm See also R O'Connell, *A Typology of Cybersexploitation and Online Grooming Practices* - http://www.uclan.ac.uk/host/cru/docs/cru010.pdf

45 In the worst cases this can include networking on private chat rooms that enable 'members to watch sexual acts by a host with a child victim via a live video link on the Internet', as was the case in the US network known as the Orchid Club which was discovered by Californian police in 1996 – Queensland Crime Commission and Queensland Police Service, *Project AXIS: Child Sexual Abuse in Queensland – the Nature and Extent*, June 2000, p 103 - http://www.cmc.qld.gov.au/data/portal/00000005/content/67709001131403329213.pdf

46 US House of Representatives, A Staff Report prepared for the use of the Committee on Energy and Commerce, *Sexual Exploitation of Children over the Internet*, January 2007, p 21 - http://republicans.energycommerce.house.gov/108/News/01032007_Report.pdf

Final Report.[47] As of May 2006, Interpol had assisted in identifying and rescuing 426 victims of online child pornography from the 475,899 images it had collected in its database.[48]

As noted, this paper does not deal with the issue of child pornography in detail.[49] It is enough to note the specific claim that child pornography is used by online predators to 'groom' children. Tony Krone, in an Australian Institute of Criminology research paper published in July 2004, wrote in this respect:

> The online groomer is a person who has initiated online contact with a child with the intention of establishing a sexual relationship involving cyber sex or physical sex. Child pornography is used to 'groom' the child – it is shown to the child to lower that child's inhibitions concerning sexual activity.[50]

While this may indeed be the case, some of the research that is relied upon is not entirely convincing. For example, in a 2001 paper published by the National Child Protection Clearinghouse Janet Stanley wrote that 'Child pornography relayed through the Internet is "regularly" used as a means of desensitising children and normalising sexual activity between adults and children'.[51] Her source was a 1999 conference paper by Marni Feather of the Queensland Police Service which claimed that this conclusion was indicated by 'research'. However, the research in question was not identified.[52] In their June 2000 report the Queensland Crime Commission and Queensland Police Service reported: 'It is quite common for offenders to send children pornography, including child pornography, which is used to lower the child's inhibitions and to desensitise them to the behaviour'.[53] Their only

---

47 JRT Wood, *Royal Commission into the NSW Police Service: Final Report – Volume V, The Paedophile Inquiry*, August 1997, Chapter 16 'The Internet and Paedophile Activity'.

48 US House of Representatives, A Staff Report prepared for the use of the Committee on Energy and Commerce, n 36, p 10.

49 This paper does not define 'child pornography', nor does it consider whether some other term, such as 'child exploitation material' would be more appropriate.

50 T Krone, *Trends and Issues in Crime and Criminal Justice: No 279 -A typology of online child pornography offending*, AIC, July 2004 - http://www.aic.gov.au/publications/tandi2/tandi279t.html

51 J Stanley, *Child Abuse and the Internet*, Child Abuse Prevention Issues No 15 Summer 2001, National Child Protection Clearninghouse, p 5. See also J Stanley, 'Downtime for children on the Internet', Family Matters, No 65 Winter 2003 at 22. It is claimed (page 24) that some child sex offenders 'use child pornography to facilitate the seduction of new victims…'. The claim is not directly referenced.

52 M Feather, 'Internet and Child Victimisation', *Paper presented at the Children and Crime: Victims and Offenders Conference, Brisbane 17-18 June 1999*, p 6 - http://www.aic.gov.au/conferences/children/feather.pdf

53 Queensland Crime Commission and Queensland Police Service, *Project AXIS: Child Sexual Abuse in Queensland – the Nature and Extent*, June 2000, p 71 - http://www.cmc.qld.gov.au/data/portal/00000005/content/67709001131403329213.pdf

reference is to an article by Chuck Esposito, a Crimes Against Children detective in the Florida Police Department, which cites a police 'sting' where a 47 year old male flew into Florida to have sex with a fictitious 14-year old. The man had previously 'sent 21 pornographic images, including 19 depicting child pornography and one of himself naked from the waist down'. The article further stated that

> posing as a young teenager, either a boy or a girl, tends to be the most effective undercover operation. Not only will you receive child pornography, but you will find those predators who are interested in meeting children for sexual liaisons.[54]

As with many issues in this field, the specific subject of the use of child pornography (as opposed to other forms of pornography) by online predators for 'grooming' purposes is one that will benefit from further research.[55] It may be that the use or non-use of such material will vary considerably, between types or sub-sets of offenders, or on a more ad hoc or case-by-case basis depending on what an individual offender thinks will best achieve their ends in a particular instance.

---

54 C Esposito, 'Hunting predators on the Internet' (September 1997) 45(9) *Law and Order* 58-63.

55 Note that what constitutes 'child pornography' for legal purposes may differ from one jurisdiction to another. The term 'child pornography' is not used under Australia's National Classification Code. Instead, material is to be Refused Classification if it describes or depicts 'in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not)'. Under s 91H of the NSW *Crimes Act 1900* the production, dissemination or possession of 'child pornography' is an offence. Child pornography is defined to mean

'material that depicts or describes, in a manner that would in all the circumstances cause offence to reasonable persons, a person under (or apparently under) the age of 16 years:
(a) engaged in sexual activity, or
(b) in a sexual context, or
(c) as the victim of torture, cruelty or physical abuse (whether or not in a sexual context)'.

5. RESEARCH FINDINGS ON INTERNET SAFETY

Since the dangers of online usage were identified in the 1990s many jurisdictions, including Australia, have engaged in research projects to identify the scope and nature of the problems at issue. Worldwide, there is now a large body of statistical data available in this field. A selection of the more recent research findings is set out below, followed by a brief comment on these findings. The subjects of 'children and Internet safety' and 'parents and Internet safety' are dealt with separately.

5.1 Children and Internet safety

2002-03 – Cyberspace Research Unit, Young People's use of Chat Rooms: Implications for Policy Strategies and Programmes of Education:[56] The original study, published in 2002, was of 1369 children aged 9-16 years of age. Two later studies were also conducted, based on a sample of 1331 children aged 8-11 years (in 2002) and 330 children aged 8-11 years (in 2003). In an overview of the findings, Rachel O'Connell et al said that both studies from 2002 'revealed a striking consistency despite the disparity in terms of age ranges between the samples', with 19% of the children surveyed using online chat rooms regularly and 10% of chatters in both samples reporting attending face-to-face meetings. Other findings from the 2002-03 studies included:

- The proportion of children reporting using chat rooms regularly decreased in 2003, which found that only 12% of 330 children aged 8-11 reported using chat rooms. However, 26% of these reported attending face-to-face meetings.
- All three studies found that the majority of children that reported attending face-to-face meetings with people they had only ever previously met online also reported positive experiences of these meetings.
- However, two children from the sample of 8-11 year olds in 2002 and two from the sample of 9-16 year olds in 2002, who had attended face-to-face meetings, reported that they had experienced verbal abuse during the course of the meeting.
- One child from the sample of 9-16 year olds in 2002 reported experiencing physical abuse, but to what extent was not ascertained.[57]

2005 – Sonia Livingstone and Magdalena Bober, UK Children Online: The study is based on a national UK survey conducted face to face with 1,511 children and young people aged 9-19, together with a survey administered to 906 of their parents, plus a series of focus group interviews and observations focusing on children's use of the Internet.[58]

---

56 For the full text of the first 2002 study see - http://www.uclan.ac.uk/host/cru/docs/cru008.pdf

57 This account is based on the overview presented in R O'Connell, J Price and C Barrow, *Cyber Stalking, Abusive Cyber sex and Online Grooming: A Programme of Education for Teenagers*, Cyberspace Research Unit - http://www.aic.gov.au/topics/cybercrime/children.html

58 S Livingstone and M Bober, *UK Children Go Online: Final Report of Key Project Findings*, April 2005 - http://personal.lse.ac.uk/bober/UKCGOfinalReport.pdf

In a wide-ranging survey of Internet use and experience, which included the risks of exposure to undesirable content, it was found that:

- One third of children and young people report having received unwanted sexual (31%) or nasty comments (33%) via email, chat, instant messaging or text messaging.
- Parents underestimate their children's negative experiences online. Only 7% of parents think that their child has received sexual comments, and only 4% think that their child has been bullied online.
- Children and young people divulge personal information online, with 46% saying that they had given out such personal information as their hobbies (27%), email address (24%), full name (17%), age (17%) and phone number (7%) to someone they met on the Internet. By contrast, only 5% of parents think their child has given out such information.
- These risks increase for older children, rising from 25% for 9-11 year olds, to 45% for 12-15 year olds and 61% for 16-17 year olds.
- Some children and young people have attended face-to-face meetings, with 30% saying they had made an online acquaintance and 8% saying they had met with someone they had first met on the Internet. Most told someone they were going to the meeting (89%), with 67% taking a friend with them and 65% meeting someone their own age. 91% said the meeting was 'good' or 'okay'. 6% said the person they met turned out to be a different age to what they expected.
- For more skilled Internet users, risky online encounters increase with increased use. It is also the case that these young people are more likely to be able to deal with the risks.

2005 – NetAlert and Ninesmsm, Online safety for teens survey: The results of this Internet safety survey conducted by Nine*msm* and NetAlert Limited, Australia's Internet safety advisory body established in 1999 by the Australian Government to provide independent advice and education on managing access to online content, were released in summary form only, as a media release headed 'Parents and teens poles apart regarding online safety'. The report was said to have 'received 3,490 valid responses from parents and 8,918 valid responses from children as defined by Nielsen/Netratings'. Its most controversial and publicised finding was that '40% of teens would potentially meet in person someone they have "met" online and only 12% would ask their parents' permission to do so'.[59]

---

59 NetAlert Ltd and Ninemsm, ''Parents and teens poles apart regarding online safety', *Media Release*, 14 December 2005 - http://www.netalert.net.au/02799-Parents-and-Teens-Poles-Apart-Regarding-Online-Safety.asp This finding was referred to in K Burke, 'Here be monsters: parents navigate online security', *SMH*, 30-31 June 2007, p 4. The authors of this paper were advised by telephone on 12 July 2007 by the Australian Communications and Media Authority that the data for the research is not available publicly. The difficulty in these circumstances is that we are presented with controversial findings but none of the methodological hardware that produced them. We know how many children were surveyed, but not whether they were a self-selecting cohort or not, or to which exact age brackets they belonged. We are told that 8,918 valid responses were received 'from children as defined by Nielsen/Netratings'. We are not told what that means. What percentage of the 40% who said they would meet in person someone they have "met" online were in fact teenagers and what, if any, percentage belonged to a younger age bracket? What question or questions were they responding to? It seems further research is proposed.

2005 – NetRatings Australia Pty Ltd, Kidsonline@home: Internet use in Australian homes:[60] This study, released in April 2005, was prepared for the then Australian Broadcasting Authority and NetAlert Limited. The three-stage methodology used in the study is clearly set out: stage one comprising the analysis of existing data on online behaviours of children and adults; set two involving a national telephone survey among 502 children and their parents; and stage three comprising qualitative research in the form of discussion groups and in-depth interviews with parents and children. Defining the study's age demographic, all respondents to the national telephone survey were asked two preliminary screening questions: whether there was a child in the home aged between 8 and 13; and whether there was a home Internet connection. Note therefore that this study relates to children (8-13 year olds) not teenagers. The study's findings include:

- A significant proportion of adults (92%) and children (89%) mentioned at least one issue of concern in relation to children's use of the Internet. The issue of most concern reported by parents was online pornography (40%), followed by communicating with strangers online (22%). The most common issue of concern among children related to such Internet security issues as electronic viruses, hacker attacks and spyware. Violent Internet content was reported as a concern by very few parents and even fewer children (10% and 1% respectively).
- Despite the level of reported concern, two-thirds of parents reported that their children had *not* had a negative online experience at home. Children's reporting of their own negative experience is, on average, higher (40% of children reported no negative online experience).
- Children's likelihood of having experienced something negative online appears to increase with age. Almost half of 12 or 13 year olds (versus less than one-third of 8 or 9 year olds) had seen websites their parents would prefer them not to see.
- 27% of 12 or 13 year olds (versus 14% of 8 or 9 year olds) had received online messages from strangers. Half of these were 'spam' emails.
- 18% of 12 or 13 year olds (versus 8% of 8 or 9 year olds) had communicated online with people they did not know.
- Children using instant messaging were three times more likely to have communicated online with strangers (25%) than children who did not use the application (8%).

2007 – A Lenhart and M Madden, Teens, Privacy and Online Social Networks: How teens manage their online identities and personal information in the age of MySpace:[61] This research, sponsored by the Pew Internet and American Life Project, a non-partisan, non-profit research centre that examines the social impact of the Internet, was based on telephone interviews with a nationally representative call-back sample of 935 teens aged between 12 and 17 years old and their parents living in US households. Its findings included:

---

[60] The full text of the report is at - http://www.acma.gov.au/webwr/aba/about/recruitment/kidsonline.pdf

[61] The full text is at - http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf

- 55% of online teens have created a personal profile online, and 55% have used social networking sites like MySpace and Facebook.
- 66% of teens who have created a profile say that their profile is not visible by all Internet users. They limit access to their profiles.
- Older girls ages 15-17 are more likely to have used social networking sites and online profiles: 70% of older girls have used an online social network compared with 54% of older boys, and 70% of older girls have created an online profile, while only 57% of boys have done so.
- 91% of all social networking teens say they use sites to stay in touch with friends they see frequently, while 82% use the sites to make plans to stay in touch with friends they rarely see in person.
- 49% of social network users say they use the networks to make new friends.
- 32% of online teens have been contacted by strangers online – this could be any kind of online contact, not necessarily contact through social network sites.
- 21% of teens who have been contacted by strangers have engaged an online stranger to find out more information about that person (that translates to 7% of all online teens).
- 23% of teens who have been contacted by a stranger online say they felt scared or uncomfortable because of the online encounter (that translates to 7% of all online teens).

One of the questions the research sought to answer was whether teenagers are sharing information online that puts them at risk of victimization? The reports summary stated:

> Most teenagers are taking steps to protect themselves online from the most obvious areas of risk. The new Survey shows that many youth actively manage their personal information as they perform a balancing act between keeping some important pieces of information confined to their network of trusted friends and, at the same time, participating in a new, exciting process of creating content for their profiles and making new friends. Most teens believe some information seems acceptable – even desirable – to share, while other information needs to be protected.

The report went on to observe:

> Still, the survey also suggests that today's teens face potential risks associated with online life. Some 32% of online teenagers (and 43% of social networking teens) have been contacted online by complete strangers and 17% of online teens (31% of social networking teens) have 'friends' on their social network profile who they have never met.[62]

2006 – Teenage Research Limited, Teen Internet Safety Survey:[63] A survey

---

62 A Lenhart and M Madden, Teens, *Privacy and Online Social Networks: How teens manage their online identities and personal information in the age of MySpace*, pp i-ii.

63 For the text of the report see - http://www.netsmartz.org/pdf/cox_teensurvey_may2006.pdf

commissioned by Cox Communications,[64] the National Centre for Missing and Exploited Children (NCMEC) and children's advocate John Walsh found that teen Internet usage and attitudes about safety present potential risks but also opportunities for education and a role for watchful parents and guardians. The research was based on a national survey of 1,000 US teenagers ages 13-17. The findings on 'online behaviour' included:

- Teens have established significant presence on social networking web pages: 61% of 13- to 17-year-olds have a personal profile on a site such as MySpace, Friendster, or Xanga. Half have also posted pictures of themselves online.
- Older teens (16-17s) and girls especially use the Internet for social interaction, meeting friends and networking.
- However, many have also been exposed to the Internet's accompanying potential risks.
- 71% reported receiving messages online from someone they don't know.
- 45% have been asked for personal information by someone they don't know.
- 30% have considered meeting someone that they've only talked to online
- 14% have actually met a person face-to-face they they've only spoken to over the Internet (9% of 13-15s; 22% of 16-17s).
- When teens receive messages online from someone they don't know, 40% reported that they'll usually reply and chat with that person.
- Only 18% said they'll tell an adult.

As for 'perceptions of Internet safety', the findings included:

- 20% of teens report that it is safe (i.e. 'somewhat' or 'very safe') to share personal information on a public blog or networking site.
- As well, 37% of 13- to 17-year-olds said they are 'not very concerned' or 'not at all concerned' about someone using information they've posted online in ways they don't want.

March 2007 – Cox Communications, Teen Internet Safety Survey, Wave II:[65] Follow up research was undertaken in March 2007 by Cox Communications, with the following results:

- The number of teens with profiles on such social networking sites as MySpace and Friendster was up 10% to 71%.
- It remains routine for youth to receive personal messages online from someone they

64 Cox Communications is a wholly-privately owned subsidiary of Cox Enterprises providing digital cable television and telecommunications services in the United States. It is the fourth-largest cable television provider in the United States, serving more than 6.7 million customers, including 2.7 million digital cable subscribers, 3.1 million Internet subscribers, and 1.7 million digital telephone subscribers - http://en.wikipedia.org/wiki/Cox_Communications

65 For the full text of the report see - http://www.cox.com/TakeCharge/includes/docs/survey_results_2007.ppt

don't know (69%).
- 19% of teens reported they'd been harassed or bullied online.
- However, in 2007 16% of teens said they'd considered meeting someone they'd talked to online (down from 30% in 2006).
- Similarly, in 2007 8% reported they'd actually met someone they knew online (down from 14% in 2006).
- In 2007 more teens ignore messages from someone they don't know (up to 57% from 47%), while 31% (down from 40%) say they reply and chat, and 60% (down from 72%) only respond to ask who the person is.

2006 – J Wolak, K Mitchell and D Finkelhor, Online Victimization of Youth: Five Years Later: Produced in cooperation with the US Department of Justice's Office of Juvenile Justice and Delinquency Prevention, NCMEC and University of New Hampshire's Crimes Against Children Research Center, this second national survey of 1,500 youth aged 10 to 17 documented their use of the Internet and experiences while online including unwanted exposure to sexual solicitation, sexual material, and harassment. The 2006 report is referred to as YISS-2; YISS-1 refers to the original study released in 1999.

- In YISS-2, compared to YISS-1, increased proportions of youth Internet users were encountering unwanted exposures to sexual material and online harassment, but decreased proportions were receiving unwanted sexual solicitations.
- In YISS-2 more than one-third of youth Internet users (34%) saw sexual material online they did not want to see in the past year compared to one quarter (25%) in YISS-1.
- The increase in exposure to unwanted sexual material occurred despite increased use of filtering, blocking, and monitoring software in households of youth Internet users. More than half of parents and guardians with home Internet access (55%) said there was such software on the computers their children used compared to one-third (33%) in YISS-1.
- Online harassment also increased to 9% of youth Internet users in YISS-2 from 6% in YISS-1.
- A smaller proportion of youth Internet users received unwanted sexual solicitations in YISS-2 than in YISS-1. Approximately 1 in 7 (13%) was solicited in YISS-2, compared to approximately 1 in 5 (19%) in YISS-1;
- However, aggressive solicitations, in which solicitors made or attempted to make offline contact with youth, did not decline. Four (4) percent of youth Internet users received aggressive solicitations — a proportion similar to the 3% who received aggressive solicitations in YISS-1.
- In YISS-2 there were declines in the proportions of youth Internet users who communicated online with people they did not know in person (34% down from 40% in YISS-1) or who formed close online relationships with people they met online (11% down from 16%).
- Four (4) percent of all youth Internet users in YISS-2 said online solicitors asked them for nude or sexually explicit photographs of themselves.
- As in YISS-1 only a minority of youth who had unwanted sexual solicitations, unwanted exposures to sexual material, or harassment said they were distressed by the incidents. The number of youth with distressing exposures to unwanted sexual

material increased to 9% of all youth in YISS-2 from 6% in YISS-1.

- Acquaintances played a growing role in many of the unwanted solicitation incidents. In YISS-2, 14% of solicitations were from offline friends and acquaintances compared to only 3% in YISS-1. The same was true of harassers. Forty-four (44) percent were offline acquaintances, mostly peers, compared to 28% in YISS-1. In addition a portion of these unwanted incidents happened when youth were using the Internet in the company of peers — 41% of solicitations, 29% of exposures, and 31% of harassment.
- As in YISS-1 few overall incidents of solicitation or unwanted exposure (5% and 2% respectively in YISS-2 and 9% and 3% respectively in YISS-1) were reported to law enforcement, Internet service providers, or other authorities.[66]

An important finding was that 90% of the sexual solicitation happened to youth ages 13 and older. This was said to reinforce what previous research has found – online sexual solicitations to youth are concentrated among teenage Internet users. The report commented:

> Research based on interviews with law enforcement about Internet-related sex crimes similarly found sex offenders who met their victims online largely sought out young teenagers, and rarely used deceit or violence. Rather they appealed to adolescents' interest in romance and sex…Internet safety programs need to take this into account and make sure they are targeting the appropriate audience and giving them accurate information.[67]

The previous research, also conducted by Janis Wolak, David Finkelhor and Kimberly Mitchell, had found that victims in Internet-initiated sex crimes were primarily 13-15 year old teenage girls (75%) who met adult offenders (76% older than 25) in Internet chat rooms. The research involved a national survey of a stratified random sample of 2574 law enforcement agencies conducted between October 2001 and July 2002. Telephone interviews were conducted with local, State and federal law enforcement investigators concerning 129 sexual offences against juvenile victims that originated with online encounters. Most offenders did not deceive their victims about the fact that they were adults who were interested in sexual relationships. Most victims met and had sex with then adults on more than one occasion. Half of the victims were described as being in love with or feeling close bonds with the offenders. Almost all cases with male victims involved male offenders. Further, in all cases offenders used violence in 5% of the episodes.[68]

---

66 This summary of the report's statistical findings is at - http://www.netsmartz.org/safety/statistics.htm The full text of the report is at - http://www.missingkids.com/en_US/publications/NC167.pdf

67 J Wolak, K Mitchell and D Finkelhor, *Online Victimization of Youth: Five Years Later,* p 24. Reference was made to an earlier study – J Wolak et al, 'Internet-initiated sex crimes against minors: implications for prevention based on findings from a national study' (2004) 35(5) *Journal of Adolescent Health* 424.

68 J Wolak et al, 'Internet-initiated sex crimes against minors: implications for prevention based on findings from a national study' (2004) 35(5) *Journal of Adolescent Health* 424 - http://www.unh.edu/ccrc/pdf/CV71.pdf

The 2006 report also commented on the 'considerable degree of peer involvement in unwanted sexual solicitations'. Of the 14% of solicitors youth knew in person, 82% of these were other youth, age 17 or younger. There was also the finding that 41% of incidents of unwanted solicitations happened where recipients were with friends or other peers. The report commented:

> This is an area of online dynamics we know little about. It may be that some youth tend to ignore Internet safety guidelines when they are in groups. They may be more likely to do things such as going to questionable chatrooms or engaging in risqué conversations with people they know only online, situations in which solicitations may be more likely to occur. We need to learn more about sexual solicitations between known peers and those that happen when youth use the Internet together in groups and fashion prevention messages aimed at these situations.[69]

The portrait to emerge from these studies by Wolak and others is a complex one where dangers exist online for minors but not always from the stereotypical sources identified with middle-aged male peadophiles. Around a quarter of the sex offenders identified in the 2004 study were under 26 years of age. Nonetheless, conforming more to type, 47% were more than 20 years older than their victims.

In their 2004 study Wolak et al observed in this context:

> The prevalent image of Internet sex crimes against minors is of strangers who are pedophiles and who deceive and lure unsuspecting children, frequently over long distances, into situations where they can be forcibly abducted or sexually assaulted.

The study suggested that the 'predominant scenario' needs to be revised in at least four ways:

- First, 'offenders in these crimes do not appear to be pedophiles. Pedophilia is a sexual deviation involving sexual attraction to prepubescent children. The victims in these cases were young adolescents. Ninety-nine percent were age 13 to 17, and none were younger than 12'.[70]

---

69 J Wolak, K Mitchell and D Finkelhor, *Online Victimization of Youth: Five Years Later,* p 24.

70 The diagnostic criteria for a 'paedophile' according to the American Psychiatric Association's Diagnostic and Statistical Manual of Mental Disorders (DSM) include: 'Over a period of at least 6 months, a recurrent, intense sexually arousing fantasies, sexual urges, or behaviours involving sexual activity with a prepubescent child or children (generally aged 13 years or younger)'. Different definitions of 'paedophile', from clinical, legal and other perspectives, were discussed in - JRT Wood, *Royal Commission into the NSW Police Service: Final Report – Volume IV, The Paedophile Inquiry*, August 1997, Chapter 1. The report adopted a 'socio-legal definition' which takes 'paedophiles' to mean 'those adults who act on their sexual preference or urge for children, in a manner which is contrary to the criminal laws of the State of New South Wales. Within this context, a child is a person who is below the relevant age of consent for the activity involved' (page 578). The report continues: 'This definition encompasses child sexual abuse both within the family and external to the family. It includes those offenders whose primary and sexual preference is

- Second, the offenders do 'not generally deceive victims about being older adults who were interested in sexual relationships. Victims usually knew this before their first face-to-face encounters with offenders'.
- Third, with a 'few frightening and dangerous exceptions, the majority of offenders did not use force or coercion to sexually abuse their victims and did not abduct them'.
- Fourth, 'it is misleading to characterize the offenders in these cases as "strangers" to their victims, because in most cases they had communicated extensively with victims, both online and off before they actually met in person'.[71]

2007 – European Commission, Directorate-General Information Society and Media, Safer Internet For Children – Qualitative Study in 29 European Countries: This qualitative study, published in May 2007, covered all 27 European Union member states, as well as Iceland and Norway. It was commissioned by the Directorate-General Information Society and Media and was carried out by the opinion research agency OPTEM and its European partners. The study, which involved children between 9 and 10 and 12 and 14 years old, was based on discussion groups, with a total of around 30 children from each country divided along age and sex lines into four groups. All participants had access to the Internet.

It was reported that in all countries it was the uses that imply the possibility of contact with adult strangers that are deemed to be the most 'risky'. Taking part in open chats/discussion forums were perceived as the most risky since this activity 'is the most conducive to a possible contact with malicious or dangerous adults'. Against this, the children said they know how to protect themselves. On closer investigation, however, when presented with a possible 'grooming' scenario, it emerged that certain children adopt more risky behaviour than they say and think. This was found to be particularly true of older youngsters 'who can show themselves to be too confident both in their own insight in unmasking false identities and interlocutors who they find especially friendly towards them – and they are reluctant to warn their parents (or only in the last resort)'.[72]

This research forms part of ongoing EU funded research in this field, conducted under the auspices of the European Commission for Information Society and Media. A fact sheet published in February 2007 reported that:

> A survey from 2003 showed that 40% of children said that people they had only met online asked to meet them in person. In 2006 22% of them actually met the

---

for children (preferential or fixated offenders), and those who act on an urge to sexually interact with a child even though their primary orientation is towards adults (situational or regressed offenders)' (page 615).

71 J Wolak et al, n 68.

72 For the text of the Summary Report see - http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/qualitative_study_2007/summary_report_en.pdf

> person – 51% of them never told their parents or teachers about this.[73]

This finding can be set alongside the that of the SAFT survey in Norway and Ireland which found that in 2006, children were more critical of the Internet and gave out less personal information than in 2003.[74]

5.2 Comment on research findings – children and Internet safety

While a significant body of research exists in this field, it is still very much a work in progress. That the use of social networking sites such as MySapce is prevalent among teenagers is agreed, as is the fact that potential dangers exist where minors, teenage girls in particular, are contacted by strangers online. European research suggests that some teenagers may be over confident of their ability to control risky behaviour. However, there is also evidence to indicate that young people are becoming more wary about divulging personal information online. In a similar vein, United States research suggests that teenagers are taking steps to protect their online identities and that they are becoming less inclined to meet someone they have met online (down to 16% in 2007 from 30% a year earlier according to the latest Cox Communications study). Likewise, in 2007 8% reported they'd actually met someone they knew online (down from 14% in 2006). In their 2006 study, Wolak et al reported that the number of unwanted sexual solicitations was also down, from 19% in 1999 to 13% in 2006. What seems to have remained more constant according to the same source are the number of teenagers who see sexual material online they did not want to see (34%), as well as the rate of aggressive solicitations online (4%). However, not all these unwanted online encounters necessarily come from strangers. A further factor to consider is that many teenagers seem to engage in more risky online behaviour in group situations, presumably where peer pressure 'dares' and the like are greatest. The research suggests that the world of online grooming is a complex place. Netsafe, the programme of New Zealand's Internet Safety Group, commented in this respect:

> Although many groomers do pretend to be younger or of a different gender, research suggests that the majority do not lie at all about themselves and what their intentions are, that is to be sexual with a child (sexually abuse them). It might come as a surprise that these overt groomers still manage to find quite a number of victims online to abuse. In addition, sometimes younger people can groom victims who are younger than themselves, are around their own age, or are even older that they are.[75]

---

73 European Commission Information Society and Media, *Fact sheet 18 – making the Internet a safer place* , 2 February 2007 - http://ec.europa.eu/information_society/doc/factsheets/018-saferinternetplus.pdf It is reported that in 2003 14% of the children surveyed actually met their online acquaitance person, but only 4% of parents were aware of this. But note that the 2003 survey itself was not located – European Commission, Safer Internet Plus, *Factsheet 18 - Making the Internet a Safer Place*, September 2004.

74 *Launch of EU Kids Online*, 6 February 2007 - http://blog.eun.org/SID2007/2007/02/launch_of_eu_kids_online.html

75 Netsafe, The Internet Safety Group -

The sharp end of the issue is where online sexual solicitation results in an actual or attempted real life sexual encounter. As discussed above, the research indicates that the most at risk from online grooming are teenage girls who become 'romantically' involved with those they meet on social networking systems. However, more research needs to be undertaken in this field, across jurisdictions, to gain a broader and truer picture of the risks involved to all minors.

5.3 Research findings – parents and Internet safety

Several of the research projects into children's use of the Internet are also concerned to study parental views and perceptions about online dangers.[76] Measures taken by parents to combat these perceived dangers have also been studied.

Australia: A case in point is the 2005 *Kidsonline@home* study, commissioned by then Australian Broadcasting Authority and NetAlert Ltd, which presented findings on[77]

- ***parents' concerns*** - the issue of most concern reported by parents was online pornography (40%), followed by communicating with strangers online (22%);
- ***parents' perceptions of children's experiences*** – two-thirds of parents reported that their children had *not* had a negative online experience at home;
- ***parents' perceptions and children's reporting*** – however parents may not be aware of their children's online experiences in the home. In 32% of households, children reported that they had experienced something 'negative' online, while the parent did not;
- ***parents' responses*** – only 9% of parents installed content filtering software for the first time in response to their child having negative online experience. 8% installed a new brand of filtering software and a similar proportion (8%) educated their child on how to use the Internet more safely. 6% said they began to participate in their child's Internet use;
- ***parental involvement*** – this includes supervision of Internet activity and the setting of rules for online behaviour. 67% of parents reported supervising their child's Internet use, while the proportion of children who say that their parents were supervising their online activities was notably less. The parental supervision that does occur also decreases as their child's age increases. A majority of parents reported setting rules on their child's access to particular websites and on the online activities their child may undertake (73% and 80% respectively). 15% of parents prohibited the use of chat rooms and a further 13% limited the way chat rooms or instant messaging were used. 35% of parents reported using software to filter inappropriate websites; and
- ***parental demand for information*** – both parents and children displayed high levels

---

http://www.netsafe.theoutfitgroup.co.nz/offenders/myths_and_misunderstandings_about_online_grooming.aspx

[76] The word 'parents' is generally used here to denote parents/carers/guardians.

[77] NetRatings Australia Pty Ltd, *kidsonline@home: Internet use in Australian homes,* Australian Broadcasting Authority and NetAlert, Sydney, April 2005.

of interest in obtaining Internet safety information. Almost four out of five parents expressed interest in learning more about how to make a complaint about something they had seen online, and almost three-quarters wanted information to help educate their children about Internet safety.

United States: A 2005 survey commissioned by Cox Communications and NCMEC, *Parents' Internet Monitoring Study*, based on a national telephone survey conducted among 503 parents of teenagers,[78] found that

- Over half (51%) of parents either do not have or do not know if they have software on their computer(s) that monitors where their teenager(s) go online and with whom they interact.
- 42% of parents do not review the content of what their teenager(s) read and/or type in chat rooms or via Instant Messaging.
- Teenagers who Instant Message use chat lingo to communicate and parents don't know the meanings of some of the most commonly used phrases. 57% don't know LOL (Laughing Out Loud), 68% don't know BRB (Be Right Back), and 92% don't know A/S/L (Age/Sex/Location).
- 95% of parents couldn't identify common chat room lingo that teenagers use to warn people they're chatting with that their parents are watching. Those phrases are POS (Parent Over Shoulder) and P911 (Parent Alert).
- Nearly three out of 10 (28%) of parents don't know or are not sure if their teens talk to strangers online.
- 30% of parents allow their teenagers to use the computer in private areas of the house such as a bedroom or a home office. Parents say they are more vigilant about where their teen(s) go online if the computer is in a public area of the household.
- 58% of parents surveyed say they review the content of what their teenager(s) read and/or type in chat rooms or via Instant Messaging; 42% do not.

The 2006 *Teen Internet Safety Survey* commissioned by Cox Communications and NCMEC[79] found that:

- 33% of 13- to- 17-year-olds reported that their parents or guardians know 'very little' or 'nothing' about what they do on the Internet. 48% of 16-17s said their parents or guardians know 'very little' or 'nothing';
- 22% of those surveyed reported their parents or guardians have never discussed Internet safety with them.
- On the other hand, 36% of youth—girls and younger teens most notably—said that their parents or guardians have talked to them 'a lot' about online safety, and 70% said their parents or guardians have discussed the subject with them during the past year.

---

78 Ketchum Global Research Network, *Parents' Internet Monitoring Study*, National Center for Missing & Exploited Children and Cox Communications, 2005 - http://www.cox.com/takecharge/includes/docs/results.pdf

79 For the text of the report see - http://www.netsmartz.org/pdf/cox_teensurvey_may2006.pdf

- Fewer teens whose families have talked to them 'a lot' about online safety have an Instant Messaging name or pictures of themselves on the Internet, compared to children whose families have not talked to them at all. More teens who have talked to parents or guardians also ignore messages from unfamiliar people, refuse to reply or chat, block unknown senders, and report these occurrences to trusted adults.

The 2006 *Online Victimization of Youth: Five Years Later* report (referred to above as YISS-2)[80] found that:

- 90% of parents and guardians were very or extremely concerned about their children being exposed to sexually explicit content on the Internet.
- 88% said they had talked to their children about giving our personal information online.
- 86% said they had also spoken with their children about the dangers of chatting online with people they do not know in person.
- On the other hand a smaller proportion (around 50%) of youth acknowledged hearing these types of prevention messages.
- Since 34% of youth surveyed revealed unwanted exposure to sexual material, the researchers were surprised to find a rise (from 33% in YISS –1 to 55% in YISS-2) in the number of parents who said there was software on their children's computers to filter or block X-rated sites or monitor their children's behaviour online.
- Such software was used by 48% of parents that monitored or controlled how their child used the Internet in other ways.
- The proportion of parents who said they knew where to report unwanted Internet experiences had increased (from 31% in YISS-1 to 35% in YISS –2). However, most of these parents (68%) could not name a specific reporting place.

***UK and European research*:** The 2005 report, *UK Chiildren Go Online*, found that 10% of UK parents said they did not know what their child do on the Internet, with 18% saying they did not know how to help their child use the Internet safely. Other findings included:

- ***Parents had ambivalent views about the Internet*** - they were concerned that it may lead children to risk their privacy (90%), and expose them to sexual (89%) and/or violent images (77%), or lead them to become isolated from others (59%). On the other hand, 73% believed that the Internet could help with their child's schooling and other worthwhile activities.
- ***Children don't want restrictions*** - 69% of 9-17 year olds said they objected to their parents restricting or monitoring their Internet use. Children also protect their privacy from parents, with 63% of 12-19 year old home Internet users hiding their online activities from parents.
- ***Filtering*** - in homes with Internet access, 35% of children said that filtering software had been installed on their computer, while 46% of parents claimed this. 23% of parents said they did not know if a filter was installed.

The same report noted the findings of the 2003 *SAFT* survey that parents across Europe

[80] The full text of the report is at - http://www.missingkids.com/en_US/publications/NC167.pdf

claim to monitor their children's Internet use more than children acknowledge. 20% of parents said they talk with their child about what he/she does online a great deal, but only 12% of 9-16 year olds agree. 20% of parents said they often sit with their child at the computer while only 3% of 9-16 year olds confirm this.[81]

The 2006 Eurobarometer survey, *Safer Internet*,[82] is part of an ongoing survey of European parents into issues of Internet safety. Questions about the use of the Internet were asked of 3,791 parents and carers whose child use the Internet. Its findings show large variation across countries:

- 18% European parents/carers believe their child (under 18) has encountered harmful or illegal content on the Internet.
- British parents are less likely to believe this than parents in Denmark, the Netherlands or Sweden, or those in Poland or Slovenia – possibly those most advanced in and those newest to the Internet have the greatest concerns.
- From comparing three very different countries, it seems British parents claim to regulate their children's use of Internet more: 62% of UK parents have rules about not giving out personal information online, but only 35% of Polish parents and 14% of Portuguese parents do so.
- Paradoxically, UK parents also seem to have more confidence in their children: 75% thought that their children would know what to do if a situation on the Internet made them feel uncomfortable (figures for Poland and Portugal are 56% and 48%).
- Possibly, safety awareness raising efforts in the UK have been more effective than in some other countries, as these have been coordinated across multiple stakeholders (government, child protection, industry, parenting organisations, etc).[83]

5.4 Comment on research findings – parents and Internet safety

The main findings are that parents know less than their children about the online environment and that the Internet is a cause of anxiety for many parents. Their response to this anxiety varies, with a growing number seemingly using filtering software of some kind and many setting rules for Internet use. That practices and perceptions may vary from one country to another is to be expected, in response to different levels of technological development, public education campaigns and other factors. Nor is it so unexpected to find that perceptions differ between parents and children, concerning the scope and nature of parental supervision and intervention, but also about online dangers. Parents want to be seen to be doing the right thing; teenagers are intent on establishing their independence and

---

81 S Livingstone and M Bober, *UK Children Go Online: Final Report of Key Project Findings*, April 2005, p 25 - http://personal.lse.ac.uk/bober/UKCGOfinalReport.pdf

82 For the text of the report see - http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf

83 *Launch of EU Kids Online*, 6 February 2007 - http://blog.eun.org/SID2007/2007/02/launch_of_eu_kids_online.html

guarding their privacy. Indeed, there is a general sense that many parents and children are reporting on parallel realities where online issues are concerned. In light of such factors, Professor Sonia Livingstone suggests that:

> Directing more safety awareness at children themselves may be the best way forward, since parents often don't know what their children are doing online.[84]

That is not to say that government should ignore parents in this context, either in terms of making filtering software more readily available or when designing more general educational initiatives. There is also the consideration that the gulf in technological know-how may tend to decrease as the youngsters of today become the parents of tomorrow. Be that as it may, the need for ongoing research in this field is clear enough.

[84] *Launch of EU Kids Online*, 6 February 2007 - http://blog.eun.org/SID2007/2007/02/launch_of_eu_kids_online.html

6. THE LEGAL FRAMEWORK IN AUSTRALIA AND OVERSEAS

6.1 The relevant Cyberlaw

The challenges posed by the Internet have resulted in the passing of laws on a number of related fronts, for the regulation of content on one side, to laws more directly focused on the problems of 'grooming' and the like. Relevant, too, are sex offender registration laws which may be adapted to combat perceived threats to minors online. These more general and specific developments are reviewed in the context of Australia and the United States. The overview of legal developments in the Canada, New Zealand and the United Kingdom focuses more directly on anti-grooming and related laws.

6.2 The age of consent

A threshold question in any debate about child sexual abuse relates to the age of consent. This varies from one jurisdiction to another, potentially a significant factor where the crimes at issue may be 'international' in character, calling for cooperation between police forces across national boundaries. In effect, what might constitute child sexual abuse in one jurisdiction may not in do so in another. A world wide summary is found at http://www.avert.org/aofconsent.htm

In most Australian jurisdictions, including ***NSW***, the age of consent is 16. The exceptions are South Australia and Tasmania where it is 17. Certain variations also apply within jurisdictions. For example, in NSW it is an offence to engage in or to attempt to engage in sexual intercourse with a person under the age of 18 if that person is under the care of the offender.[85]

Subject to similar variations, in ***Europe*** the age of consent varies from a low of 13 in Spain, to 14 (Italy, Hungary, Austria, Croatia, Serbia), 15 (France, Denmark, Sweden, Poland), 16 (England and Wales, Netherlands, Germany) and 17 (Northern Ireland).

Similar differences and exceptions apply in North America. In ***Canada*** the age of consent is 14. However, the Criminal Code provides a 'close in age' or 'peer group' exception, so that a 12 or 13 year old can consent to engage in sexual activity with another person who is less than two years older and with whom there is no relationship of trust, authority or dependency. The age of consent rises to 18 where the sexual activity involves exploitative activity, such as prostitution, pornography or where there is a relationship of trust, authority or dependency. This last exception was introduced by Bill C-2, Protection of Children and Other Vulnerable Persons, which passed in July 2005.[86] In the ***United States***, the picture is again complex, with the general age of consent varying between 16 (eg, Alabama, Connecticut, Georgia,), 17 (eg, New Mexico, New York, Texas) and 18 (eg, California, Arizona, Oregon).

---

85 *Crimes Act 1900*, s 73 (NSW). Note that Queensland has a 'sodomy law' (s 208 of the Criminal Code) meaning the legal age of consent for anal intercourse is 18 and vaginal intercourse 16.

86 http://canadajustice.ca/en/dept/clp/faq.html

6.3 Australia – Internet content laws

Legal responses to the perceived dangers posed to children by the new technologies have been many and varied in nature. Anti-grooming laws focus on the individual offender and these are considered later. Another level of regulation targets the online industry itself, establishing a co-regulatory scheme that seeks to control the content of online material that can be accessed by young people. The law relating to Internet content is discussed briefly, to offer a broader picture of the governmental response to the online environment.

Commonwealth – Internet content laws: At the Commonwealth level, Internet content regulation is based on Schedule 5 (and now Schedule 7) of the *Broadcasting Services Act 1992* (Cth). Schedule 5, which came into effect on 1 January 2000, established a co-operative regulatory scheme, between Government and industry, administered by the Australian Communications and Media Authority [ACMA]. The scheme, as first introduced, was restricted to the regulation of ***Internet Service Providers (ISPs) and Internet Content Hosts (ICHs)***.[87] Provision was made for the development of industry codes of practice, the most recent of which were approved in May 2005. Among other things, these codes of practice require ISPs and ICHs to assist parents to supervise and control children's access to Internet content. In respect to such content, the classification system used for films and computer games was applied.

A revised framework was introduced by the *Communications Legislation Amendment (Content Services) Act 2007*.[88] The major difference is that under this new scheme ISPs are still regulated under Schedule 5 whereas content hosts are now regulated under the new Schedule 7, which is headed 'Content Services'. Basically, the purpose of this legislation is to deal with the challenges posed by the new convergent technologies, such as broadband services to mobile handsets, by extending the coverage of the Internet content laws beyond material 'stored'[89] on the Internet to include 'live' or ephemeral convergent content services. This last category includes streamed audiovisual material and interactive chat services. Schedule 7 regulates '***content service providers***', a term that is defined broadly to include 'a service that allows end-users to access content using a carriage service'.[90] The development of industry codes is again provided for, in a scheme that is co-regulatory in nature.

In summary, a complaints based system is established by which a person may make a

---

87 An 'internet service provider' is a person who 'supplies, or proposes to supply, an Internet carriage service to the public' – *Broadcasting Services Act 1992*, Schedule 5, cl 8.

88 Assented to on 20 July 2007. As at 1 August 2007 the substantive provision had not been proclaimed to commence. Schedule 1, Parts 1 and 2 are due to commence in any event 6 months from the Act's Royal Assent; Schedule 2 is due to commence in any event 12 months from the Act's Royal Assent.

89 This refers to content kept on a data storage device.

90 Various exceptions apply, including for an 'exempt parliamentary content service' and a licensed free-to-air broadcasting service.

complaint to the ACMA about ***prohibited content***, or ***potential prohibited content***.[91] In response to a complaint about a content service provider with an 'Australian connection',[92] the ACMA may:

- in the case of a hosting service – issue a take-down notice;
- in the case of a live content service – issue a service cessation notice;
- in the case of a links service – issue a link-deletion notice.

Content is prohibited content if:

- it has been classified 'RC' or 'X 18+'; or if it has been classified 'R18+' and access is not subject to a 'restricted access system'; or
- it has been classified 'MA 15+', access is not subject to a 'restricted access system', the content does not consist of text and/or one or more still visual images and the content is provided by a commercial service. In other words, this would apply to a film or computer game classified 'MA 15+'; or
- it has been classified 'MA 15+', access is not subject to a 'restricted access system' and the content is provided by a mobile premium service.

The background to Schedule 7, including the challenges posed by the new convergent technologies, is discussed in detail in the Explanatory Memorandum to the Bill, as is its proposed mode of operation. It is said that:

> The new framework imposes obligations on content providers that supply content services to ensure that they are provided in a manner which is not likely to result in children being exposed to material that would be likely to offend a reasonable adult. Service providers who do no more than provide a carriage service that enables content to be accessed or delivered [that is, ISPs] are excluded from the regime.[93]

The Explanatory Memorandum again explains:

> The second objective, which is again focussed on children, is that service providers should be required to establish safety measures to address the potential misuse of certain new services for the purpose of making inappropriate contact. In so doing, the framework recognises the important role of consumer education in promoting

---

91 This relates to publications which, if they were classified, there is a substantial likelihood that the content would be prohibited content (that is, 'RC', category 2 restricted or category 1).

92 This is defined by *Communications Legislation Amendment (Content Services) Act 2007,* Schedule1, cl.3.

93 *Explanatory Memorandum, Communications Legislation Amendment (Content Services) Bill 2007*, p 1. As noted, it is reported that ISPs will be required to filter web content at the request of parents: P Coorey, 'Veto for parents on web content', *SMH*, 10 August 2007, p 1

> safe use in the modern communications environment.[94]

In essence, adult chat services and the like which have an 'Australian connection' are able to operate under Schedule 7, but subject to a requirement for age verification. Chat services that are sexually explicit in nature therefore, as defined by the various classification standards, are not to be directly accessible to minors. It remains the case, however, that the direct regulation of 'grooming' related activities is dealt with under the provisions of the Commonwealth Criminal Code, as discussed below.

States/Territories – Internet content laws: As first introduced in 2000 and revised in 2007, the Commonwealth scheme under Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth) does not preclude the States and Territories from passing concurrent legislation in this field. To this end, some jurisdictions, notably Victoria,[95] South Australia,[96] Western Australia[97] and the Northern Territory,[98] have inserted specific provisions dealing with online services into their classification legislation.[99]

A similar course was followed in New South Wales, with the *Classification (Publications, Films and Computer Games) Enforcement Amendment Act 2001* (NSW) inserting Part 5A 'On-line services' into the classification regime. Part 5A creates two offences relating to the production of Internet content: (a) knowingly or recklessly 'making available or supplying objectionable matter on on-line service' (s 45C), by which is meant 'RC' or 'X 18+' material; and (b) knowingly or recklessly 'making available or supplying matter unsuitable for minors on on-line service' (s 45D), by which is meant 'R 18+' material. Section 45D(1) provides:

> (1) A person must not, by means of an on-line service, make available, or supply, to another person, any matter unsuitable for minors:
>
> (a) knowing that it is matter unsuitable for minors, or
>
> (b) being reckless as to whether it is matter unsuitable for minors.

It is a defence that the matter was 'subject to an approved restricted access system', by which is meant a filtering system as defined under the Commonwealth broadcasting legislation. This provision appears to have been drafted with some aspects of online grooming in mind. In answer to a question without notice on 25 October 2001, the Attorney

---

94 *Explanatory Memorandum*, n 93, p 8.

95 *Classification of Publications, Films and Computer Games (Enforcement) Act 1995* (Vic), ss 56-59.

96 *Classification (Publications, Films and Computer Games) Act 1995* (SA), ss 75A-75E.

97 *Censorship Act 1996* (WA), ss 99-102.

98 *Classification of Publications, Films and Computer Games Act 1985* (NT), ss 50X-50ZA.

99 For a commentary on these laws see – G Griffith, *Censorship in Australia: Regulating the Internet and other developments*, NSW Parliamentary Library Briefing Paper No 4/2002.

General foreshadowed the introduction of the Classification Enforcement Amendment Bill 2001, commenting:

> The practical effect will be that, for example, a predatory paedophile who creates a porn site on the Internet, aimed at luring young children into communication, will be able to be charged under these new provisions. This is in addition to the host of offences under the Crimes Act that such an offender is likely to have committed. In other words, this new legislation gives police another string to their bow. We will create another brick in the wall against online sex offenders.[100]

It must be noted, however, that Part 5A has not been proclaimed to commence and is therefore not in force as at 1 August 2007.

6.4 New South Wales – child pornography laws

Other criminal laws also impinge on the online environment, notably those relating to child pornography. Division 15, ss 91C-91H of the *Crimes Act 1900* (NSW) is headed 'Child prostitution and pornography'. The law on child pornography was revised in 2004. The former offence of 'Possession of child pornography' under s 578B of the *Crimes Act 1900* (NSW) was repealed. In its place a new offence of 'Production, dissemination or possession of child pornography' was created under s 91H of the Crimes Act. A feature of this revised law is that it no longer ties the definition of 'child pornography' material to the 'RC' classification under the censorship legislation. This has the practical effect of removing the former requirement for material to be classified by the Classification Board for proceedings to commence. Under the revised scheme the courts can make their own determination as to whether material is or is not child pornography.[101] 'Material' is defined to include 'any film, printed matter, electronic data or any other thing of any kind (including any computer image or other depiction)'. Section 91H therefore applies equally to online as it does to off-line material.[102]

6.5 New South Wales – child sex offences

Before looking directly at laws specifically designed to combat online grooming in other jurisdictions, note can be made of the fact that such provisions operate alongside a host of

---

100 *NSWPD*, 25 October 2001, p 18038.

101 *NSWPD*, 11 November 2004, p 12738. All Australian jurisdictions have specific criminal offences relating the child pornography. For example, the Commonwealth Criminal Code includes offences for using a telecommunications carriage service to access, transmit, publish or distribute either 'child pornography' or 'child abuse material' (*Criminal Code* (Cth), s 474.19 and s 474.22). Specific offences also relate to possessing, controlling, producing, supplying or obtaining either 'child pornography' or 'child abuse material' for use through a telecommunications carriage service.

102 The same applies in respect to the offence of 'Publishing indecent articles' under s 578C of the *Crimes Act 1900* (NSW), where both the words 'article' and 'publish' are broadly defined.

child sexual offences. For NSW, these were set out in Briefing Paper No 20/2003. The table headed 'Sexual offences in the *Crimes Act 1900* that specify child victims' is reproduced at Appendix 3.[103]

Of course where real life contact is made and an illegal sexual act involving a young person is committed then the relevant statutory provision can be applied, including those provisions under s 66A and C of the Crimes Act which relate to sexual intercourse with a child of various ages. In different circumstances other offences of a preparatory nature may also be relevant. In particular, the offence of 'Act of indecency on a person under 16 years' under s 61N(1) of the Crimes Act includes the offence of *inciting* a person under 16 to commit such an act, either with the accused or with another person.[104] Interpretation of what constitutes incitement in this and other contexts is left to the common law. Glanville Williams describes incitement as one of the offences 'that enable the police to nip criminal tendencies in the bud'. Like attempt and conspiracy, incitement is an 'inchoate crime', in that it does not need to be fully consummated before the criminal law takes cognizance of it. An inciter, according to Williams 'is one who counsels, commands or advises the commission of a crime.'[105] However, a number of obstacles may lie in the way of a successful prosecution. If the law is constructed narrowly, an intention to commit, and an incitement to be involved with, a specific act of indecency will have to be proved. As explained by Childnet International in its submission to the UK Home Office, if the only evidence is that the accused had a general intent to persuade a minor to have sexual relations of some kind with him, without any specific evidence of incitement to commit particular unlawful acts, then the charge could not be made out.[106]

The common law of attempt may also apply in this context. More specifically, an offence of attempting to have sexual intercourse with a minor is created under s 66D of the Crimes Act. But note in this context the following comment made by the Victorian Law Reform Commission:

> An attempt offence covers conduct that is more than merely preparatory to the commission of the offence, and immediately and not remotely connected with the commission of the offence. This means that the accused's conduct must be sufficiently close to the commission of an offence to qualify as an attempt.[107]

---

103 R Johns, *Child Sexual Offences: An Update on Initiatives in the Criminal Justice System*, NSW Parliamentary Library Briefing Paper No 20/2003, pp 2-3.

104 Note that s 61N(2) further provides that 'Any person who commits an act of indecency with or towards a person of the age of 16 years or above, or incites a person of the age of 16 years or above to an act of indecency with or towards that or another person, is liable to imprisonment for 18 months'.

105 G Williams, *Criminal Law, The General Part*, 2nd ed, Stevens and Sons Ltd 1961, pp 609-613.

106 Childnet International, *Online grooming and UK law* - http://www.childnet-int.org/downloads/online-grooming.pdf

107 Victorian Law Reform Commission, *Sexual Offences: Interim Report*, 2003, p 386.

Writing on the difficulties involved, Childnet International commented:

> This is what happened in the case of Kenneth Lockley in the UK, May 2000. Following a tip off by the Californian police that Lockley was searching for a six year old girl to have sex with, Scotland yard set up a sting operation and arranged a meeting at a hotel in London…Four condoms were found on him. However, the charges of attempting to have unlawful sex with a girl under 16 were dropped because, as the defence argued, there was no actual attempt to have sexual intercourse as there was no actual child involved.[108]

As discussed in section **[7.4]** of this paper, in the absence of a specific NSW online grooming offence, NSW Police can (and does) refer prosecutions to the Commonwealth Director of Public Prosecutions.

6.6 Australia – online grooming laws

While NSW has not passed online grooming laws, several Australian jurisdictions have done so, either in terms of provisions exclusively concerned with electronic means of communication (Queensland, Commonwealth, Western Australia), or applying to all forms of communication (South Australia, Tasmania).

In summary, the main Australian laws expressly targeting online sexual predators are directed towards some or all of the following acts:

- using the Internet (or other form of communication) with the intention of 'procuring' a child to engage is sexual activity (Commonwealth, Queensland, South Australia, Tasmania and Western Australia);
- 'grooming' a child, by sending indecent material to a child or otherwise engaging in prurient communication with a child, with the intention of making it easier to procure a child to engage in sexual activity (Commonwealth, South Australia);
- 'exposing' a child to indecent or pornographic material (Queensland, Tasmania, Western Australia, ACT, NT).

These offences can be set out in tabular form, as follows:

---

[108] Childnet International, n 106.

Online Grooming Offences in Australia

Jurisdiction	Statute	Section	Offence	Maximum penalty
ACT	Crimes Act 1900	66	Suggest child under 16 takes part in sexual act and making pornographic material available.	First offence 5 years; second offence 10 years
Commonwealth	Criminal Code	474.26	Intent to procure child under 16 by use of carriage service	15 years
		474.27(1), (2)	Grooming child under 16 by use of carriage service	12 years
		474.27(3)	Grooming two children by use of carriage service	15 years
Queensland	Criminal Code Act 1899	218A(1)	Intent to procure by Internet and exposing child under 16 to indecent matter	5 years (10 years if child under 12 or believed to be under 12 years)
South Australia	Criminal Law Consolidation Act 1935	63B(3)	Procure, intent to procure and grooming child under 16 by any means	10 years (12 years if child under 14 years)
Tasmania	Criminal Code Act 1924	125D	Intent to procure by any means and exposing children under 17 to indecent material	No statutory maximum penalty
Western Australia	Criminal Code	204B	Intent to procure by Internet and exposing child under 16 to indecent matter	5 years (10 years if child under 13)
Victoria	Crimes Act 1958	58(1)	Soliciting or procuring child under 16	10 years
Northern Territory	Criminal Code Act	131	Attempt to procure child under 16	5 years (adult offender); 3 years (non-adult offender)
		132(2)(e)	Exposing child under 16 to indecent material	10 years (14 years if child under 10)

ACT: In 2001 the ACT was the first Australian jurisdiction to introduce a specific provision designed to combat Internet grooming. Section 66 of the *Crimes Act 1900* (ACT) creates an offence where an adult uses electronic means to 'suggest' to a person under 16 years that he or she commits or takes part in (or watches someone else committing or taking part in) an act of a sexual nature. An 'act of a sexual nature' is defined to mean 'sexual intercourse or an act of indecency'.[109] The key physical elements of the crime, therefore, are that the accused uses electronic means to make a suggestion of this kind. Presumably, an 'act of indecency' could be committed online, but this is left to the courts to decide in the circumstances of the case.

By s 66(2) it is also an offence 'to send or make available pornographic material to a young person. 'Pornographic material' is defined to mean material that has been, or is likely to be, classified 'RC', 'X18+' or 'R18+'.

A defence is provided to ISPs where they had no knowledge that the accused's Internet facilities were used to commit the offence. The accused is also provided with a defence where they can prove that they believed on reasonable grounds that the young person in question was at least 16 years old. Consent on the part of the young person is not a defence.

Unlike its Queensland counterpart, in the ACT no legislative sanction is provided for covert operatives posing as fictitious children.

Queensland: Queensland was the first Australian State to pass laws directly aimed against the use of the Internet for the procuring of minors for sexual purposes and for the employment of police 'stings' to entrap persons who do use the Internet for that criminal purpose. Section 218A was inserted into the State's *Criminal Code Act 1899* (Qld) in 2003. It is headed 'Using internet etc. to procure children under 16'. As explained by the Explanatory Notes, the provision is based in part on s 172.1 of the Canadian Criminal Code. Reference was also made to *Ridgeway v The Queen*,[110] where the High Court acknowledged that police methodology sometimes necessarily involves law enforcement officers in 'subterfuge, deceit and the intentional creation of opportunities for the commission by a suspect of a criminal offence'.[111] In that case a common law defence of entrapment was rejected.[112] However, a discretion to exclude evidence on public policy

---

109 Section 66(1) provides: 'A person must not, using electronic means, suggest to a young person that the young person commit or take part in, or watch someone else committing or taking part in, an act of a sexual nature'. For the full text of the provision see - http://www.austlii.edu.au/au/legis/act/consol_act/ca190082/s66.html

110 (1995) 184 CLR 19.

111 (1995) 184 CLR 19 at 37.

112 Mason CJ, Deane and Dawson JJ discussed whether the common law recognises a defence of entrapment, After noting that the defence had been rejected by State Supreme Courts and by courts in other comparable jurisdictions, they commented 'The decisions to that effect are not surprising since it is a central thesis of our criminal law that a person who voluntarily and with the necessary intent commits all the objective elements of a criminal offence is guilty of that offence regardless of whether he or she was induced to act by another, whether private citizen or law enforcement officer' (at p 28).

grounds was recognised, where evidence was obtained either by unlawful or improper conduct on the part of the authorities. No hard and fast rules were drawn. In the their joint judgment, Mason CJ, Deane and Dawson JJ commented 'It is neither practicable nor desirable to seek to define with precision the borderline between what is acceptable and what is improper in relation to such conduct'.[113]

With the admissibility of evidence obtained through police undercover operations in mind, the Explanatory Notes further explained:

> The new section 218A will permit the police to be pro-active so that paedophiles can be stopped before a child is damaged. The law at present is more reactive, and there is a much higher risk that a child will be hurt before action is taken. The offence will also have a strong deterrent and educative effect.
>
> The advantage of investigators using the Internet is that there will be real time recordings of the interaction between the alleged offender and the child (or police officer pretending to be a child) to be examined by the court.[114]

New offences are created under the Queensland provision, relating to the use of electronic communication for grooming purposes specifically, and separately to the exposure of a person under 16 years of age to 'indecent matter'. Section 218A(1) provides:[115]

> Any adult who uses electronic communication[116] with intent to –
> (a) procure a person under the age of 16 years, or a person the adult believes is under the age of 16 years, to engage in a sexual act, either in Queensland or elsewhere; or
> (b) expose, without legitimate reason, a person under the age of 16 years, or a person the adult believes is under the age of 16 years, to any indecent matter, either in Queensland or elsewhere;[117]
> commits a crime.[118]

---

113 (1995) 184 CLR 19 at 37. The joint judgment did refer to 'a degree of harassment or manipulation which is clearly inconsistent with minimum standards of acceptable police conduct in all the circumstances…'.

114 *Queensland Acts 2003, Volume 1 – Explanatory Notes Acts Nos 1-31*, pp 82-83.

115 The full text is available at - http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf

116 The term 'electronic communication' is defined to mean 'email, Internet chat rooms, SMS messages, real time audio/video or other similar communication.

117 The intention of this aspect of the provision is to overcome territorial limits on State powers by providing a connection with Queensland: N Dixon, *Catching 'Cyber Predators': the Sexual Offences (Protection of Children) Amendment Bill 2002* (Qld), Queensland Parliamentary Library Research Bried No 23/2002, p 13.

118 Maximum penalty – 5 years imprisonment. By s 218A(2) the maximum penalty rises to 10 years imprisonment where the person is, or the adult believes, is under 12 years.

It is s 218A(1)(a), the procuring offence, that is of most direct relevance at present. Two distinct offences are created, as follows:

- where an adult uses electronic communication with the intent to procure a person *who is in fact under the age of 16 years* to engage in a sexual act; and
- where an adult uses electronic communication with the intent to procure a person the adult *believes is under the age of 16 years*, to engage in a sexual act.

The word 'procure' is defined to mean 'knowingly entice or recruit for the purposes of sexual exploitation'. What is meant by 'sexual act' is defined by s 218A(3)(4)(5) and (6) and is 'not limited to sexual intercourse or acts involving physical contact'. Enticing a young person to engage in masturbation online is seemingly covered by the provision. This suggests that, for the commission of the offence of online procurement, the accused does not have to plan to meet with the young person concerned.[119] Note, too, that 'it is not necessary to prove that that the adult intended to procure the person to engage in any particular sexual act'. Indeed it does not matter that, 'by reason of circumstances not known to the adult', that it was impossible in fact for the person to engage in the sexual act. For an offence to be committed therefore an actual sexual act need not occur; what is required is the *intention* on the part of the accused to procure such an act, either online or in the context of an offline meeting.

By s 218A(7) for evidence obtained through police 'sting' operations to be admissible 'it does not matter that the person is a fictitious person represented to the adult as a real person'.[120] By s 218A(9) a defence is provided where the accused can prove that he 'believed on reasonable grounds' that the person was at least 16 or 12 years, as the case may be. The evidential burden rests therefore on the accused.

In summary, the elements of the offence under s 218A(1)(a) are that the prosecution must prove that:

- the offence occurred at the time and place alleged; and
- the offender was the accused; and
- the accused is an adult; and
- the accused, by use of electronic communication, *intended* to entice or recruit a person to engage in a sexual act; and
- the person (the victim) was in fact under the age of 16 or 12, as the case may be; *or*
- the accused *believed* the victim was under the age of 16 or 12, as the case may be (the belief element).

---

119 On the other hand, where the intent is to perform a sexual act offline, then the courts may require evidence of a plan to meet in person.

120 The section does not provide a general rule of admissibility for evidence gained by police undercover operations. It refers only to the fact that the supposed recipient of the communications was in fact a fictitious person. It seems to leave open the possibility that the court may exercise its discretion to exclude evidence on the basis that some conduct engaged in by the police was 'improper'.

The issue of 'belief' in s 218A raises certain difficulties, where it applies either as an element of the offence, or by way of a defence, where the accused seeks to prove that he 'believed on reasonable grounds' that the person was at least 16 or 12 years, as the case may be. Whatever evidence exists in respect to belief is after all more likely to be in the possession of the accused. For this reason, a rebuttable presumption is created by s 128A(8) that if a person is represented to be under the age of 16 (or 12 years) then, in the absence of evidence to the contrary, this is proof that the accused believed the person to be under that age. In *R v Shetty* the Queensland Court of Appeal held that s 218A(8)

> does not alter the position that the jury must be satisfied that the accused had the belief essential to establish a contravention of s 218A(1). The legislature has determined that the jury must be so satisfied if they conclude that it was represented to the adult that a person was under a certain age and the adult does not adduce evidence that the representation did not induce in him the belief which that representation was apt to induce. If the adult does adduce evidence as to what he or she actually believed, then it is a matter for the jury whether or not this evidence should be accepted.[121]

In that case the trial judge erroneously directed the jury that it was not sufficient to rebut the presumption for the accused to tell them that he didn't have any belief one way or another as to the age of the person he was chatting to. The trial judge wrongly directed the jury that they could proceed on the basis that the accused believed the person he was chatting to on the Internet was under 16 years of age.

As noted, s 218A(1)(b) also makes it a crime to make a communication with intent to expose, without legitimate reason, a young person under the age of 16 years (or a person the accused believes is under 16) to indecent matter.[122] This 'exposure' offence is not equivalent to that created under s 474.27 of the Commonwealth Criminal Code, in that it is not linked to the procurement of a minor for sexual purposes.

Commonwealth: The Explanatory Memorandum notes that ss 474.26 to 474.29 of the Commonwealth Criminal Code:

> contain an offence regime targeting adult offenders who exploit the anonymity of telecommunications services (for example, the Internet) to win the trust of a child as a first step towards the future sexual abuse of that child. The practice is known as 'online grooming'.

Sections 474.26 to 474.29 were inserted into the Commonwealth Criminal Code in 2004. While these offences build on s 218A of the Queensland Criminal Code, they also diverge from that model in important respects. In particular, the Commonwealth scheme establishes a separate offence where the use of 'indecent' material is used in the grooming process.

---

121 [2005] QCA 225 at [26] (Keane JA, McPhersonJA and McMurdo J agreeing).

122 'Indecent matter' is defined by s 1 of the Queensland Criminal Code to include 'indecent film, videotape, audiotape, picture, photograph or printed or written matter'. Whether matter is indecent is left to the court or jury to determine, as a question of fact not law.

The Explanatory Memorandum continued:

> There are two steps routinely taken by adult offenders leading up to a real life meeting between adult and child victim that results in child sexual abuse:
>
> (i) The adult wins the trust of a child over a period of time. Adults often use 'chat rooms' on the Internet to do this. They may pose as another child, or as a sympathetic 'parent' figure. Paedophiles reportedly expose children to pornographic images as part of this 'grooming' process. It is proposed to specifically criminalize this practice. Specific offences would remove any doubt about whether online 'grooming' of a child before actual contact is 'mere preparation' (i.e. not a criminal offence) or an unlawful attempt to commit child sexual abuse.
>
> (ii) With the child's trust won, adults often use telecommunications services to set up a meeting with the child. Although this step is more likely to be characterised as an attempt to commit child sexual abuse than step (i), it is desirable to provide a firm justification for police action by enacting specific 'procurement' or 'solicitation' offences. This is consistent with the underlying rationale for the new offences: to allow law enforcement to intervene before a child is actually abused.[123]

In summary, s 474.26 'Using a carriage service to *procure* persons under 16 years of age' creates several distinct offences, namely, where an adult transmits a communication with the intention of procuring a person *who is*, or *who he believes is* under 16 years of age

- to engage in, or submit to, sexual activity *with the sender*, or
- to engage in, or submit to, sexual activity *with another person who is, or who the sender believes to be, at least 18 years of age*, or
- to engage in, or submit to, sexual activity *with a person who is under 18 years of age in the presence of the sender or another person who is, or who the sender believes to be, at least 18 years of age*. In other words, the offender 'procures' two children to engage in sexual activity in the presence of that offender or another adult.[124]

Following the Queensland legislation 'sexual activity' is defined broadly and need not involve 'physical contact between people'. Again, the focus of the offence is on the *intention* to procure a young person to engage in, or submit to, sexual activity. Presumably, this planned sexual activity may occur online, either with the sender, or with another adult. In these circumstances, there need be no actual physical meeting, or any plan to meet in person.[125]

---

123 Explanatory Memorandum, *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No 2) 2004* - http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=1860&TABLE=OLDEMS

124 For all three offence the maximum penalty is imprisonment for 15 years.

125 Where an actual meeting and physical sexual contact occurred, that particular offence

Section 474.27 - 'Using a carriage service to "*groom*" persons under 16 years of age' - is structured along the same lines, but is concerned specifically with the sending of 'indecent' material to minors. Whether material is 'indecent' will be a matter for a court and/or jury to decide, by a reference to the community standards test of 'according to the standards of ordinary people' (s 474.27(5)).[126] Reference to 'material' in this context is to pornography in pictorial or non-pictorial form, or to a combination of the two.[127] Again several distinct offences are created, namely, where an adult transmits *indecent material* with *the intention of making it easier to procure* a person *who is*, or *who he believes is* under 16 years of age:

- to engage in, or submit to, sexual activity *with the sender*, or
- to engage in, or submit to, sexual activity *with another person who is, or who the sender believes to be, at least 18 years of age*,[128] or
- to engage in, or submit to, sexual activity *with a person who is under 18 years of age in the presence of the sender or another person who is, or who the sender*

---

would have to be prosecuted under the relevant State or Territory child sex offence law.

126 According to the Explanatory Memorandum: 'Courts are well practiced at applying the standards of ordinary people in the criminal law context. An example illustrates how this physical element of the 'grooming' offences would operate. A sender may send child pornography material to the recipient in an effort to suggest the types of activities the sender would like to engage with the recipient. It seems clear that the child pornography material would be regarded as indecent according to the standards of ordinary people.

Alternatively, the sender may send adult pornographic material through to the recipient. There may be members of the Australian community that would not regard this material as indecent. However, the context in which the communication is sent is also important to this element of the 'grooming' offences. The sending of pornographic material to a child, or a person the sender believes is under 16 years of age, would presumably be viewed differently to the sending of pornographic material to another adult. The fact that a child recipient is involved would usually be sufficient to mean that the communication involved 'material that is indecent'. Another example could be a chain of communications between sender and recipient where the sender inquires about the recipients clothing, including undergarments, and makes other sexually suggestive comments. In circumstances where the recipient is a child, or a person the sender believes to be under 16 years of age, it is likely that this would be considered indecent according to the standards of ordinary people'.

127 According to the Explanatory Memorandum: 'The term 'material' would be defined consistently with the definition of material in the proposed Internet child pornography offences (proposed section 473.1 defines material to include material in any form, or combination of forms, capable of constituting a communication)'.

128 For the first two offences the maximum penalty is imprisonment for 12 years. The Explanatory Memorandum explained: 'The "grooming" offences would often involve using a carriage service to send pornographic images, including child pornography material. Therefore, a maximum penalty of at least imprisonment for 10 years is necessary to maintain consistency with the proposed offences targeting the distribution of child pornography material, also included in the Bill. The penalty for "grooming" should be lower than the proposed penalty of imprisonment for 15 years for 'procuring': the act of "procurement" is arguably more serious, being closer to the commission of actual child sexual abuse'.

> *believes to be, at least 18 years of age*. In other words, the offender 'grooms' two children to engage in sexual activity in the presence of that offender or another adult.[129]

Based on the Queensland model, s 474.28 contains a number of provisions designed to make prosecution of these offences easier. It specifically provides that for the purpose of these offences, it does not matter that the recipient is a fictitious person (s 474.28(9), or that it was impossible for sexual activity to take place (s 474.28(8). In addition, by s 474.28(1) and (2) 'absolute liability' applies to whether the recipient is under 16 and to whether a third person for whom the recipient is being procured or groomed is over 18. This means the prosecution does not have to prove intention, knowledge, recklessness or negligence on the part of the defendant in relation to these physical elements of an offence.[130] This would seem to apply to those offences where the recipient of the communication is under 16 years of age. On the other hand, where police 'stings' are mounted and the 'belief' of the accused is an element of the offence, by s 474.28(3) and (4) a rebuttable presumption is created similar to that found under s 218A(8) of the Queensland Criminal Code.

Note that under s 474.29 it is a defence if the defendant believed the recipient was not under 16, or that a third person was not at least 18, although a jury can take into account whether the alleged belief was reasonable.

South Australia: Introduced in 2004, as part of a general review of child pornography and related laws was s 63B(3) of the South Australian *Criminal Law Consolidation Act 1935*. The law does not make direct mention of 'online grooming' or the Internet, and is indeed capable of operating in other contexts. This was confirmed by Second Reading speech for the relevant legislation, where the Minister commented 'It should be noted that the provisions are drafted in general terms and are not limited to the use of the internet'.[131]

Section 63B(3)(1) provides:[132]

> A person who
> (a) procures a child,[133] or makes a communication with the intention of procuring a child to engage in, or submit to, a sexual activity; or
> (b) makes a communication for a prurient purpose[134] and with the intention of

---

129 The maximum penalty is imprisonment for 15 years.

130 'Absolute liability' is defined by s 6.2 of the Commonwealth Criminal Code.

131 *SAPD (House of Assembly)*, 26 October 2004, p 562 (MJ Atkinson, Attorney General).

132 For the full text of the provision see - http://www.legislation.sa.gov.au/LZ/C/A/CRIMINAL LAW CONSOLIDATION ACT 1935/CURRENT/1935.2252.UN.RTF The provision is in addition to s 63B(1) which creates an offence where a person 'incites or procures the commission by a child of an indecent act', or 'acting for a prurient purpose' causes or induces a child to expose any part of their body or to make a record from which an image of a child engaged in a private act may be reproduced.

133 'Child' means a person under, or apparently under, the age of 16 years (s 62).

134 'Prurient purpose' is defined to mean 'a person acts for a prurient purpose if the person acts with the intention of satisfying his or her own desire for sexual arousal or gratification or of

> making a child amenable to a sexual activity
> is guilty of an offence.[135]

Sections 63B(3)(a) is described as a 'procuring' offence, while s 63B(3)(b) is characterised as a 'grooming' offence. The Second Reading speech commented in this respect: 'The offences are drafted as separate offences, which is appropriate, given that grooming is a preparatory offence and procuring involves more substantial acts'.[136] The 'procuring' offences are as follows:

- to procure a child to engage in, or submit to, a sexual activity; or
- to make a communication with the intention of procuring a child to engage in, or submit to, a sexual activity.

The 'grooming' offence is

- to make a communication for a prurient purpose and with the intention of making a person under (or apparently under) 16 years amenable to a sexual activity.

This last 'grooming' offence is different to s 474.27 of the Commonwealth Criminal Code. Under the South Australian provision it is the 'prurient *purpose*' of the communication that is at issue. Whereas under the Commonwealth provision the prosecution is required to prove that the content of the material sent to the minor was 'indecent'. It is a question of fact that falls to be answered. Of course the one may inform the other. The content of a communication is indicative of the purpose for sending it, although not exclusively or determinatively so. For example, hypothetically an irresponsible adult might send a minor an 'indecent' text intended as a joke, albeit one in very bad taste.

Section 63B(3)(b) of the South Australian Criminal Law Consolidation Act can also be contrasted with s 218A(1)(b) of the Queensland Criminal Code.[137] Under the South Australian regime, the mere exposure of a minor to such material is not an offence. Whereas under the Queensland provision it is the exposure *per se*, without legitimate reason, of a person under or believed to be under 16 years to indecent matter that is at issue.

Further, evidentiary issues are not dealt with expressly under the South Australian legislation, including the admissibility of communications sent to a fictitious person

---

providing sexual arousal or gratification for someone else' (s 62).

135 The maximum penalty for a basic offence is 10 years imprisonment; for an aggravated offence it is 12 years imprisonment. Aggravated offence is defined by s 5AA(e) to mean an offence against a person under 14 years of age.

136 *SAPD (House of Assembly)*, 26 October 2004, p 562.

137 See also s 204B(2)(a)(ii) and (b)(ii) and s 204B(3)(a)(ii) and (b)(ii) of the Western Australian Criminal Code, and s 125D(3) of the Tasmanian Criminal Code.

represented to the offender as a real person.[138]

Tasmania: In 2005 the Tasmanian *Criminal Code Act 1924* was revised to insert s 125C – 'Procuring unlawful sexual intercourse with person under 17 years' – and s 125D – 'Communications with intent to procure person under 17years'. As to the latter, the Second Reading Speech made it clear that the provision was intended to pave the way for covert police operations. The Minister explained:

> The primary purpose of section 125D is to target those who seek to groom and procure children for sexual purposes through internet chat rooms or via email. The provision is broad enough, however, to include communications made by any means, including by ordinary mail and other forms of electronic communication, such as SMS messages.[139]

The Minister continued:

> 'Grooming' is the term used for the process that paedophiles use to prepare children for future abuse. For example, paedophiles may show pornographic or indecent material to children in order to promote discussion of sexual matters and thereby persuade them that such activity is normal.

Based on the Queensland model, s 125D(1) of the Tasmanian Criminal Code makes it a crime for a person[140] to make a communication with intent to procure a child under the age of 17 years (or a child the accused believes is under 17 years) to engage in an unlawful sexual act.[141] The prosecution must prove beyond reasonable doubt that the accused actually intended to procure, by means of a communication, a person under the age of 17 years to engage in an unlawful sexual act.

By s 125D(7) of the Tasmanian legislation, the same rebuttable presumption applies in relation to the accused's belief as was discussed above in respect to s 218A(8) of the Queensland Criminal Code. Police 'sting' operations are provided for by s 125D(6). More innovative are ss 125D(5)(a) ad (b) which provide a defence to ensure that young persons communicating with each other will not be prosecuted under the provision. This defence

---

138 The Second Reading speech does say that 'The Bill excludes from the orbit of the new offence the situation where a police officer, using the internet, poses as a child to attract those who would "groom" or procure a child for pornographic purposes'. However, the explanation offered is ambiguous: *SAPD (House of Assembly)*, 26 October 2004, p 562.

139 *Tasmanian Parliamentary Debates*, 14 June 2005 - http://www.hansard.parliament.tas.gov.au/isysquery/irl25d5/1/doc

140 As in South Australia and the ACT, the reference is to 'person' not 'adult'.

141 'Unlawful sexual act' is defined as an act that would, if committed in relation to a person under 17 years, constitute an offence under section 124, 125B, 126, 127, 127A, 133 or 185. For the full text of the provision see - http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_id=69%2B%2B1924%2BJS1%40GS125C%40EN%2B20070807000000;histon=Y;prompt=;rec=;term=

relates to where the recipient is at least 15 years old and the accused no more than 5 years older, or where the recipient is at least 12 year old and the accused no more than 3 years older.

Based on s 218A(1)(b) of the Queensland Criminal Code, s 125D(3) of the Tasmanian legislation also makes it a crime to make a communication with intent to expose, without legitimate reason, a young person under the age of 17 years (or a person the accused believes is under 17) to indecent material.

Western Australia: Section 204B - 'Using electronic communication to procure, or expose to indecent matter, children under 16' - was inserted into the Western Australian Criminal Code in 2006.[142] This provision is also modelled on s 218A of the Queensland Criminal Code. The Western Australian provision creates separate offences:

- where an adult uses electronic communication intending to procure a person *who is in fact under 16 (or 13 years)* to engage in sexual activity,
- where an adult uses electronic communication intending to 'procure a person the offender *believes*' is under 16 (or 13 years) to engage in sexual activity.[143]

Similar evidentiary provisions apply as in Queensland, including a provision permitting police 'sting' operations (s 204B(8)).

Again, based on s 218A(1)(b) of the Queensland Criminal Code, s 204B of the Western Australian Criminal Code creates further offences in respect to using electronic communication to expose a person under 16 (or 13 years) to 'any indecent matter', or separately in respect to using electronic communication to expose a person the offender *believes* is under 16 (or 13 years) to 'any indecent matter'.

Victoria: By s 58(1) of the Victorian *Crimes Act 1958* it is an offence for an adult to 'solicit' or 'procure' a person under 16 to take part in an act of sexual penetration, or an indecent act, outside marriage, either with themselves or another person.[144] The provision was expanded in 2006 to take account of online developments, but without actually making the use of the Internet a physical element of the offence. This followed a Victorian Law Reform Commission report which recommended against an Internet-specific procuring offence, stating 'In our view, the criminality of the conduct should not be based on the medium used by the alleged offender to prepare the child to participate in sexual activity'.[145]

---

142 For the full text of the provision see - http://www.slp.wa.gov.au/statutes/swans.nsf/be0189448e381736482567bd0008c67c/6e61b1ab8d5ce33248257142003079e1?OpenDocument

143 The maximum penalty is five years imprisonment where the victim is under 16 years, and 10 years imprisonment where the victim is under 13 years.

144 Maximum penalty 10 years imprisonment.

145 Victorian Law Reform Commission, *Sexual Offences: Interim Report*, 2003, p 388.

Instead, as amended s 58(1) creates an offence of '*soliciting*' as well as 'procuring' a child under 16 years to take part in an '*indecent act*', as well as in an act of 'sexual penetration'.[146] The Law Reform Commission's Interim Report explained:

> The addition of the word 'soliciting' will broaden the application of the section 58 provision. The emphasis in the word 'soliciting' is upon the making of an offer or request for a particular action. Whereas, 'procuring' connotes a more careful process of contrivance in order to bring about a particular result.[147]

'Soliciting' in this context relates to a preparatory act, evidence in relation to which is likely to be similar to that required to establish an *intention to procure*, which is the focus of Queensland's s 218A(1)(a) and other similar online grooming laws.

The Victorian Law Reform Commission's Final Report stated:

> In the Interim Report we recommend that where an offer is made to a child to participate in some form of sexual activity, or the child is urged or persuaded by an adult to take part in sexual acts, this will be sufficient to constitute an offence. The new offence will require that the accused do something more than engage in sexually explicit conversation with the child. In our view a person should only be criminally liable once he or she has formed the intent to commit a wrongful act.[148]

The 2004 Final Report went on to note that the need for reform in this area could be overtaken by the introduction of the Commonwealth Internet procuring and grooming offences.

Northern Territory: Predating the current online grooming laws, but relevant nonetheless in this context, is s 131 of the Northern Territory Criminal Code Act.[149] This is an *attempt* provision. It creates an offence for a person to attempt to procure a child under 16 years to have sexual intercourse, or to commit, perform or engage in an act of gross indecency.[150] The provision is not tailored to deal with online activity specifically, but it has been used in this context.[151]

---

146 *Crimes (Sexual Offences) Act 2006* (Vic).

147 Victorian Law Reform Commission, *Sexual Offences: Interim Report*, 2003, pp 388-9. See also the Commission's *Final Report* at pp 450-451.

148 Victorian Law Reform Commission, *Sexual Offences: Final Report*, 2004, p 451.

149 The original version of the attempt provision dates back from the *Criminal Code Act 1983* (NT) when the offence was headed 'Attempts at procuration of young person or mentally ill or handicapped females'.

150 Maximum penalty 5 years imprisonment for an adult; 3 years for a non-adult.

151 The provision was applied in *R v Henry*, unreported Northern Territory Supreme Court, Thomas J, 13 July 2004 (the case is discussed in section **[8.5]** of this paper).

Further, s 132(2)(e) of the Criminal Code Act[152] creates an offence where a person, 'without legitimate reason, intentionally exposes a person under 16 years to an indecent object or film, video tape, audio tape, photograph or book'.[153] Again, the provision may be applied in an online context.

Both provisions provide a defence where it can be proved that: (a) the child was at least 14 years old; and (b) that the accused believed on reasonable grounds that the child was at least 16 years old.[154]

6.7 Australia - sex offender registration laws

In 2000, the NSW Government established the first child sex offender registration scheme in Australia.[155] The legislation requires child-sex offenders, and other serious offenders against children, to keep police informed of certain personal details for a period of time after their release into the community. It also requires the police to maintain a Child Protection Register in relation to these offenders. The relevant personal information to be reported by a 'registrable person' includes their: name; any other name by which the person is known; date of birth; residential address; and the name and address of the person's employer.[156] Public access to this information is not permitted.

The Australasian Police Ministers Council subsequently developed model legislation to implement across Australia. In September 2004, the National Child Offender Register was launched. Child offender registration legislation has now been passed in all States and Territories. [157] In 2004, NSW amended its legislation having regard to the model legislation.[158]

At this stage, none of these statutes require a sex offender to provide their email address or other Internet identifiers, such as chat room usernames. As noted, the Commonwealth has

---

152 Inserted by the *Criminal Code Amendment Act (No 3) 1994* (NT). Section 132 is headed 'Indecent dealing with child under 16 years' and includes an offence of procuring 'a child under the age of 16 years to perform an indecent act' (s 132(2)(d)).

153 Maximum penalty imprisonment for 10 years, or 14 years if the child is under 10 years.

154 *Criminal Code Act* (NT), s 131(3) and s 132(5). This defence was inserted by the *Law Reform (Gender, Sexuality and De Facto Relationships) Act 2003*, ss 7 and 9.

155 *Child Protection (Offenders Registration) Act 2000* (NSW).

156 *Child Protection (Offenders Registration) Act 2000* (NSW), s 9.

157 *Child Protection (Offender Reporting) Act 2004* (Qld); *Child Sex Offenders Registration Act 2006* (SA)*; Sex Offenders Registration Act 2004* (Vic); *Community Protection (Offender Reporting) Act 2004* (WA). *Community Protection (Offender Reporting) Act 2005* (Tas); *Crimes (Child Sex Offenders) Act 2005* (ACT); *Child Protection (Offender Reporting and Registration) Act 2004* (NT).

158 *Child Protection (Offenders Registration) Amendment Act 2004* (NSW).

indicated it does not intend to revise the requirements for the National Child Offender Register. In NSW, on the other hand, the Police Minister has foreshadowed amendments to the legislative scheme to require sex offenders to disclose their email address.[159]

6.8 New South Wales - banning sex offenders from the Internet

Note, too, that sex offenders may be prohibited from using Internet chat rooms and the like under legislation that allows for the making of prohibition orders. In NSW, under the *Child Protection (Offenders Prohibition Orders) Act 2004*, the Local Court is empowered to make a prohibition order (s 8(1)) which 'may prohibit conduct of the following kind…(b) being in specified locations or kinds of locations, (c) engaging in specified behaviour'. It may be that either s 8(1)(b) or (c) may permit the Court to prevent a sex offender from using the Internet ('a kind of location', admittedly non-physical in nature, or a form of 'specified behaviour' such as using the Internet for certain proscribed purposes). By s 6 of the Act, a prohibition order can last up to 5 years, or in the case of a 'young registrable person, not more than 2 years'.

Further, under the *Crimes (Serious Sex Offenders) Act 2006* the Supreme Court, on an application from the Attorney General, can make a supervision order against a serious sex offender, who is due to complete his sentence of imprisonment, where the Court is satisfied to a high degree of probability that there is an unacceptable risk that the offender will commit a serious sexual offence if released from custody. The Court is empowered to impose a supervision order that directs the offender to do or not to do a wide range of things, including 'not to engage in specified conduct or classes of conduct' (s 11(h)). Conceivably, this might include a directive not to use Internet chatrooms. Further, the list provided in s 11 is not exhaustive and the Court has the discretion to impose its own directions, which may be quite specific in nature.[160]

6.9 United States – Internet content laws

United States – internet content laws: Federally, the US Government has passed at least two statutes, designed to regulate content on the Internet, for the express purpose of protecting minors and other vulnerable people from 'harm'. In the event, both these statutes have been held to be unconstitutional, further to the protection of free speech under the First Amendment of the US Constitution.

The first attempt at legislation was the *Communications Decency Act* of 1996 which the Supreme Court held was unconstitutional because it was not narrowly tailored to serve a compelling governmental interest and because less restrictive alternatives were available,

---

159 P Coorey, 'Veto for parents on web content', *SMH*, 10 August 2007, p 1; M Farr, 'Porn-proof web pledge', *Daily Telegraph*, 10 August 2007, p 5.

160 Most other Australian States have similar legislation in place, including Queensland's *Dangerous Prisoners (Sexual Offenders) Act 2003*, WA's *Dangerous Sexual Offenders Act 2005*, and Victoria's *Serious Sex Offenders Monitoring Act 2005*. South Australia has enacted laws in relation to continued detention but not supervision – *Statutes Amendment (Sentencing of Sex Offenders) Act 2005*.

notably various forms of Internet content filtering technology.[161]

The *Child Online Protection Act* [COPA]of 1998 was designed to directly address the faults that the Supreme Court found in the earlier legislation. It sought to protect children from exposure to commercial pornography placed on the Internet by imposing criminal penalties of a $50,000 fine and six months in prison for the knowing posting, for 'commercial purposes', of World Wide Web content that is 'harmful to minors'.[162] Minors were defined as 'any person under 17 years of age'. A defence was provided whereby commercial providers were required to demonstrate that they had placed pornographic material behind Internet 'screens' readily accessible to adults who produce age verification. This second statute also ran into constitutional difficulty in the courts, initially when the District Court of Pennsylvania issued a preliminary injunction against its enforcement. In later proceedings the Supreme Court confirmed the injunction, pending a full trial on the merits.[163] Delivering the opinion of the Court, Justice Kennedy wrote that filters were both 'less restrictive' and 'more effective' than COPA. Cited was a report of the federal Commission on Child Online Protection which 'unambiguously found that filters are more effective than age-verification requirements'. This was followed by a decision in March 2007 in which District Judge Lowell A. Reed, Jr. issued a permanent injunction against the enforcement of COPA, in part on the basis that the legislation was 'impermissibly vague and overbroad'.[164] The Act was held to violate both the First and Fifth Amendment rights of the plaintiffs, to free speech and due legal process respectively.

The current position in the US seems to be therefore that, while child pornography is illegal,[165] attempts to regulate Internet content generally have foundered on constitutional objections.

---

161 *Reno v ACLU* 521 US 844 (1997)

162 Congress defined material that is harmful to minors as: any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that- (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest; (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

163 *Ashcroft v ACLU* 542 US 656 (2004). For the background to the protracted litigation see - http://www.epic.org/free_speech/copa/

164 *ACLU v Gonzales*, 22 March 2007, District Court for the Eastern District of Pennsylvania - http://www.paed.uscourts.gov/documents/opinions/07D0346P.pdf

165 Child obscenity and pornography offences were updated by the *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act* of 2003, the full text of which is at - http://www.amberillinois.org/PDF/protectact2003.pdf

6.10 United States – other Internet legislation to protect minors

Cited with approval by the Supreme Court in *Ashcroft v ACLU*[166] were two further laws regulating the Internet in an attempt to protect minors. One referred to a prohibition on misleading Internet domain names, the purpose of which is to prevent Web site owners from disguising pornographic Web sites in a way likely to cause uninterested persons to visit them.[167] Also cited was a statute creating a 'Dot Kids' second-level Internet domain, the content of which is restricted to that which is fit for minors under that age of 13.[168]

6.11 United States – federal anti-grooming and related legislation

More directly, the omnibus legislation, the *Protection of Children from Sexual Predators Act* of 1998,[169] contained several measures designed to make online facilities safer for minors. This included a provision prohibiting the knowing transfer, or attempted transfer, of 'obscene' material to a person under 16 years of age.[170]

A further provision prohibits the use of the United States Postal Service or other interstate or foreign means of communication, to 'knowingly initiate' the transfer of information about a person under 16, such as their name, address or telephone number, '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…'.[171]

---

166 542 US 656 (2004)

167 Section 521 of the *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act* of 2003 which inserted Chapter 110, 18 United States Code s 2252A. The full text of the 2003 Act is at - http://www.amberillinois.org/PDF/protectact2003.pdf

168 *Dot Kids Implementation and Efficiency Act* of 2002 – 47 U.S.C.A s941 (Supp 2004) - http://www.temple.edu/MARTEC/publications/update/kidslaw.pdf The *Children's Internet Protection Act* (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding support for Internet access or internal connections from the "E-rate" program – a program that makes certain technology more affordable for eligible schools and libraries.

169 For the full text of the Act see - http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ314.105.pdf

170 Chapter 71, 18 United States Code s 1470. The provision states: 'Whoever, using the mail or any facility or means of interstate or foreign commerce, knowingly transfers 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 not more than 10 years, or both'.

171 Chapter 117, 18 United States Code s 2425. The provision states: '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

A separate provision of the same omnibus *Protection of Children from Sexual Predators Act* – Chapter 117, 18 United States Code s 2422(b) – forbids the use of the United States Postal Service or other interstate or foreign means of communication, such as telephone calls or use of the Internet, to groom any person under 18 to be involved in a criminal sexual act. As enacted, the relevant provision reads:

> 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 persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or 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 and imprisoned not less than 5 years and not more than 30 years.[172]

For the provision to apply, the proposed sexual activity has to be illegal under State or federal law. Criminal liability under the legislation is therefore contingent on criminal sexual activity as defined by another statute. One potential consequence is that the legislation can operate differently as between jurisdictions, owing to the varying laws relating to the age of consent. However, as affirmed in *United States v Dhingra*,[173] the legislation does apply to situations where both parties are within the same State, but use the Internet based America Online Instant Messenger service whose servers are in another State.[174] In that case a 40-year old Californian male used the Internet to solicit sexual activity from a 14-year old girl, also based in California. However, the conversations were sent through America Online's computer service in Virginia and therefore traveled across State boundaries via a means of interstate commerce.[175] In June 2004 the United States Court of Appeals for the Ninth Circuit held that the legislation was constitutionally valid. It

---

> 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'.

172 For the text see - http://www.law.cornell.edu/uscode/search/display.html?terms=2422&url=/uscode/html/uscode18/usc_sec_18_00002422----000-.html

173 US Court of Appeals for the Ninth Circuit, June 2004 - http://www.ca9.uscourts.gov/ca9/newopinions.nsf/9E57C1EF6508BFE988256EAD005AF18C/$file/0310001.pdf?openelement

174 The term 'instant messenger', like Internet 'chat rooms', refers to a type of Internet service that enables users to engage in real-time dialogue.

175 According to the Tenth Amendment, the federal government of the United States has the power to regulate only matters specifically delegated to it by the Constitution. Other powers are reserved to the States, or to the people. The Commerce Clause is one of those few powers specifically delegated to the federal government and thus its interpretation is very important in determining the scope of federal legislative power. Article I, Section 8, Clause 3 of the United States Constitution, known as the Commerce Clause, reads as follows: 'The Congress shall have Power ...To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes'.

was neither overbroad nor vague, and nor did it violate the First and Tenth Amendments[176] for incorporating State criminal sexual offence statutes.

United States v Dhingra affirmed the earlier ruling of the Court in *United States v Meek*[177] that the federal legislation - s 2422(b) - regulates 'conduct' not 'speech' and therefore falls outside the guaranteed protection afforded by the First Amendment. In effect, the statute only criminalises 'conduct', namely the targeted inducement of minors for illegal sexual activity. 'Speech', in this context, is merely the vehicle through which a paedophile ensnares the victim. In *United States v Meek* a male was found to have used the Internet to attempt to induce a 14-year old boy to engage in sexual activity, in violation of the federal legislation and, by the incorporation of the relevant State law, s 288.2(b) of the Californian Penal Code. With the permission of the boy's father, the police operation involved an officer posing online as the boy. In this capacity, the officer received communications from Meek, using his screen name 'Capnjeffry'. The officer at the outset warned Meek that he was not free to chat as his parents were 'kinda watching'. Meek nevertheless proceeded to engage in sexually graphic conversation with the officer, discussing the possibility of a future sexual encounter. The following principles of interpretation were confirmed:

- The elements of criminal liability are that a person must 'knowingly': (a) actually or attempt to; (b) persuade, induce, entice or coerce; (c) a person under 18 years of age; (d) to engage in sexual activity that would constitute a criminal offence.
- The term 'knowingly' refers to the verbs – 'persuades, induces, entices, or coerces' – as well as to the object – 'a person who has not achieved the age of 18 years'.
- In this context knowledge is subjective – it is what is in the mind of the defendant. That Meek was mistaken in his knowledge is irrelevant.
- An 'actual minor' victim is not required therefore for an 'attempt' conviction under the federal legislation. A 'belief' that a minor was involved is sufficient to sustain an 'attempt' conviction.
- Criminal liability is attached to the attempt to commit a criminal act and is therefore imposed regardless of whether the defendant succeeded in the commission of his intended crime.

6.12 United States – data preservation legislation

It is critically important in police investigations involving the online sexual exploitation of minors that law enforcement agents are able to access Internet Protocol address data linked to a subscriber, particularly that information kept by ISPs that provide connections to the Internet. Pursuant to 18 United States Code s 2703(f), once a law enforcement agent sends a data preservation request to an ISP, the ISP must retain the data described in the request

176 The Tenth Amendment provides: 'The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved for the States respectively, or to the people'.

177 US Court of Appeals for the Ninth Circuit, 19 April 2004 - http://www.ca9.uscourts.gov/ca9/newopinions.nsf/04CD40619CE61BB688256E78007D2667/$file/0310042.pdf?openelement

for 90 days, a period which can be extended an additional 90 days.[178]

6.13 United States – registration of child sex offenders

In the United States, all 50 States have passed laws requiring child sex offenders to register with police authorities. In part, these laws were in response to a 1994 federal statute called the *Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act*. This established guidelines for the States to track sex offenders by confirming their place of residence annually for ten years after their release into the community or quarterly for the rest of their life if the sex offender was convicted of a violent sex crime.[179] Further, during the mid 1990s every US jurisdiction passed a 'Megan's Law', including the federal 'Megan's Law' of 1996 which provided for the public dissemination of information held on the sex offender registries.[180] The federal statute required State and local law enforcement agencies to release relevant information necessary to protect the public about persons registered under a State registration program established under the *Jacob Wetterling Act*. The federal law also provided that information collected under State registration programs could be disclosed for any purpose permitted under a State law.

In practice, the details of the public notification system established under the federal Megan's Law varied from one jurisdiction to another. The US Department of Justice advises in this respect that 'not all State Internet sites provide for public disclosure of information about all sex-offenders who reside, work, or attend school in the State'.[181]

Responding to these jurisdictional differences, the *Pam Lyncher Sex Offender Tracking and Identification Act* of 1996 required the Attorney General to establish a national database for the FBI to track the location of a certain category of sex offenders. The law mandated sex offenders living in a State without a minimally sufficient program to register with the FBI. The following year the *Jacob Wetterling Act* was amended, among other things to direct States to participate in the national sex offender registry.

With the purpose of establishing a more comprehensive and consistent scheme, this area of the law was revisited in the *Adam Walsh Child Protection and Safety Act* of 2006, the text of which can be accessed at - http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ248.109.pdf. This law

---

178 US House of Representatives, A Staff Report prepared for the use of the Committee on Energy and Commerce, *Sexual Exploitation of Children over the Internet*, January 2007, p 4 - http://republicans.energycommerce.house.gov/108/News/01032007_Report.pdf

179 For the full text of the Act see - http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=103_cong_bills&docid=f:h3355enr.txt.pdf

180 For the full text of the Act see - http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_bills&docid=f:h2137enr.txt.pdf

181 US Department of Justice - http://www.nsopr.gov/ In the United States offenders are often classified in three categories: Level I offenders, who are at low risk to re-offend; Level 2 offenders, who are at moderate risk to re-offend; and Level 3 offenders, who are at high risk to re-offend.

implements new uniform requirements for sex offender registration across the States. Features of the law are a new national sex offender registry, standardised registration requirements for the States, and new and enhanced criminal offences related to sex offenders. The legislation's first title is headed the *Sex Offender Registration and Notification Act* (SORNA) and its purpose is to:

- upgrade sex offender registration and tracking provisions;
- strengthen child pornography prevention laws;
- establish a Sex Offender Management Assistance (SOMA) program within the United States Justice Department to help jurisdictions implement the previous sections of the Act; and
- create the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART Office) to administer the standards for sex offender notification and registration,

SORNA establishes a national baseline for sex offender registration and notification programs. In other words, the Act generally constitutes a set of minimum national standards and sets a floor, not a ceiling, for the programs established in the States and Territories. Hence, for example, a jurisdiction may have a system that requires registration by broader classes of convicted sex offenders than those identified in SORNA. Section 124 of SORNA sets a general time frame of three years for implementation, running from 27 July 2006. The Attorney General is authorised to provide up to two one-year extensions of this deadline. Failure to comply within the applicable time frame would result in a 10% reduction of federal justice assistance funding to the States and Territories under the Byrne Justice Assistance Grant funding.

The sex offences covered by s 111(7) of the SORNA regime include all offences by child predators, including:

- solicitation to engage in sexual conduct;
- use in sexual performance;
- video voyerurism;[182]
- possession, production, or distribution of child pornography;
- criminal sexual conduct involving a minor, or the use of the Internet to facilitate or attempt such conduct; and
- any conduct that by its nature is a sex offence against a minor.

According to the proposed guidelines for the SORNA regime, issued by the US Department of Justice, the ***minimum information required for sex offender registries*** include 'Internet identifiers and addresses', such as email and instant messaging addresses. This is not expressly required under the legislation, but is provided for by the 'expansion authority'

182 This clause covers 'video voyeurism' against a minor as described in section 1801 of title 18, United States Code. The cited federal offence in essence covers capturing the image of a private area of another person's body, where the victim has a reasonable expectation of privacy against such conduct.

under s 114(a)(7) and (b)(8) which authorize the Attorney General to specify additional information that must be obtained and included in the registry. The proposed guidelines comment:

> INTERNET IDENTIFIERS AND ADDRESSES (§ 114(a)(7)): In the context of Internet communications there may be no clear line between names or aliases that are required to be registered under SORNA § 114(a)(1) and addresses that are used for routing purposes. Moreover, regardless of the label, including in registries information on designations used by sex offenders for purposes of routing or self-identification in Internet communications—e.g., e-mail and instant messaging addresses—serves the underlying purposes of sex offender registration and notification. Among other potential uses, having this information may help in investigating crimes committed online by registered sex offenders—such as attempting to lure children or trafficking in child pornography through the Internet—and knowledge by sex offenders that their Internet identifiers are known to the authorities may help to discourage them from engaging in such criminal activities. The authority under section 114(a)(7) is accordingly exercised to require that the information included in the registries must include all designations used by sex offenders for purposes of routing or self-identification in Internet communications or postings.[183]

SORNA further provides national standards for the ***disclosure and sharing of information*** held on the sex offender register. The requirements appear primarily in s 118, which is concerned with sex offender websites, and s 121, which is concerned with community notification in a broader sense. Section 118(a) of SORNA states a general rule that jurisdictions are to 'make available on the Internet, in a manner that is readily accessible to all jurisdictions and to the public, all information about each sex offender in the registry'. The information that must be available to the public through public websites include: the name of the sex offender, including all aliases; the address of each residence at which the offender resides or will reside; the address of where the offender works or will work; the license plate number of the offender's vehicle; and a current photograph of the sex offender. This general requirement is subject to certain mandatory and discretionary exemptions. The mandatory exemptions include any information relating to the identity of the victim and the offender's social security number. The discretionary exemptions include information about a Tier 1 sex offender (the lowest category of sex offender) that refers to a conviction for an offence other than a specified offence against a minor. The US Department of Justice asked in this context whether 'offender email addresses and phone numbers should be included on public websites?' The Department commented:

> Posting phone numbers and email addresses of sex offenders on public websites in the same manner as other information is problematic. The public availability of this type of information could allow sex offenders to network with one another, reinforcing negative behavior and providing opportunities for coordinated criminal

183 US Department of Justice, *The National Guidelines for Sex Offender Registration and Notification – Proposed Guidelines, May 2007* - http://www.ojp.usdoj.gov/smart/proposed.htm

> activity.
>
> On the other hand, appropriately designed forms of access to offender email addresses and phone numbers may further the public safety objectives of sex offender registration and notification. For example, the operators of Internet social networking services that serve children may wish to check the email addresses of individuals on their user lists to detect registered sex offenders who are attempting to use their services to contact children. Likewise, a parent may wish to check whether the email address or phone number of an unknown individual who is communicating with his or her child belongs to a registered sex offender.

The US Department of Justice went on to state:

> Jurisdictions are therefore encouraged to include a function on their public websites that allows members of the public to enter an email address or phone number and find out whether that email address or phone number is registered to a sex offender. The Justice Department is currently developing software for jurisdictions to support this type of 'reverse lookup' function, and plans to include this type of function with nationwide scope on the national sex offender website.[184]

The current position in the US seems to be therefore that, under the SORNA regime, sex offenders will be required to register their Internet identifiers and addresses but that these will not be directly available on the public sex offender website. However, search facilities will be made available to the public to check whether a particular email or possibly other Internet address belongs to a registered sex offender.

6.14 United States – Proposed laws on sex offender email registration

Federally, two bills in similar terms were introduced in January 2007, one sponsored by Senators John McCain and Senator Charles Schumer, the other by Earl Pomeroy in the House of Representatives. Both bills were titled *Keeping the Internet Devoid of Sexual Predators*. Their purpose is to amend s 114 of SORNA to expressly require convicted sex offenders to provide any Internet identifiers to the National Sex Offender Registry and to keep such information current. These bills would further require jurisdictions that maintain information about sex offenders to exempt from public disclosure any electronic mail address, instant message address, or other similar Internet identifier used by a sex offender. The federal Attorney General would also be required to maintain a system to allow commercial social networking websites to compare their databases of users to the Internet identifiers of persons in the National Sex Offender Registry. Under the bills such websites are exempted from civil liability if compliant with the requirements of the proposed legislation.[185]

---

184 US Department of Justice, *Frequently Asked Questions: The SORNA Proposed Guidelines* - http://www.ojp.usdoj.gov/smart/pdfs/sorna_faqs.pdf

185 For the text of these bills and information as to their progress see - http://www.washingtonwatch.com/bills/show/110_HR_719.html

These developments at the federal level are to some extent a reflection of what is happening in the States. In December 2006 Virginia's Attorney General Bob McDonnell foreshadowed legislation making it the first State to require registration of email addresses and instant-messaging identities on the State's sex offender registry.[186] Similar legislation was later proposed in Illinois, to amend the State's sex offender registration legislation by inserting into the reporting requirements the words 'all e-mail addresses, instant messaging identities, chat room identities, and other Internet communications identities that the sex offender uses or plans to use'.[187] In July 2007 the *Washington Post* reported that 'Ten states, including Virginia, have passed laws that require sex offenders to also register their e-mail addresses'.[188] The *New York Times* reported that 'Currently such legislation is signed or pending in 13 states'.[189]

6.15 United States – Proposed laws in relation to social networking sites

Federally and at the State level proposed laws have been introduced to regulate social networking sites. These include the Deleting Online Predators Act of 2006, a bill brought before the United States House of Representatives in May 2006 for the purpose of prohibiting schools and public libraries from providing access to 'commercial social networking websites' and 'chat rooms'. In July 2006 the bill was approved by the House of Representatives but was not subsequently voted on by the Senate. On 4 January 2007 the proposal was reintroduced in the Senate as part of a larger legislative package titled 'Protecting Children in the 21st Century Act'. This bill has been referred to the House Committee on Energy and Commerce. Similar bills have been introduced in Oklahoma and Illinois. Oklahoma's HB 1715 would require public libraries to block access to email and social networking sites or deny minors access to the Internet in its entirety. The Illinois Social Networking Prohibition Act would require all public libraries and schools to block access to any social networking site for users of all ages.[190]

In February 2007, the North Carolina Attorney General introduced a bill that would require social networking sites to obtain parental permission before allowing children under the age of 18 to join up.[191] The bill would also require the sites to verify the parent's

---

186 M Felberbaum, 'Va. Attorney General wants sex offenders' online names', *Fox News.com*, 11 December 2006 – http://www.foxnews.com/wires/2006Dec11/0,4670,MySpaceSexOffenders,00.html

187 - http://12.43.67.2/legislation/fulltext.asp?DocName=09500HB0260sam001&GA=95&SessionId=51&DocTypeId=HB&DocNum=0260&GAID=9

188 S Diaz, 'A multi-front battle against Web predators', *Washingtonpost.com*, 31 July 2007.

189 B Stone, 'New security for Facebook over predators', *NYTimes.com*, 30 July 2007.

190 This summary is based on - http://en.wikipedia.org/wiki/Deleting_Online_Predators_Act_of_2006

191 Protect Children from Sexual Predators Act: Senate Bill 132. For an explanatory statement, see North Carolina Attorney General's Office 'Protecting Children from Sexual Predators: SB 132 – Attorney General Roy Cooper', 24 July 2007 accessed at: http://www.ncdoj.com

identity.[192] The Attorney General insists that the technology exists to do this and he explains that 'companies can choose a method that works best for them. For example, verification by credit cards, public databases, follow-up questions and other methods can be used'.[193] Some experts have suggested that this law is not foolproof, 'because children could fabricate their parents' information and purported consent'.[194] On 3 August 2007, it was reported that the bill had 'passed the [North Carolina] Senate unanimously but was gutted after technology industry lobbyists from Washington packed the House Judiciary II Committee to oppose the bill'.[195] The Attorney General said that he would pursue these laws in the next session and would also push social networking sites to voluntarily adopt a requirement for parental permission.[196]

In March 2007, the Connecticut Attorney General announced a similar bill that would require social networking sites to verify the ages of people signing up and to obtain parental permission before allowing people under the age of 18 to join up.[197] The Attorney General argued that age verification would prevent children from being exposed 'to sexual predators who may be older men lying to seem younger'. He maintained that, 'there is no excuse in technology or cost for refusing age verification. If we can put a man on the moon – or invent the Internet – we can reliably check ages'. He added:

> The fact is, contrary to some industry claims, age verification is easy and effective. Sites can confirm the ages of younger users by requiring publicly available information from a parent or guardian. They can confirm information about parents and contact them directly.[198]

It appears that this bill has also not progressed. On 13 August 2007, the Attorney General issued a press release stating that a coalition of 50 States was calling on social networking sites to immediately introduce age and identity verification and parental permission.[199] The issue of age verification is discussed further in section **[9.3].**

---

192 North Carolina Attorney General's Office, n 191.

193 North Carolina Attorney General's Office, n 191.

194 'MySpace: 29,000 sex offenders have profiles', *MSNBC,* 24/7/07.

195 Roy Cooper, North Carolina Attorney General, 'Cooper welcomes new help in fighting crime, protecting consumers', *Media Release,* 3/8/07.

196 North Carolina Attorney General, n 195.

197 Connecticut Attorney General's Office, 'Attorney General, General Law Committee Leaders Announce Bill Requiring Age Verification, Parental Permission and Access at Social Networking Web Sites', *Media Release,* 7/3/07.

198 Connecticut Attorney General's Office Media Release 7/3/07, n 197.

199 Connecticut Attorney General's Office, 'CT Attorney General Calls For Additional Action To Purge Sex Offenders From Social Networking Web Sites', 13/8/07.

6.16 Canada – online 'luring' of children laws

In 2002, s 172.1 was added to the Canadian Criminal Code. It is headed 'Luring a child'. Its purpose is to criminalise electronic communication with a person *who is* or the accused *believes* to be a child *for the purpose of facilitating the commission* of various sexual offences. In other words, online communication is made with the intention of committing a specified sex offence. Depending on the offence, the requisite age (real or believed) of the intended victim varies from 14 to 18.[200] For example:

- read with s 153(1) of the Criminal Code, by s 172.1(a) an offence is committed where the accused, who is an 'a position of trust or authority' towards a person under 18 years of age, uses a 'computer system' to facilitate the forming of a sexual relationship with that young person;
- read with s 280 of the Criminal Code, by s 172.1(b) an offence is committed where the accused uses a 'computer system' to facilitate the abduction of a person who is or who he believes to be under 16 years of age;
- read with s 151 of the Criminal Code, by s 172.1(c) an offence is committed where the accused uses a computer system to facilitate sexual interference against a person who is or who he believes to be under 14 years of age.

Section 172.1(3) of the Canadian Criminal Code is the model for the rebuttable presumption created by s 128A(8) of Queensland's Criminal Code. Its Canadian equivalent provides:

> 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.

Further, by s 172.1(4), for the accused to rely on the defence that he believed that the victim was at least 18, 16 or 14 years old, as the case may be, the accused must prove that he 'took reasonable steps to ascertain the age of the person'.

Covert police operations are not expressly provided for under the legislation.

The first test case involved a 32-year-old Edmonton man (Christopher Legare) who had engaged in sexually explicit online conversations with a 12-year-old girl. Legare had claimed he was 17, whereas the girl said she was 13. While he made telephone contact with the girl, it seems Legare did not suggest that they meet in person. Legare told the court he had no intention of doing so. In the event, Court of Queen's Bench Justice John Agrios acquitted Legare of luring a child over the Internet and a second charge of invitation to sexual touching. Judge Agrios held that more than 'intimate conversation' is required for

---

200 As noted, the general age of consent in Canada is 14. By s 172.1(2) Internet luring of children is punishable on summary of conviction. The maximum penalty is a fine of $2000, and/or imprisonment for up to six months. For an indictment, imprisonment is up to 5 years. For the full text see - http://laws.justice.gc.ca/en/showdoc/cs/C-46/bo-ga:l_V-gb:s_163//en?noCookie

grooming to meet the criminal test of 'luring'. He listed four examples of other conditions:

- an adult asks about the child's home situation;
- the adult asks if the child has run away from home before;
- the adult suggests a meeting; and
- the adult offers to fly out to meet the child.[201]

Note that these indicia may not apply in every case. This is because not all of the specified child sex offences listed under s 172.1 would seem to require actual physical contact between the accused and the victim. For example, s 173(2) refers to the exposure of genital organs to person under 14, an act that must occur 'for a sexual purpose' but 'in any place', a phrase that may be interpreted to include a place on the online environment.

Much would depend on the particular facts of any case, but it would seem that the conditions set out by Judge Agrios would not apply generally to the Australian 'grooming' provisions discussed above. There is no equivalent of the preparatory offences under s 474.27 of the Commonwealth Criminal Code and s 63B(3)(b) of South Australia's *Criminal Law Consolidation Act 1935*. In any event, in-person meetings, either actual or planned, do not seem to be required under such 'procuring' provisions as Queensland's s 218A, where the requisite intention of the accused is to engage a young person in a sexual act, a term that is broadly defined, to include sexual acts that may be performed online.

6.17 England and Wales – meeting following grooming laws

In England and Wales sexual offences were overhauled in 2003, a process that included the creation of the offence of 'Meeting a child following sexual grooming etc' – s 15 of the *Sexual Offences Act 2003* (UK).[202] According to the Explanatory Notes:

> The section is intended to cover situations where an adult (A) establishes contact with a child through, for example, meetings, telephone conversations or communications on the Internet, and gains the child's trust and confidence so that he can arrange to meet the child for the purpose of committing a 'relevant offence' against the child. The course of conduct prior to the meeting that triggers the offence may have an explicitly sexual content, such as A entering into conversations with the child about the sexual acts he wants to engage her in when they meet, or sending images of adult pornography. However, the prior meetings or communication need not have an explicitly sexual content and could for example simply be A giving the child swimming lessons or meeting her incidentally through a friend.[203]

---

201 C Purdy, 'Internet sex chat with girl not luring', *National Post*, 1 April 2006 - http://www.canada.com/nationalpost/news/story.html?id=c0fecf3e-7b7d-4c28-9dda-f1893d6767b9&k=90695

202 For the full text see - http://www.opsi.gov.uk/ACTS/acts2003/20030042.htm

203 Explanatory Notes, *Sexual Offences Act 2003* - http://www.opsi.gov.uk/ACTS/en2003/2003en42.htm

Section 15 is intended to protect children from adults who communicate (by any means) with them and then arrange to meet them with the intention of committing a sexual offence against them, either at that meeting or subsequently. The offence is committed when the offender meets the child or travels with the intention of meeting the child. In summary, s 15 provides that an adult commits an offence if

(a) having met or communicated at least twice before with a person *who is* under 16 years *and* the adult does not reasonably believe is over 16; and
(b) the adult intentionally meets, or travels with the intention of meeting, the young person; and
(c) the adult, at the time, intends[204] to commit a 'relevant offence', which include the child sex offences under the 2003 Act.[205]

For the purposes of s 15:

- the communication can take place anywhere in the world;
- the offender must either meet the child or travel to the pre-arranged meeting;
- the meeting or at least part of the travel must take place within the jurisdiction; and
- the intended offence does not have to take place.

The focus here is on actual physical meetings. The accused and the child concerned must have met or communicated twice before, but these meetings or communications need not have had any sexual content. The law could be said therefore to be more about going to meet a young person with intent to commit an offence than about grooming as such.

The child concerned must be under the age of 16, with the added requirement that the accused did not reasonably believe that the child was over 16. Express provision is not made for police 'sting' operations. However, where the child's place has been taken by an undercover police officer, then the offender could be charged with attempt.[206] Thus, if the police conducted a sting operation, the offender could be charged with attempting to commit the offence even if the offence itself could not technically have been committed as there was no child involved.[207] But, again, for this to occur the accused must proceed sufficiently far down the path of seeking to commit the offence that an attempt to commit a particular unlawful act can be said to have been made.

The Metropolitan Police reported in 2006 that, in the first two years of the operation of the

---

204 The Explanatory Notes comment that 'The evidence of A's intent to commit an offence may be drawn from the communications between A and the child before the meeting or may be drawn from other circumstances, for example if A travels to the meeting with ropes, condoms and lubricants' - http://www.opsi.gov.uk/ACTS/en2003/2003en42.htm

205 The offence carries a maximum of 10 years imprisonment on indictment.

206 The Crown Prosecution Service, *Sexual Offences Act 2003* - http://www.cps.gov.uk/legal/section7/chapter_a.html - 73

207 A Thorp, *The Sexual Offences Bill [HL], Bill 128, 2002-03*, House of Commons Research Paper No 62/2003, p 29.

Sexual Offences Act 2003, six cases of online grooming had been brought.[208]

6.18 New Zealand – meeting following grooming laws

Section 131B of the New Zealand *Crimes Act 1961* was inserted by the *Crimes Amendment Act (No 2) 2005*. It is headed 'Meeting young person under 16 following sexual grooming, etc'. The provision is closely modeled on s 15 of the *Sexual Offences Act 2003* (UK). In summary, the New Zealand law provides that it is illegal to meet with, or to travel with the intention of meeting with, a person under the age of 16 with the intention of having a sexual connection or performing an indecent act.[209] It is a defence if the accused took 'reasonable steps to find out whether the young person' was 16 or older and if the accused 'believed on reasonable grounds' that the young person was 16 or more.

---

208 Cited in J Davidson, 'Internet sex offending: assessing and managing the risk', *Paper delivered at the Risk Management Authority Best Practice Session, Glasgow, 8 September 2006* - http://www.rmascotland.gov.uk/ViewFile.aspx?id=206

209 The maximum penalty is imprisonment for 7 years. For the full text see - http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes

7. POLICE OPERATIONS

7.1 Specialist police units in Australia

Specialist police units have been formed in Australia to combat online child exploitation. These include:

NSW Police: In 1999, NSW police set up the Child Exploitation Internet Unit within the State Crime Command Child Protection and Sex Crimes Squad**.** This specialist unit investigates 'child sexual abuse and exploitation of children that is facilitated through the use of the Internet, related computer and telecommunication devices'.[210]

Federal Police: In March 2005, the Australian Federal Police (AFP) established the Online Child Sex Exploitation Team (OCSET)**,** which performs an investigative and coordination role for multi-jurisdictional and international online child sex exploitation cases.[211] These cases include those from State and Territory Police, government and non-government organisations (including Internet companies), the Australian High Tech Crime Centre (see below), the Virtual Global Task Force (see below), international law enforcement agencies, Interpol and the public. In August 2007, the Federal Government committed an additional $43.5 million over four years to OCSET and the Federal Police's hi-tech crime units, which will result in 36 new staff in 2007/08, and 90 new staff by 2009/10.[212]

7.2 The Australian High Tech Crime Centre[213]

The Australian High Tech Crime Centre was established in July 2003. It is hosted in Canberra by the AFP and is staffed by members of the AFP and State and Territory police, as well as representatives from private industry and government departments. The Centre's main role is to 'provide a nationally coordinated approach to combating serious, complex and multi-jurisdictional technology enabled crimes, especially those beyond the capability of single jurisdictions'. Technology enabled crimes include online child exploitation.

7.3 National Strategy to Counter Online Child Sex Abuse

At the June 2005 Council of Australian Governments' meeting it was reported that, 'the Australasian Police Ministers' Council has endorsed a National Strategy to Counter Online Child Sex Abuse, which will formalise and strengthen cross-jurisdictional law enforcement arrangements'.[214] It appears that the details of this strategy are not publicly available.

---

210 NSW Police Online, 'Child Exploitation Internet Unit', accessed at http://www.police.nsw.gov.au/community_issues/children/child_exploitation

211 This information was sourced from the AFP website: http://www.afp.gov.au/business/reporting_crime/reporting_national_crime/online_child_sex_exploitation.html

212 Coonan, n 7.

213 This information was sourced from the AHTCC website: http://www.ahtcc.gov.au/

214 http://www.coag.gov.au/meetings/030605/index.htm#child

7.4 Covert police operations targeting online grooming

NSW and Federal police: In August 2005, it was reported that NSW police were going to rely on the new Federal laws to 'launch an undercover operation on the Internet to capture predators targeting children in chat rooms'.[215] This operation was 'part of a joint effort involving the Australian Federal Police and State police'.

Queensland police: After the new State laws came into force in 2003, Queensland police (Task Force Argos) engaged in covert operations to detect adults using electronic means to procure children for sexual activity.[216]According to a study conducted by Tony Krone, in the period from June 2003 to September 2004, the police completed 25 investigations into online grooming offences.[217] Krone reported that:

- All 25 suspects were male;
- Suspects' ages ranged from 19 to 55 years with a mean age of 34 years;
- In 22 cases a police officer had posed as a girl between 13 and 16 years of age;
- In the 3 other cases, the police became involved following complaints about the suspect contacting real children (one 10 year old girl and two boys) online;
- Sixty-eight per cent of suspects discussed, sought or arranged to meet the child.
- In eight cases the police investigation was completed in less than one day and in a further 11 cases the investigation was completed within a month.
- Multiple charges were laid - in 18 cases the primary charge was for seeking to procure a child online for sexual purposes; and in the other eight cases, the primary charge was for exposing a child to indecent material.[218]

7.5 International police cooperation: the Virtual Global Taskforce

In December 2003, the Virtual Global Taskforce (VGT) was established. It is made up of law enforcement agencies from around the world (including the Australian High Tech Crime Centre) that are working together to fight online child abuse.[219] The VGT website allows reports to be made about online child abuse. By way of example of its operations (although not one directed at online *grooming*), on 19 June 2007 it was reported that the VGT had facilitated an international police investigation, code named Operation Lobate, into users of an Internet chat room that showed still images and videos of children being abused.[220] As at 19 June, the operation had 'resulted in 63 arrests across 35 countries, with

---

215 'Sting to stop Net sex crime', *The Sunday Telegraph,* 7/8/05.

216 T Krone, 'Queensland Police Stings in Online Chat Rooms', Australian Institute of Criminology, *Trends and Issues in Crime and Criminal Justice,* No. 301, July 2005, p2.

217 Krone (2005), n 216, p1.

218 Krone (2005), n 216, p3.

219 http://www.virtualglobaltaskforce.com

220 See Australian Federal Police, 'AFP Integral in International Hunt for On-line Predators', *Media Release,* 19/6/07; 'Aussie caught in pedophile ring' *Sydney Morning Herald,* 19/6/07;

14 of the persons arrested being classed as contact offenders, and the rescue of 22 child victims of abuse'.[221] In Australia, four people had been arrested and one convicted of child pornography offences, and two others were before the court.[222]

'More arrests after paedophile ring bust', *The Australian,* 19/6/07; and 'Paedophile web ring reaches Australia', *The Age,* 19/6/07. See also 'VGT Collaboration Smashes Global Online Child Abuse Network', *Virtual Global Taskforce Newsletter,* Issue 4, Summer 2007, p1.

221 'AFP Integral in International Hunt for On-line Predators', n 220.

222 'AFP Integral in International Hunt for On-line Predators', n 220.

8. PROSECUTIONS FOR OFFENCES

8.1 Overview

There have been over 130 completed prosecutions for online procuring, grooming and exposure offences in Australia. Most of these have been for offences under the Queensland provision (118 cases) with prosecutions also occurring under the Commonwealth provision (4 cases), the West Australian provision (8 cases) and the Northern Territory provision (at least one case). There have been at least two prosecutions for offences under South Australian law but it is not clear whether either of these cases involved the use of the Internet.[223] There have not yet been any prosecutions under the Victorian or Tasmanian provisions.[224] No information is available about prosecutions under ACT law.

8.2 Prosecutions under Queensland law[225]

Statistics: There have been 58 completed prosecutions for an online procuring offence (under s 218A(1) of the Criminal Code Act 1899). The defendant pleaded, or was found, guilty in 36 of these cases (in the 22 other cases, the defendant was found not guilty). Most cases involved a charge of intending to procure a child under 16 but three involved a charge of intending to procure a child under 12 (in one of these cases the defendant pleaded, or was found, guilty). There have also been 60 completed prosecutions under s 218A(1) for exposing a child to indecent matter online. The defendant pleaded, or was found, guilty in 41 of these cases (in the other 19 cases, the defendant was found not guilty).

Summary of some cases: A summary of five Court of Appeal cases involving procuring offences (some also involving exposure offences) is presented in the Table below.

Name	Summary of facts	Sentence
Kennings[226]	25-year-old male sent via the internet sexually explicit messages to a police officer posing as a 13 year-old girl. He also arranged to meet her. He pleaded guilty and had no prior convictions. Prior to sentence, he sought treatment from a psychiatrist.	2½ years imprisonment suspended after 9 months for period of 4 years. On appeal: reduced to 18 months imprisonment

223 This information was sourced from a document provided to the authors by the Office of Crime Statistics and Research (SA) dated 21 August 2007. It refers to completed prosecutions as at 31 March 2007. Three other cases had not been completed by that date.

224 The information about Victoria was sourced from correspondence with the Office of Public Prosecutions dated 14 August 2007. The information about Tasmania was sourced from correspondence with the Director of Public Prosecutions dated 31 July 2007.

225 The statistics presented in this section are sourced from a document provided to the authors by the Department of Justice and Attorney General (Qld). Note that there was no District Court data for 2003/04 and 2004/05 and the data may therefore understate the total number of prosecutions.

226 *R v Kennings* [2004] QCA 162 (Court of Appeal).

		suspended forthwith (after he had served 3 months).
Campbell[227]	22-year-old male sent via the internet sexually explicit messages and photos of himself masturbating to a police officer posing as a 13-year-old girl. He asked her to masturbate. He also arranged to meet her. He pleaded guilty and had no prior convictions.	18 months imprisonment suspended after 3 months for a period of 4 years. His appeal against sentence was dismissed.
Burdon[228]	50-year-old male sent via the internet sexually explicit messages and a sexually explicit photo of himself to a police officer posing as a 13-year-old girl. He also arranged to meet her and told her that he would perform indecent acts upon her. He pleaded guilty and had no prior convictions. Prior to sentence, he sought treatment from a psychologist.	240 hours community service and 18 months imprisonment wholly suspended. The Crown's appeal against sentence was dismissed.
McGrath[229]	19-year-old male sent via the internet sexually explicit messages to police officers posing as two 13-year-old girls. He gave one 'girl' information about how to perform various sexual acts. A meeting in person was discussed but no arrangement was made. He pleaded guilty and had no prior convictions. Prior to sentence, he had received some treatment from a psychologist and a psychiatrist said that he did not meet the diagnostic criteria for paedophilia.	4 months imprisonment. On **appeal:** sentence suspended after 6 days (the time he had served) for a period of 12 months; offender placed on probation for 12 months with special condition that he submit to treatment.
Hays[230]	29-year-old male sent via the internet sexually explicit messages to a police officer posing as a 13-year-old girl and via a webcam showed real-time images of himself masturbating. He told her how to masturbate herself. He also asked for the names of her friends and he sent sexually explicit messages to a police officer posing as a 13-year-old friend. He pleaded guilty and had no prior convictions.	18 months imprisonment suspended after 3 months for a period of 2 years. His appeal against sentence was dismissed.

Court of Appeal's sentencing observations: The Queensland Court of Appeal has made some general observations about sentencing for these offences. In *Burdon*, a case where the offender arranged to meet a police officer posing as a child, President McMurdo stated:

> …people who are considering using the internet like Burdon to attempt to make contact with young people with a view to corrupting or sexually exploiting them

227 *R v Campbell* [2004] QCA 342 (Court of Appeal).

228 *R v Burdon* [2005] QCA 147 (Court of Appeal).

229 *R v McGrath* [2005] QCA 463 (Court of Appeal).

230 *R v Hays* [2006] QCA 20 (Court of Appeal).

> must now be on notice that such behaviour will be likely to result in a salutary penalty generally involving a term of actual imprisonment, even where physical contact does not and could not eventuate.[231]

In *Hays,* Chief Justice de Jersey confirmed that an offender may be sentenced to imprisonment even if he did not attempt a face-to-face meeting.[232] He explained:

> A meeting for the purpose of sexual exploitation carries particular risk to the immature victim. But so does indecent communication by an offender of mature years directed at an immature and therefore vulnerable child over the Internet. The graphic, salacious nature of what this [offender] said, and did, if directed to a truly vulnerable 13 year old girl, would have carried serious potential to corrupt.[233]

8.3 Prosecutions under Commonwealth law

There have been 4 completed prosecutions under the Criminal Code.[234] It appears that 3 of these prosecutions were for an online procuring offence (under s 474.26) and 1 was for an online grooming offence (under s 474.27). The cases are shown in the Table below.

Name	Summary of facts	Sentence
Holmes[235]	Holmes sent via the internet sexually explicit messages to a person he believed was an 11-year-old girl in the UK (in fact it was an adult male). He also attempted to meet up with the 'girl' for the purpose of having sex. This offence was discovered when police seized his computer as part of investigation into an online paedophile network. He pleaded guilty.	2 years and 9 months imprisonment with non-parole period of 1 year and 8 months

231 *R v Burdon* [2005] QCA 147, p12-13.

232 *R v Hays* [2006] QCA 20, paras 20-21.

233 *R v Hays* [2006] QCA 20, para 22.

234 This information was, in part, sourced from a document provided to the authors by the Office of the Commonwealth Director of Public Prosecutions, dated 7 August 2007. The DPP also advised that proceedings in another 2 cases are ongoing. On 20 August 2007, a sailor in the US Navy pleaded guilty to an online grooming offence (under Commonwealth law it seems): see 'Sailor guilty of net grooming', *Sydney Morning Herald,* 20/8/07.

235 The information about this case was sourced from Commonwealth Director of Public Prosecutions, *Annual Report 2005-2006,* Commonwealth of Australia, 2006, p40. The sentencing citation is *R v Holmes* (NSW District Court, Williams DCJ, 19 May 2006).

Meehan[236]	A 14-year-old Canberra girl accidentally sent a mobile phone SMS to a Melbourne man, Meehan, while trying to contact an old school teacher. He responded and they sent each other text messages. He later sent her an email and chatted with her over the Internet. They continued to communicate and some messages were sexual in nature. He subsequently visited the girl – he requested that she kiss him and he touched her buttocks. He pleaded guilty.	2 years imprisonment, suspended after serving 3 months.
Fing[237]	A 20-year-old male sent via the internet child pornography material and sexually explicit messages to a police officer posing as a 14-year-old girl. He pleaded guilty to child pornography offences but not guilty to an online grooming offence under s 474.27. The jury was apparently directed to acquit for this offence, as there was no evidence that he intended to meet the 'girl' to engage in sexual activity.	For child pornography: recognizance for 3 years and required to submit to supervision of probation and parole.
Tector[238]	In an internet cafe a 41-year-old male passed a note to a 13-year-old boy asking to be included in his chat group. He then sent the boy a message asking if he would perform an indecent activity in exchange for $10. The boy ended the chat and told his mother about the incident. The mother then went online and posed as her son. The man asked further questions about the indecent activity. The police then became involved and posed as the child. He pleaded not guilty but was found guilty. He had prior convictions for child sex offences.	11 years imprisonment with minimum term of 7 years imprisonment.

8.4 Prosecutions under Western Australia law

There have been 8 completed prosecutions under s 204B of the Criminal Code.[239] In all of

236 The information about this case was sourced from Commonwealth Director of Public Prosecutions, *Annual Report 2005-2006,* n 235, p41-42; and from Senator Chris Ellison, 'First internet predator jailed under new anti-grooming laws', *Media Release,* 22/7/06. See also 'Internet predator jailed under new laws', Transcript of ABC - PM program, 21/7/06, accessed at http://www.abc.net.au/pm/content/2006/s1693718.htm. The sentencing citation is *R v Meehan* (Victoria County Court, 21 July 2006).

237 The information about the facts in this case was sourced from 'Jury told to acquit – child sex intent unproven', *The Herald, Newcastle and Hunter,* 11/10/06. The information about the sentence was sourced from a private communication with the Commonwealth DPP.

238 The information about the facts in this case was sourced from various media articles: 'Man accused of luring boy in internet chat room', *The Sun Herald,* 27,8/06 'Mum became a pedophile decoy', *The Sunday Telegraph,* 27/8/06; and 'Pedophile targets café', *The Sydney Morning Herald,* 2/4/07. The information about the sentence was sourced from correspondence with the Office of the Commonwealth DPP.

239 This information was sourced from a document provided to the authors by the WA Office of the Director of Public Prosecutions, dated 1 August 2007. The DPP advised that one of these cases was on appeal. It also advised that there were 21 other cases still active.

these cases the defendant pleaded guilty to the offence. In one case, the defendant received a suspended sentence but in all other cases the defendants had a custodial sentence imposed on them.[240] These custodial sentences ranged from 10 months to 27 months.

8.5 Prosecutions under Northern Territory law

Information was not available about the number of prosecutions under s 131 of the Criminal Code Act. However, there has been at least one case under s 131. In *The Queen v Henry* [241], a 35-year-old male who lived in the Northern Territory contacted in an Internet chat room a police officer using the name 'blondetiffany3'. He offered to travel to Brisbane to meet the 'girl' but she said that she still attended school. He asked her whether she liked having sex and she responded that she was 15 years old and was a virgin. They had subsequent communications via the Internet and he paid for her to fly from Brisbane to Alice Springs and stay in a hotel room with him. In response to being asked online when they would have sex, the offender said 'probably as soon as we see each other, get back to the room and rip each other's clothes off'. He pleaded guilty and prior to sentencing consulted a psychologist who was of the opinion that he would not be a risk to the community. He received a sentence of 1year imprisonment suspended for a period of 2 years with a condition that he submit to supervision and continue treatment.

8.6 Comment

First, it is not known why there have been so many more prosecutions in Queensland compared to other jurisdictions (even allowing for the fact that Queensland was the first State to enact anti-grooming laws). Second, it is not known how many prosecutions have arisen as a result of online police stings (ie police posing online as children) compared to those involving real children. Only one of the Commonwealth cases arose out of a police sting whereas the five Queensland appeal cases outlined above all involved police stings Turning to sentencing, Commonwealth prosecutions have resulted in custodial sentences ranging from 3 months up to almost the maximum of 12 years. No data is available yet about sentencing outcomes in Queensland prosecutions but the five appeal cases outlined above suggest that an 18 month custodial sentence suspended after three months may be typical. In Western Australia, custodial sentences have usually been imposed but all sentences have been less than half of the five-year maximum. To better understand the volume, nature and outcomes of cases, more data and ongoing analysis is needed.

240 WA Office of DPP, n 239.

241 Northern Territory Supreme Court, Thomas J, 13 July 2004.

9. INDUSTRY MEASURES TO PROTECT CHILDREN

9.1 Measures taken by some chat room operators

In September 2003, in response to problems caused by online paedophiles and junk e-mailers, Microsoft announced that it would close most of its chat rooms in 34 countries (including Australia) leaving only a small number of supervised chat rooms still operating.[242] In June 2005, it was reported that Yahoo had 'shut down all of its user-created chat rooms amid concerns that adults were using the sites to try to have sex with minors'.[243] Chat rooms created by Yahoo remained open. In October 2005, Yahoo announced that it would restrict all chat rooms to users above the age of 18. [244] However, 'it was not clear how the company would prevent children from signing up as adults because credit cards are not required'. Yahoo said that it would also make it easier to report any threats to child safety, it would give priority to such complaints and it would develop education materials on its network to promote the safe use of chat rooms.

9.2 Measures taken by some social networking websites

MySpace and Facebook have taken some measures to protect children:

- ***Minimum age:*** The minimum age to sign up to Facebook is 13 and the minimum age to sign up to MySpace is 14. However, neither site currently has a process for verifying that a person who signs up is actually of or above the minimum age (discussed further below). If MySpace becomes aware of under-age members (through reports by other members or its own monitoring), it deletes their profiles. In April 2006, it was reported that MySpace had deleted more than 250,000 profiles of under-age members since the site began.[245]

- ***Special privacy controls for children:*** MySpace and Facebook have some special privacy controls for children in addition to privacy controls available to all members (see **Appendix 2**). On Facebook, the full profiles of members under 18 are not shown to members who are over 18, unless they are confirmed friends. [246] On MySpace, the full profiles of members under 16 are only shown to members who are on their friends list; other members can only view their age, gender and home city.[247] This setting can be changed to allow all members under the age of 18 to view their full profile. Since June 2006, MySpace has also prevented members

242 'Pedophiles force Microsoft to close its chat rooms', *The Australian Financial Review,* 25/9/03.

243 'Yahoo shuts chat rooms amid child sex concerns', *ABC Online,* 24/6/05.

244 'Yahoo to restrict chat room use', *The Age,* 13/10/05.

245 'MySpace tackles teen safety fears', *BBC News,* 11/4/06.

246 'New Scrutiny for Facebook over Predators', *The New York Times,* 30/7/07.

247 'MySpace to curb access to youths', *Sydney Morning Herald,* 21/6/06.

over 18 from asking to be on the friends list of members under 16 unless they already know the member's email address or full name.[248] Note that online predators can get around these restrictions by signing up as a person under the age of 18.

- ***Deleting profiles of sex offenders:*** As noted in section **[2.1]**, MySpace has recently introduced measures to check its members' names against a national database of sex offenders in United States and to date has deleted 29,000 profiles belonging to sex offenders. It has proposed a similar crosschecking scheme against the national sex offender register in Australia. Facebook apparently does not have access to the same database but it has proposed building a database of names and e-mail addresses for sex offenders that could be compared to the membership roll of Internet sites.[249]

- ***Safety tips:*** The MySpace website contains some safety tips for parents and children: for example, 'don't post anything you wouldn't want the world to know', 'People are not always who they say they are. Be careful about adding strangers to your friends list', 'avoid meeting people in person whom you do not fully know'.[250] These tips now pop up when a person registers as a member and if a member changes their settings to allow anyone to see their full profile. The link to the safety tips also appears at the bottom of the pages on the MySpace website. MySpace has also created a guidebook for parents, teachers and law enforcement agencies that highlight the site's safety features.[251] The Facebook website also has a range of safety tips for users and parents.[252] The link to these safety tips is not prominently displayed on the site but the link to privacy controls is.

- ***Reporting misconduct:*** Both MySpace and Facebook allow users to report inappropriate content or conduct on the site. MySpace also has a special hotline for law enforcement officials that is available 24 hours a day, seven days a week.[253]

9.3 Calls for social networking sites to introduce further safeguards

In January 2007, it was reported that a coalition of 33 United States State Attorneys General had called for MySpace to raise the minimum age for joining from 14 to 16 and to introduce measures to verify the ages of its users.[254] The purpose of age verification would

248 'MySpace to curb access to youths', *Sydney Morning Herald,* 21/6/06.

249 'New Scrutiny for Facebook over Predators', *The New York Times,* 30/7/07; and 'Alarm over Facebook predators', *Sydney Morning Herald,* 31/7/07.

250 http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safetytips

251 'A Multi-Front Battle Against Web Predators', *Washington Post,* 31/7/07.

252 http://www.facebook.com/help.php?tab=safety

253 'A Multi-Front Battle Against Web Predators', *Washington Post,* 31/7/07.

254 'MySpace Moves to Give Parents More Information', *The Wall Street Journal,* 17/1/07.

be to ensure that children could not overstate their age and that predators could not understate their age (in particular by stating that they are under the age of 18). According to the article, MySpace said that there is no technology that can reliably verify the age of members who are under the age of 18.[255] The article added:

> Privately, News Corp officials [News Corp owns MySpace] and others in the industry say that age verification is difficult to implement for kids under the age of 18, because they often lack a driver's license or other government-issued verification. It can be done with parental permission slips – but it's not always easy to verify the relationship between a parent and a child.[256]

Instead, MySpace was proposing to make monitoring software available to parents, which would allow them to find out what name, age and location their children are using to represent themselves on MySpace.[257] The program would continue to send updates about changes in these details, even when the child logs on from other computers.[258] Connecticut Attorney General, Richard Blumenthal criticised this response:

> MySpace's 'Zephyr' software is a shortsighted and ineffective response to a towering danger to kids. Children can easily evade the software's purported protections by creating profiles from computers outside the home…
>
> Predators will continue to prey on children using MySpace until the web site and its parent company implement real age verification…Age verification for users 18 and older using publicly available data is easy and effective. MySpace can confirm the ages of younger users by requiring information from a parent or guardian.[259]

As outlined in section **[6.15]** of this paper, Attorneys-General in Connecticut and North Carolina have both introduced bills to require social networking sites to obtain parental permission before allowing children under the age of 18 to join up and (in Connecticut) to verify the ages of people signing up. These bills have not progressed but the coalition of (now 50) State Attorneys General is continuing to advocate that social networking sites voluntarily adopt age verification and parental permission.[260] In a sign that the industry

---

255 'MySpace Moves to Give Parents More Information', *The Wall Street Journal,* 17/1/07.

256 'MySpace Moves to Give Parents More Information', *The Wall Street Journal,* 17/1/07. For further discussion about age verification technology, see 'Why MySpace Doesn't Card', *Forbes.com,* 25/1/07; and A Thierer, *Social Networking and Age Verification: Many Hard Questions, No Easy Solutions*, The Progress and Freedom Foundation, March 2007.

257 'MySpace Moves to Give Parents More Information', *The Wall Street Journal,* 17/1/07.

258 According to a later report, the program will include a 'lockdown' feature that would prevent children from misrepresenting their ages and would allow parents to delete a profile from the site: see 'A Multi-Front Battle Against Web Predators', *The Washington Post,* 31/7/07.

259 Connecticut Attorney General, 'Attorney General Says Proposed MySpace Software Fails to Protect Children, Renews Call for Age Verification', *Media Release,* 17/1/07.

260 Connecticut Attorney General, 'CT Attorney General Calls For Additional Action To Purge Sex Offenders From Social Networking Web Sites', 13/8/07.

might take some action on this front, it was reported recently that Facebook officials had agreed that age and identity verification were 'affordable and feasible' and said they 'want to cooperate and do the right thing'.[261] Some people are concerned that the introduction of age verification will create a false sense of security for children and parents.[262]

9.4 Measures proposed by Skype

Skype's website reports that it 'is actively taking a number of steps with the release of Skype 3.5 Beta for Windows to increase the safety of users under 16 years old, including:

- Restricting the privacy settings of users under 16 years old, so that they are always at maximum safety. This means that only people who they have already added to their Skype contact list can call or initiate chats with them.
- Limiting the availability of date of birth, gender and age information in the user profile of under 16 year olds.
- Increasing privacy and security awareness for users under 16 to the impact of approving authorization requests from unknown people by providing them with a warning message…that asks "Do you know this person? If not, please consider carefully whether you want them to contact".
- Hiding under 16 year olds from search results unless there is an exact match with the Skype Name or email address.
- Disallowing SkypeMe mode for under 16 year olds...[263]

Skype version 3.5 was released on 7 August 2007 but it is not clear whether it incorporates all or any of the above safety features for young users.

---

261 'Alarm over Facebook predators', *Sydney Morning Herald,* 31/7/07.

262 See A Thierer, n 256, p32-33.

263 Skype website: http://support.skype.com/index.php?_a=knowledgebase&_j=questiondetails&_i=1371

10. EDUCATING CHILDREN AND PARENTS

Educating children and parents about online safety is clearly an important way of preventing children from falling victim to online sexual predators. This section provides a brief overview of measures introduced by the Federal Government and NSW Government to educate families about online safety. It also refers to organisations in other countries that provide education and information about online safety.

10.1 Federal Government initiatives

NetAlert: Internet Safety Advisory Body: In December 1999, the Federal Government established an Internet safety advisory body known as NetAlert. Its objectives include:

- To educate the community about current and emerging Internet safety issues, including matters relating to contact in cyberspace, particularly contact which may result in harmful or exploitative contact in the real world;
- To provide advice, particularly through the website and helpline;
- To consult with educational bodies, law enforcement and child protection agencies to assist with Internet safety, particularly prevention issues;
- To consult with industry bodies on Internet safety;
- To commission relevant research into filtering and other technological solutions, Internet usage patters and behaviours and other relevant matters.[264]

Information on website: The NetAlert website contains a range of Internet Safety information including Internet safety guides for various groups (parents, teachers, librarians), a list of Internet safety tips for various groups (teens, families, librarians, teachers) and information sheets on various topics (eg paedophiles and online grooming).[265] The safety tips for families includes the following:

- Spend time online with your children and explore websites together. Take an interest in what they like to do online.
- Help your children use the Internet as an effective research tool - learn about handy homework tips for children and also good searching ideas.
- Be aware of your children communicating with people they don't know, particularly in chat rooms. Set house rules about what information your children can give out.
- Put the Internet enabled computer in a public area of the home, such as the living room, rather than a child's bedroom.
- Talk to your children about their Internet experiences - the good and the bad. Let them know it is OK to tell you if they come across something that worries them and that it does not mean that they are going to get into trouble.
- Teach your children the ways to deal with disturbing material - they should not

264 http://www.netalert.gov.au/about_netalert/goals_and_objectives.html

265 http://www.netalert.gov.au

respond if someone says something inappropriate and they should immediately exit any site if they feel uncomfortable or worried by it.

- Teach children that information on the Internet is not always reliable.
- Encourage children to treat others in the same way that they would in real life by giving them an understanding of netiquette.
- Know the best ways of avoiding spam and how to identify it when it when it first appears.
- Set some appropriate guidelines for Internet use and discuss them with the children in your care.[266]

Email enquiries and helpline: The NetAlert website allows people to send email enquiries about Internet safety and other topics. As part of the August 2007 online safety reforms, NetAlert now operates a national Internet safety helpline to provide advice to parents to help them manage their child's online experience and provide technical filter information.[267] The toll free helpline operates from 8am to 10pm seven days a week. It will eventually have the capacity to take up to 400 enquiries a month.[268]

Educational programs:[269] These programs include:

- ***CyberSafe Schools****:* NetAlert, together with State and Territory educational bodies, developed this Internet safety program for primary and secondary school students. Interactive resources for primary schools (CyberQuoll) and secondary schools (CyberNetrix) were delivered to schools nationally in 2005 and 2006.

- ***Think U Know program****:* NetAlert, in partnership with the Virtual Global Taskforce, Microsoft and Ninemsn, is organising the Think U Know program, which will use a network of accredited trainers to deliver face-to-face training in primary and secondary schools for students, parents and teachers. Schools can register for the program which will commence in 2008.

- ***Netty's World website****:* NetAlert designed this website for young children starting out on the Internet. It provides a safe environment for children to play in, whilst providing important messages about Internet Safety.

As part of the 2007 online safety reforms, the Government announced that it would commit $11.7 million over 4 years to increase NetAlert's highly successful 'outreach function',

---

266 NetAlert, 'Safety tips for families', accessed on the NetAlert website at: http://www.netalert.gov.au/advice/safety_advice_by_group/internet_safety_tips_for_families.html

267 Coonan, n 7. The helpline was launched on 20 August 2007.

268 'Cyber safety hotline goes live', *The Sydney Morning Herald,* 20/8/07.

269 The information in this section was sourced from the NetAlert website at: http://www.netalert.gov.au/programs.html

which 'has taken the internet safety message to over 3,400 school and community groups'.[270] It is not clear what this 'outreach function' is referring to. On 21 August 2007, NetAlert advised that it is currently in the process of developing the outreach program.[271] In response to a request for details as to how the program has operated in the past, NetAlert referred to the CyberSafe Schools program and the Think U Know program.[272]

Australian Communications and Media Authority: In accordance with its functions under the *Broadcasting Services Act 1992* (Cth)[273], the Australian Broadcasting Authority (ABA), which in July 2005 became the Australian Communications and Media Authority (ACMA), has conducted community awareness and education programs in relation to online safety. These programs have included:

- ***Cybersmart kids website****:* In December 2001, the ABA launched this website, which provides Internet safety advice for children, parents and teachers.[274] The site was reviewed in 2005 and an updated site was launched in January 2006.[275]

- ***Cybersmart brochures***: Since 2001, the ABA has published several brochures on online safety topics (eg staying safe in chat rooms), which have been distributed through school, police and community networks.[276] In 2004/05, the ABA released the *Cybersmart Guide*, a brochure containing a range of Internet safety tips for parents and children, which was endorsed by Federal and State police forces.[277] As at 30 June 2006, almost 1 million copies of the guide had been distributed.[278]

- ***Cybersmart detectives***:[279] Launched in 2003, this is an online activity that teaches school students about online safety, particularly how to chat safely. The activity is targeted at young people in the upper primary school to lower secondary school age range. The ACMA website reports that 'ACMA has run nine [of these] activities nationally to date, involving approximately seventy schools around Australia. A further twenty activities are planned for the first half of 2007'.

---

270 Coonan, n 7.

271 Private email correspondence from NetAlert dated 21 August 2007.

272 Private email correspondence from NetAlert dated 21 August 2007.

273 See Schedule 5, clause 94(b), (c).

274 The address for the website is: www.cybersmartkids.com.au. This website replaced the Australian Families Guide to the Internet site which the ABA launched in 1998.

275 Australian Communications and Media Authority, *Annual Report 2005-06*, p49.

276 See Australian Broadcasting Authority, *Annual Report 2002-03,* p 51 and Australian Broadcasting Authority, *Annual Report 2003-04,* p41.

277 Australian Broadcasting Authority, *Annual Report 2004-05*, p37.

278 Australian Communications and Media Authority, *Annual Report 2005-06*, p49.

279 This information was sourced from the ACMA website: http://www.acma.gov.au

New public awareness and education campaign: As part of the August 2007 online safety reforms, the Federal Government is launching a new national public awareness and education campaign to inform parents and carers of children about online safety issues - in particular about online predators – and to provide information about where they can go to receive support and assistance.[280] It has committed $22 million over three years.

10.2 NSW Government initiatives

In 2003, the NSW Department of Education decided to use the ABA's *Cybersmart Kids* brochure (mentioned above) in conjunction with its roll out of Internet access to all students in the state education system.[281] As noted in section **[2.2]**, in August 2007 the NSW Government announced that a technology guide for parents would be distributed to all schools in NSW by the end of the year. The Minister for Education, Hon John Della Bosca MLC said that the technology guide would help parents protect their children against the 'risks involved with the internet and mobile phones'.[282] The guide will contain:

- Information about the types, capacity and potential of information technology used in public schools and the gadgets parents may buy for their children;
- Advice on how computers should be kept in a central place in the home so parents can monitor what students are accessing; and
- Hints on how to spot and handle cyber bullying, access to inappropriate websites and how to protect children from online predators.[283]

10.3 Online safety education initiatives in other countries

Some online safety education initiatives in other countries are outlined below:

- ***New Zealand****:* The Internet Safety Group runs the *NetSafe* program, which provides cybersafety education to children, parents, schools, community organisations and businesses.[284] The *NetSafe* website[285] contains a range of information, including information on 'sex offenders and grooming'. In April 2003, the *NetSafe Kit for Schools* was sent to every school and library in New Zealand.
- ***United Kingdom****:* Launched in April 2006, the Child Exploitation and Online Protection Centre (CEOP) is a national law enforcement agency focused on

---

280 Coonan, n 7.

281 Australian Broadcasting Authority, *Annual Report 2003-04*, p 41.

282 'School manual fights the cyber predators', *Daily Telegraph,* 9/8/07.

283 'School manual fights the cyber predators', *Daily Telegraph,* 9/8/07.

284 The ISG is an independent non-profit organisation whose members represent various stakeholders including the police, the judiciary, the Ministry of Education, educators, parents and students, and community organisations and businesses.

285 http://www.netsafe.org.nz/

tackling sexual abuse of children, especially on the Internet.[286] CEOP also provides education to parents and young people and promotes community awareness. It has created the *ThinkUKnow* website[287], to help young people stay safe online. It is also delivering *ThinkUKnow* training to school students throughout the UK.

- ***Canada**:* The Canadian Centre for Child Protection operates *Cybertip.ca*, which is a national tip line for reporting the online sexual exploitation of children.[288] Cybertip also provides the public with information, referrals and other resources about online safety. The Centre has also developed the *Kids in the Know* personal safety program for school students, which also has activities for families.[289]

- ***United States**:* The National Centre for Missing and Exploited Children (NCMEC) operates a cybertipline and provides information and education for parents and children on online safety.[290] The NCMEC has created *NetSmartz*, an interactive, educational safety resource to teach children about online safety[291]; and *NetSmartz411*, a website that answers parents' questions about online safety.[292] NMEC has also launched a number of online safety campaigns for teenagers including: *2Smart4U, Think Before You Post* and *Don't Believe the Type*.[293]

The European Union is raising awareness about online safety as part of its *Safer Internet Plus Programme*, a four year program (2005-2008) that the European Parliament and Council adopted in May 2005.[294] A European network of awareness agencies has been set up across 23 countries, which carry out awareness actions and programs in cooperation with all concerned parties at national, regional and local levels; and a European coordination agency ensures exchange of best practices. The network organises the Safer

286 http://www.ceop.gov.uk/

287 http://www.thinkuknow.co.uk

288 http://www.cybertip.ca

289 http://www.kidsintheknow.ca

290 http://www.missingkids.com

291 http://www.netsmartz.org. An evaluation of the NetSmartz program in 2005 found that participation in the program 'increased the children's awareness of Internet dangers and allowed them to be more comfortable and confident Internet users': see M Brookshire and C Maulhardt, *Evaluation of the Effectiveness of the NetSmartz Program: A Study of Maine Public Schools,* George Washington University, 22 August 2005.

292 http://www.netsmartz411.org

293 Links to these campaigns can be found at: http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3026

294 http://ec.europa.eu/information_society/activities/sip/index_en.htm. The following summary of awareness initiatives is taken from European Commission Information Society and Media, 'Making the Internet a Safer Place', *Fact Sheet,* 2/2/07.

Internet Day, which has taken place each year in February since 2004. Since May 2006, European parents, teachers and children can get free information on the safe use of the internet through Europe Direct, the European Commission's free information service.

11. INTERNET FILTERING SOFTWARE

11.1 What is filtering software?[295]

Internet filtering software, which can be installed on a home computer, can block children from using the computer to access inappropriate content (eg sexually explicit material) on the Internet. The filtering programs commonly do this by blocking access to websites or website pages that have been included on a 'black list' of inappropriate sites. Some programs 'use more advanced techniques, including key word and phrase searches to help screen out offensive content that has not been included on a black or exclusion list'. Some programs can block access to all websites except those included on a 'white list'.[296]

In addition to blocking access to websites (and of more relevance to the issue of protecting children from online predators), some filtering programs can block chat, instant messaging and email communications. Some programs allow children to use instant messaging and email but 'only permit the sending and receiving of messages from authorized individuals, and will block emails or instant messages containing inappropriate words or any images'.[297] Some programs can prevent children from giving out personal information online.[298] Some software allows parents 'to monitor activities such as the use of computer programs, websites visited, chat room activity and social network sites accessed'.

11.2 How effective is filtering software?

The effectiveness of filtering software in blocking access to inappropriate content varies but no product is likely to be 100 per cent effective.[299] In September 2001 the CSIRO published a report commissioned by NetAlert and the Australian Broadcasting Authority on the effectiveness of a number of filtering products.[300] The study found that eight products blocked 80 to 100 percent of pornographic content, two products blocked 60 to 80 percent of this content, one product blocked 40 to 60 percent and one product only blocked 20 to 40 percent. In 2001, Janet Stanley reported that 'research on six of the most popular filters used in the United States has shown that they fail to block one offensive site in five'.[301] In a

---

295 Unless otherwise indicated, this information was sourced from the NetAlert website at: http://www.netalert.gov.au/filters/faqs.html#q8. For a more detailed explanation of Internet software filtering, see NetAlert and the Australian Broadcasting Authority, *Effectiveness of Internet Filtering Software Products,* September 2001, p4ff.

296 http://www.netalert.gov.au/advice/parental_controls/safe_zones/What_is_a_safe_zone.html

297 See American Civil Liberties Union v Gonzales (United States District Court for the Eastern District of Pennsylvania, 22 March 2007), p27.

298 http://www.cybersmartkids.com.au/for-parents_filters-and-labels.htm

299 White list blocking can be 100 percent effective because, as noted above, it only allows the user to access websites that have been approved.

300 NetAlert and the Australian Broadcasting Authority, *Effectiveness of Internet Filtering Software Products,* September 2001, p4ff.

301 J Stanley, 'Child abuse and the Internet', *Child Abuse Prevention Issues,* No. 15, Summer

United States District Court decision in 2007, the court observed that 'filtering products have improved over time and are now more effective than ever before'.[302] The court also accepted evidence that filtering programs 'generally block about 95% of sexually explicit material'.[303] There does not appear to be any research on the effectiveness of filtering programs in blocking Internet communications or in monitoring Internet activity (which, as noted above, is of more relevance in protecting children from online predators).

11.3 Can children circumvent filtering software?

Filtering programs 'have built in mechanisms to prevent children from bypassing or circumventing the filters, including password protection and other devices to prevent children from uninstalling the product or changing the settings'.[304] However, it may still be possible for technologically minded children to get around the software (see below).

11.4 To what extent do parents use filtering software?

A 2005 study on Internet use in Australian homes reported on the extent to which parents use filtering software to prevent children from accessing inappropriate websites:

> Software to filter inappropriate websites was reported to be used by 35 per cent of parents: 29 per cent used filtering software on a regular basis and six per cent on an occasional basis. This is an increase since 2001, at which time 17 per cent of Internet-connected households with a child aged under 18 reported using such software. The use of filtering software was similar across all children's age groups, however, parents with three or more children were also more likely to have blocking software that parents with fewer than three children.[305]

Research does not appear to have been carried out on the extent to which parents use filtering software to prevent children from communicating with strangers online.

11.5 The National Filter Scheme

On 10 August 2007, the Federal Government announced that it would introduce a National Filter Scheme (costing $84.8 million) that will provide every family with free access to the best available Internet filtering technology.[306] Under this scheme, which commenced on 20 August 2007, parents can download accredited filtering programs from the NetAlert

---

2001, p11.

302 American Civil Liberties Union v Gonzales, n 297, p33-34.

303 American Civil Liberties Union v Gonzales, n 297, p35.

304 American Civil Liberties Union v Gonzales, n 297, p34.

305 NetRatings Australia Pty Ltd, *kidsonline@home: Internet use in Australian homes,* Australian Broadcasting Authority and NetAlert, Sydney, April 2005, p62.

306 Coonan, n 7.

website or have them delivered by post. Programs available under the scheme must block access to prohibited websites as classified by the Australian Communications and Media Authority, be easy to install and use, and come with technical support.[307]

There are currently three approved filtering programs: *Integard, Optenet Web Filter* and *Safe Eyes*. NetAlert compares these programs and tells families to choose the one that best suits their Internet activities and values. Relevant features of these programs include:

- All can block additional Internet sites as selected for a specific user;
- All can block all sites other than those selected for a specific user;
- All can block access to internet chat rooms;
- None can block access to internet games;
- Only one (Integard) can block the sending of personal information;
- Two (Integard and Safe Eyes) can monitor chat room usage;
- All can report on internet usage by different users.[308]

The NetAlert website tells parents that filtering programs do not provide total protection and are a tool to be used in conjunction with parental supervision.[309] On 27 August 2007 it was reported that it took only half an hour for a 16-year-old student to completely override one of the filters approved for the national filtering scheme.[310]

Under the National Filter Scheme, the Federal Government is also proposing to require Internet Service Providers to provide a free *server-based* Internet filtering service to families who prefer this option.[311] This type of Internet filtering system will be implemented following a joint government and industry feasibility study.[312]

---

307 http://www.netalert.gov.au/filters/Compare_internet_content_filters.html

308 http://www.netalert.gov.au/filters/Compare_internet_content_filters.html#Availablefilters

309 http://www.netalert.gov.au/filters/your_family_-_your_choice.html

310 'Teen hacks 'useless' Govt porn filter', *ABC News,* 27/8/07.

311 Coonan, n 7.

312 Some ISPs are of the view that this plan for ISP filtering is not feasible: see 'ISP-level filters 'unworkable'', *The Sydney Morning Herald,* 10/8/07.

12. CONCLUSION

In Australia, as elsewhere, the dangers and perceived dangers posed by online sexual predators have generated widespread community concern. Foremost is the concern that these predators are using calculating grooming tactics to lure vulnerable children into online and real life sexual encounters. Child sexual abuse is the proper term to describe such encounters. Chat rooms were originally the main danger zones but predators are now also targeting the very popular social networking websites.

The true extent of the online grooming problem is not yet clear. A US study in 2006 found that one in seven children aged 10-17 received unwanted online sexual solicitations and that 86% of these were from strangers. Some studies have also found that a significant proportion of children are willing to meet online contacts in person. However, teenagers may be becoming more aware of the dangers. One recent US study found that in 2007 16% of teenagers had considered meeting someone they had talked to online, down from 30% in 2006, and fewer teenagers (8%) had actually met an online contact in 2007, down from 14% in 2006. Further research is required into children's online experiences and, if a truer picture of offenders and victims is to be gained, into actual online grooming cases.

Governments in Australia have introduced a number of measures to protect children. Online grooming offences have been enacted in most States as well as at the Federal level. The NSW Government has not enacted a new offence, presumably because it considers that the federal offence is sufficient. State and Federal police forces have set up specialist units to deal with online child exploitation and there have been over 130 prosecutions for online grooming offences (most in Queensland). In addition to the legal response, the Federal Government has introduced programs to educate children and parents about online safety and it has set up a national hotline. The NSW Government is contributing to this education effort in schools. The Federal Government's new national filtering scheme may also help to protect children from online predators.

The Internet industry is also taking some action. Social networking sites have introduced privacy controls and safety tips for children. In the US, MySpace has also crosschecked its members' names against a national sex offender database. It has proposed a similar scheme in Australia but the Federal Government has not yet endorsed the scheme. There has been a related proposal in Australia (recently introduced in the US) for sex offenders' email addresses to be included in the national sex offender database. The NSW Police Minister has referred this proposal to Cabinet. In the US, State Attorneys General have criticised social networking sites for not doing enough to protect children and they have called for these sites to introduce age verification and parental permission requirements.

The protection of children from online sexual predators will no doubt develop incrementally, as research hopefully identifies the dangers more clearly, as governments adapt their legal and administrative strategies to meet the challenges of the online environment and as parents and children themselves become more aware of the risks involved. One thing is sure; the Internet will continue to evolve, creating new opportunities for communication and, with these, new concerns about the safety of children.

APPENDIX 1

Overview of Skype

The table below presents an overview of relevant features of Skype.[313]

	Skype summary
What is the minimum age?	There does not appear to be a minimum age.
What is on a user's profile?	A user's profile (optional) can show a photo of themselves and personal information including their full name, sex, date of birth, home city, phone numbers, email address and a blurb about themselves.
Who can view a user's profile?	All Skype users can view all of the information on a user's profile except that only people in the user's contact list will see their photo and no users will see their email address. Note that user profiles are deleted from the user directory within 72 hours after a user last used Skype.
Can someone browse or search for other users?	Users can search for other users by name and/or by any other information that is listed in a user's personal profile.
Who can contact a user?	By default, any user can contact another user via voice or video call or instant messaging. Users can change their settings to only allow contact from authorised people in their contact list. If a user selects the Skype Me mode it disables their settings and allows anyone to contact them.
Can a user block another user from contacting them?	A user can block another user from contacting them by clicking on their username and selecting the "block this user" function.

313 The information in this summary was largely sourced from the Skype website's user guides: http://www.skype.com/help/guides

APPENDIX 2

Overview of MySpace and Facebook

The table below presents an overview of relevant features of MySpace and Facebook:[314]

	MySpace summary	**Facebook summary**
What is the minimum age?	14	13
What is on a member's profile?	A member's profile can display a photo of themselves and personal information including: their first name, age, occupation, home city, school, interests and a blurb about themselves. It also has links to the member's friend's profiles.	A member's profile can display a photo of themselves and personal information including: their full name, age, home city, contact details, interests, school and university, and work details. It also has links to the member's friend's profiles.
Who can view a member's profile?	Members under 16: Only friends can view the member's full profile – other members can view their partial profile (photo, age, gender and city). A member can change this setting to allow all members under 18 to view the full profile. All other members: Only friends can view the member's full profile but all members can view a member's partial profile. A member can change their profile setting to allow all other members, or all other members over the age of 18, to view their full profile.	Members under 18: Only friends and other members under the age of 18 can view the member's full profile – other members can view their partial profile (photo, name and network). All other members: Friends and members in the same network (eg region, school) can view the member's full profile – other members can view a partial profile. By default, only friends can view the member's contact details. A member can change their profile setting to allow only friends to view their full profile, or to allow members in their network to view their contact details.
Can someone browse or search for other members?	Members can search for other members by entering in search criteria such as sex, age, height, and country (note that members cannot enter an age under 18 in the fields). Members can also search for other members by name (note the results can include members under 16).	Members can browse members who are in the same network (eg Australia). Members can also search for members in the same network by entering in search criteria such as name, sex, and/or city; or they can search all networks by name. A member can change their settings to only allow friends to search for them.
Who can send a message to a member?	Any member can send a message to another member by clicking on the "send message" function on the other member's profile. MySpace also has instant messaging for which there is three settings: anyone, only friends, or no one.	Any member can send a message to another member by clicking on the "send a message" function on the other member's profile. A member can change their settings to not allow contact from a member who found them via a search and who cannot view their full profile.

314 The information in this summary was obtained by the author looking at various pages on MySpace (http://www.myspace.com) and Facebook (http://www.facebook.com).

	MySpace summary	**Facebook summary**
How can someone join a member's list of friends?	Members under 16: Only members under the age of 18 can ask to join the young member's list of friends. All other members: Any member can ask to join another member's list of friends by clicking on the "add to friends" function on the other member's profile. If the other member approves, the two members will appear on each other's list of friends.	Any member can ask to join another member's list of friends by clicking on the "add to friends" function on the other member's profile. If the other member approves, the two members will appear on each other's list of friends.
Can a member block another member?	Members can block another member from contacting them by clicking on the "block user" function on the other member's profile. They cannot block another member from viewing their profile.	Members can block another member from searching for them, from viewing their profile, and from contacting them.

APPENDIX 3

Sexual offences in the *Crimes Act 1900* (NSW) that specify child victims

Type of offence	Section number	Maximum penalty of imprisonment
Aggravated sexual assault – the listed circumstances of aggravation include that the victim is under 16 years, or is under the authority of the offender.	61J	20 years
Aggravated indecent assault – the listed circumstances of aggravation include that the victim is under 16 years, or is under the authority of the offender.	61M	7 years, or 10 years if the victim is under 10 years of age.
Act of indecency on a person under 16 years, or inciting a person under 16 years to commit an act of indecency.	61N(1)	2 years
Aggravated act of indecency on a person under 16 years, or inciting a person under 16 years to commit an act of indecency. The listed circumstances of aggravation include that the victim is under the authority of the offender.	61O(1)& (2)	5 years, or 7 years if the victim is under 10 years of age.
Sexual intercourse with a child under 10 years	66A	25 years
Attempting, or assaulting with intent, to have sexual intercourse with a child under 10 years	66B	25 years
Sexual intercourse with a child aged from 10 years to under 14 years	66C(1)	16 years
Aggravated sexual intercourse with a child 10-14 years – circumstances of aggravation include being in authority, inflicting (or threatening) actual bodily harm, being in company, or the victim having a serious physical or intellectual disability.	66C(2)	20 years
Sexual intercourse with a child aged from 14 years to under 16 years	66C(3)	10 years
Aggravated sexual intercourse with a child aged from 14 years to under 16 years	66C(4)	12 years
Attempting, or assaulting with intent, to commit an offence under s 66C	66D	Same as penalties under 66C(1)-(4).
Persistent sexual abuse of a child, by engaging in conduct that constitutes a sexual offence, on 3 or more separate days.	66EA	25 years
Sexual intercourse with a child aged from 16 years to under 18 years by a step-parent, teacher etc. The child must be	73	8 years if victim is aged 16 years

under the 'special care' of the offender, who is a step-parent, guardian, foster parent, school teacher, instructor (eg. religion, sport, music), custodial officer, or health professional.		to under 17 years. 4 years if victim is aged 17 years to under 18 years.
Incest, where a person has sexual intercourse with a close family member who is aged 16 years or above.	78A	8 years
Attempted incest	78B	2 years
Sexual assault by self-manipulation, where the offender compels a person, by means of a threat, to sexually penetrate themselves with an object.	80A	14 years, or 20 years if victim is under 10 years.
Aggravated sexual servitude – sexual servitude entails the victim providing sexual services due to the use of force or threats by another person. The listed circumstances of aggravation include that the victim is under 18 years.	80D(2)	19 years

Source: R Johns, *Child sexual offences: an update on initiatives in the criminal justice system*, NSW Parliamentary Briefing Paper No 20/2003. It is noted that 'The maximum penalties quoted above refer to the maximum period of imprisonment that may be imposed if the offender is prosecuted on indictment in the District Court. Some sexual offences may be disposed of summarily, that is, dealt with in the Local Court before a Magistrate. These offences are listed in Schedule 1 of the *Criminal Procedure Act 1986*. If prosecuted in the Local Court, the maximum penalties that may be imposed are much lower'. For maximum penalties in the Local Court, see ss 267-268 of the *Criminal Procedure Act 1986.*

Recent Research Service Publications

To anticipate and fulfil the information needs of Members of Parliament and the Parliamentary Institution.

[Library Mission Statement]

Note: **For a complete listing of all Research Service Publications contact the Research Service on 9230 2093. The complete list is also on the Internet at:**

http://www.parliament.nsw.gov.au/prod/web/PHWebContent.nsf/PHPages/LibraryPublist

BACKGROUND PAPERS

Principles, Personalities, Politics: Parliamentary Privilege Cases in NSW by Gareth Griffith 1/04
Indigenous Issues in NSW by Talina Drabsch 2/04
Privatisation of Prisons by Lenny Roth 3/04
2004 NSW Redistribution: Analysis of Draft Boundaries by Antony Green 4/04
2004 NSW Redistribution: Analysis of Final Boundaries by Antony Green 1/05
Children's Rights in NSW by Lenny Roth 2/05
NSW By-elections, 1965-2005 by Antony Green 3/05
The Science of Climate Change by Stewart Smith 1/06
NSW State Electoral Districts Ranked by 2001 Census Characteristics by Talina Drabsch 2/06
NSW Electorate Profiles: 2004 Redistribution by Talina Drabsch 3/06
Parliamentary Privilege: Major Developments and Current Issues by Gareth Griffith 1/07
2007 NSW Election: Preliminary Analysis by Antony Green 2/07
Manufacturing and Services in NSW by John Wilkinson 3/07

BRIEFING PAPERS

Infrastructure by Stewart Smith 1/04
Medical Negligence: an update by Talina Drabsch 2/04
Firearms Restrictions: Recent Developments by Rowena Johns 3/04
The Future of Water Supply by Stewart Smith 4/04
Plastic Bags by Stewart Smith 5/04
Tourism in NSW: after September 11 by John Wilkinson 6/04
Drug Offences: An Update on Crime Trends, Diversionary Programs and Drug Prisons by Rowena Johns 7/04
Local Development Assessment in NSW by Stewart Smith 8/04
Indigenous Australians and Land In NSW by Talina Drabsch 9/04
Medical Cannabis Programs: a review of selected jurisdictions by Rowena Johns 10/04
NSW Fishing Industry: changes and challenges in the twenty-first century by John Wilkinson 11/04
Ageing in Australia by Talina Drabsch 12/04
Workplace Surveillance by Lenny Roth 13/04
Current Issues in Transport Policy by Stewart Smith 14/04
Drink Driving and Drug Driving by Rowena Johns 15/04
Tobacco Control in NSW by Talina Drabsch 1/05
Energy Futures for NSW by Stewart Smith 2/05
Small Business in NSW by John Wilkinson 3/05
Trial by Jury: Recent Developments by Rowena Johns 4/05
Land Tax: an Update by Stewart Smith 5/05
No Fault Compensation by Talina Drabsch 6/05
Waste Management and Extended Producer Responsibility by Stewart Smith 7/05
Rural Assistance Schemes and Programs by John Wilkinson 8/05
Abortion and the law in New South Wales by Talina Drabsch 9/05
Desalination, Waste Water, and the Sydney Metropolitan Water Plan by Stewart Smith 10/05
Industrial Relations Reforms: the proposed national system by Lenny Roth 11/05

Parliament and Accountability: the role of parliamentary oversight committees by Gareth Griffith 12/05
Election Finance Law: an update by Talina Drabsch 13/05
Affordable Housing in NSW: past to present by John Wilkinson 14/05
Majority Jury Verdicts in Criminal Trials by Talina Drabsch 15/05
Sedition, Incitement and Vilification: issues in the current debate by Gareth Griffith 1/06
The New Federal Workplace Relations System by Lenny Roth 2/06
The Political Representation of Ethnic and Racial Minorities by Karina Anthony 3/06
Preparing for the Impact of Dementia by Talina Drabsch 4/06
A NSW Charter of Rights? The Continuing Debate by Gareth Griffith 5/06
Native Vegetation: an update by Stewart Smith 6/06
Parental Responsibility Laws by Lenny Roth 7/06
Tourism in NSW: Prospects for the Current Decade by John Wilkinson 8/06
Legal Recognition of Same Sex Relationships by Karina Anthony and Talina Drabsch 9/06
Uranium and Nuclear Power by Stewart Smith 10/06
DNA Evidence, Wrongful Convictions and Wrongful Acquittals by Gareth Griffith and Lenny Roth 11/06
Law and Order Legislation in the Australian States and Territories: 2003-2006 by Lenny Roth 12/06
Biofuels by Stewart Smith 13/06
Sovereign States and National Power: Transition in Federal- State Finance by John Wilkinson 14/06
Reducing the Risk of Recidivism by Talina Drabsch 15/06
Recent Developments in Planning Legislation by Stewart Smith 16/06
Commonwealth-State Responsibilities for Health – 'Big Bang' or Incremental Reform? by Gareth Griffith 17/06
The* Workplace Relations Case – *Implications for the States by Lenny Roth and Gareth Griffith 18/06
Crystal Methamphetamine Use in NSW by Talina Drabsch 19/06
Government Policy and Services to Support and Include People with Disabilities by Lenny Roth 1/07
Greenhouse Gas Emission Trading by Stewart Smith 2/07
Provocation and Self-defence in Intimate Partner and Homophobic Homicides by Lenny Roth 3/07
Living on the Edge: Sustainable Land Development in Sydney by Jackie Ohlin 4/07
Women, Parliament and the Media by Talina Drabsch 5/07
Freedom of Information: Issues and Recent Developments in NSW by Gareth Griffith 6/07
Domestic Violence in NSW by Talina Drabsch 7/07
Election Finance Law: Recent Developments and Proposals for Reform by Gareth Griffith and Talina Drabsch 8/07
Multiculturalism by Lenny Roth 9/07
Protecting Children From Online Sexual Predators by Gareth Griffith and Lenny Roth 10/07