Child Abuse Review Vol. **16**: 153–170 (2007)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/car.939

Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet

Stefan C. Dombrowski*
Rider University
USA

Karen L. Gischlar
Lehigh University
USA

Theo Durst
Rider University
USA

Over the past 20 years, the internet has provided an expedient mode of communication and access to a wealth of information. The internet is a valuable tool; however, it can also be detrimental to the wellbeing of children due to numerous online hazards. There is the potential for children to be abused via cyberspace through online sexual solicitation and access to pornography. Indeed, the internet is replete with inappropriate material, including pornography, chatrooms with adult themes and access to instant messaging wherein others could misrepresent themselves. Because children are actively utilizing the internet where unknown others can have access to them or where they can be exposed to inappropriate sexual materials, they require safeguarding and education in safe internet use. The purpose of this article is to provide a discussion of how to safeguard children from and educate them about online sexual solicitation and pornography. We contend that society needs an overall conceptual shift in its attitude towards young people's internet use.

KEY WORDS: internet; child abuse; online grooming; pornography

'A discussion of how to safeguard children from and educate them about online sexual solicitation and pornography'

The internet poses challenges to those responsible for the developmental wellbeing of young people due to numerous online hazards. Although there are a variety of ways in which children can be victimized, two of the more pernicious threats involve online sexual solicitation and access to pornography. As a result, there is need for increased discussion about how to safeguard young people from these threats.

* Correspondence to: Stefan C. Dombrowski, Rider University, 2083 Lawrenceville Road, Lawrenceville, NJ, USA 08648. Tel: (609) 895-5448. E-mail: sdombrowski@rider.edu

 Accepted 22 February 2006

'98% of children between the ages of 9 and 19 years reported regular weekly use of the internet'

Emerging research regarding the online habits of young people suggests high internet use and therefore exposure opportunity to these threats. According to a study conducted in 2004, 75% of all households with children in the United Kingdom had domestic internet access (Livingstone *et al.*, 2005). Moreover, 98% of children between the ages of 9 and 19 years reported regular weekly use of the internet (92% reported access at school; 75% reported home usage; and 64% reported using the internet elsewhere). In this study, 36% of children who claimed to be regular users stated that they had received no instruction in internet safety; more girls than boys reported receiving internet guidance. This same study revealed that 38% of children between the ages of 9 and 19 had received a pornographic pop-up; 36% had visited a pornographic website by accident; and 25% had received pornographic email. These same children were questioned about personal information: 70% stated that they would share personal information on the internet to win a prize and 46% reported having previously released information to a person they had met online (Livingstone *et al.*, 2005).

Computer usage among young people in the United States closely mirrors that of young people in the United Kingdom. According to the National Centre for Education Statistics (as cited in Viadero, 2005), nearly 25% of children under the age of 6 use the internet; 91% of school-aged children (ages 6–18) use computers and 59% of students (ages 4–18) access the internet on a regular basis. Moreover, a second recent US-based study (Cyberspace Research Unit, 2002, as cited in Kennison, 2005) revealed that 33% of child respondents (no ages provided) indicated that they had chatted with someone who later confessed to being up to 5 years older than originally introduced; 40% admitted to engaging in chatroom conversations of a sexual nature; and 25% of child internet users had been solicited for a face-to-face encounter.

'40% admitted to engaging in chatroom conversations of a sexual nature'

In one recent investigation, Greenfield (2004) explored websites that cater to children and adolescents and found that while young people are targets of adult creations on the internet, they are also active participants, engaging in chatrooms, instant messaging and creating websites. Because children are utilizing the internet actively where unknown others can have access to them (Dombrowski *et al.*, 2004) or where they can be exposed to developmentally inappropriate sexual materials (Suzuki and Calzo, 2004), they require safeguarding.

The purpose of this article is to provide a discussion of how to protect children from online sexual solicitation and access to pornography. This discussion will include a presentation of the technology that is available and how it might be utilized for online sexual solicitation and dissemination of pornography. It will also include a discussion of the technological and psychoeducational

DOI: 10.1002/car

mechanisms for safeguarding children from exposure to sexual predators and pornography. Finally, we offer an internet use contract for caregivers and their children.

At the current time, there is no clear scientific consensus regarding the effects that sexually explicit material may have on young people and their development (Thornburgh and Lin, 2004). However, given the lack of knowledge in this area, it may be in the best interest of children to remain vigilant until more research can be conducted. This precaution seems especially salient when one considers that recently, Finkelhor *et al.* (2000) reported that one in five young internet users reported being solicited sexually within a year's time and that one in four of those solicited found the event very distressing. In an Australian study, 27% of adolescent internet users believed they had been contacted by a sexual predator while using a chatroom (Stanley, 2001). A similar percentage (23%) of young people in the Finkelhor study found exposure to pornography very/extremely distressing. Moreover, Finkelhor *et al.* reported that even those children who were distressed by the incident failed to report it to an adult. Thus, it appears that internet sexual solicitation and pornography pose threats to at least a percentage of children and adolescents.

'One in four of those solicited found the event very distressing'

The Internet as a Medium for Online Sexual Solicitation and Exposure to Pornography

The internet has changed the way in which many people establish relationships and communicate. It has also provided a vast, anonymous, expedient means for pornography exposure.

'A vast, anonymous, expedient means for pornography exposure'

A New Medium for Grooming

Particularly among the younger generations, the internet represents a forum for seeking out friendships and romantic relationships (Wolak *et al.*, 2003). Research also indicates the existence of an internet disinhibition effect (e.g. Suler, 2004), whereby some people who establish online relationships share deeply personal information, more so than they would in face-to-face interaction. Some of these individuals may eventually meet in person and may even form more permanent relationships.

There are possible dangers to young people regarding online communication with a previously unknown individual. The internet represents an appealing medium for grooming and soliciting youth for sexual encounters (Medaris and Girouard, 2002). It provides access to countless children in a relatively anonymous environment. An online predator can masquerade as a young person with similar background, age and interests. Further, the cyber predator can

DOI: 10.1002/car

join with the young person in the disinhibition process and encourage discussion of sexual fantasies at too early an age. The purpose of this dialogue might be to play out sexual deviant fantasies. However, the purpose might also be to desensitize the young person to child–adult sexual activity (via sending of pornography, for instance), with the ultimate goal of perpetrating offline (Chase and Statham, 2005; Dombrowski *et al.*, 2004; O'Connell, 2003).

Most of the available empirical literature regarding the profile of an online sexual predator emerges from Finkelhor *et al.*'s (2000) pioneering study regarding online sexual solicitation. The findings from this study revealed that instead of the stereotypical older, middle-aged male perpetrator, juveniles made 48% of the online solicitations and a similar percentage of aggressive solicitations. Although adults made 25% of all solicitations, only 4% were known to be over the age of 25, with most adult solicitors in the age range 18–25. Interestingly, females made about 33% of solicitations and 25% of aggressive solicitations, respectively, which is quite a different percentage from the typical paedophile profile, wherein 85–90% of predators are male. However, given the anonymity of the internet, and because the victim in almost all cases within this study never met the perpetrator, the age and gender of the perpetrator are unverifiable.

'Juveniles made 48% of the online solicitations and a similar percentage of aggressive solicitations'

The impact of such online solicitation on young people's emotional status, however, is quantifiable. Of those who were targeted, 25% felt extremely upset or distressed, with younger people (age 10–13) reporting significantly more feelings of distress than the older young person (age 14–17). It was reported that boys were targeted in about one-third of the solicitations, a much higher percentage than that reported in the general perpetrator literature. The Finkelhor *et al.* (2000) report acknowledged that both parents and reporting authorities may not be aware of the majority of online sexual solicitations. Therefore, caution is urged when attempting to discern who is being targeted and the characteristics of online predators.

A New Medium for Access to Pornography

It is generally agreed that pornographic material is ubiquitous on the internet (Finkelhor *et al.*, 2000) and one need not seek it to become inundated. There are several ways that adults and young people with internet access might be exposed to or gain access to pornography: pop-up advertisements, websites, internet searches and via email. Some of these routes (e.g. websites) are passive. However, a large amount of pornographic content that is presented is unrequested by the recipient (Clearswift, 2005), in an attempt to elicit active engagement. The underlying purpose may be to direct

'A large amount of pornographic content that is presented is unrequested'

DOI: 10.1002/car

the recipient to a pornographic website or a chatroom. However, gathering personal information as a prelude to identity theft or intrusion into the recipient's computer are more likely goals (Clearswift, 2003). Pornography has proven to be a very effective lure for internet users in general.

Although the available literature on the impact that pornography viewing may have on young people is sparse (Thornburgh and Lin, 2004), the limited studies that have been conducted in this area suggest that precautions should be taken to protect children from exposure. For example, in a recent investigation with Taiwanese adolescents, Lo and Wei (2005) found that participants accessed internet pornography much more frequently than they did other sources, such as magazines and books. Furthermore, the results of the Lo and Wei study suggested that this exposure was associated with a greater likelihood of sexually permissive attitudes and behaviour. Haggstrom-Nordin *et al.* (2005) completed a second study in which adolescents in Sweden revealed that a number of male participants became sexually aroused by, fantasized about or tried to perform acts seen in a pornographic film. Moreover, Finkelhor *et al.*'s (2000) research regarding pornography exposure suggests that unwanted exposure can evoke strong negative feelings and lead to significant stress in 23% of exposed young people. However, research is unavailable regarding how long such feelings last or how much of an impact they have on young people. Regardless, Finkelhor *et al.* conclude that such impact 'should mobilize our concern' (p. 30) and requires further discussion and intervention.

'Unwanted exposure can evoke strong negative feelings and lead to significant stress'

Current Technology for Online Sexual Solicitation and Access to Pornography

Since it has been demonstrated that the internet can pose a threat to young people's emotional functioning, young people require safeguarding. As part of this process, the specific technological means by which the internet might serve as a medium for access to pornography or exposure to online sexual solicitation will be discussed.

Technology for Pornography

Young people have ample access to pornography and sexually explicit material. Simple internet searches for words that have sexually explicit meanings often provide access to pornographic images or pornographic websites. In addition, websites containing pornographic material are ubiquitous on the internet. For instance, typing the word 'sex' into the Google search engine brings up more than 87 million sites, many of which are pornographic.

DOI: 10.1002/car

'Pornography sometimes appears via "pop-up" advertisements while browsing websites on the internet'

Pornography sometimes appears via 'pop-up' advertisements while browsing websites on the internet. These advertisements may be pornographic or they might provide a link to a website that contains pornographic material. Ideally, they are targeted at the readership of the website that hosts them. Unfortunately, they are often intrusive and unrelated to the content. As their intention is to divert the reader from the web page, closing one pop-up may open a second or a third (*ad nauseam*). The appearance of pornographic pop-up ads on a computer may indicate that the computer was previously used to access adult material.

Another possible mechanism of transmission of pornography is email exchange. In fact, this may be a common modus operandi of cyber sexual predators who attempt to desensitize young people to the adult–child sexually explicit material. Also, email messages may contain links to pornographic websites or, when opened, may install pop-up advertisements that display the pornographic website. Only by opening an email can its contents be seen. As a result, 'spammers' (senders of unsolicited email) carefully disguise the nature of their messages to convince the recipient to open it. Generally, spam is not targeted and response to such messages, by clicking on a hyperlink, informs the sender that the message was received, increasing the chances of further unsolicited mailings. While the prevalence of pornographic spam may be declining (Clearswift, 2005), the risk of exposure remains high.

'While the prevalence of pornographic spam may be declining (Clearswift, 2005), the risk of exposure remains high'

Children often use P2P (peer to peer) networks for the acquisition of music, video and software (often in violation of the rights of the copyright holder). In these networks, each user acts as a peer, able to download, share and search for files on the computers of other peers. These networks are often used for the illegal distribution of media and have been flagged as a major conduit for child porn. Just as the contents of an email need to be opened prior to viewing, the names of files shared across P2P networks may not reflect their contents. A child may intentionally seek out explicit sexual material or unintentionally be exposed by a misleading title. As these networks were developed to obscure the identity of participants, they offer effective anonymity for those who wish to disseminate pornography.

More prevalent is the use of messaging (synchronous chat networks, such as AOL Instant Messenger) by children. In addition to text messages, most are capable of transmitting voice and images. As always-connected, broadband access becomes more common, these networks offer an easy method of establishing and maintaining geographically extended relationships. They are sufficient to permit the development of fulfilling online relationships, and participants sometimes consider these online friends to be closer and more accepting of their true selves than relationships formed offline (McKenna *et al.*, 2002). The limited stimuli and perceived anonymity

'Participants sometimes consider these online friends to be closer and more accepting of their true selves'

DOI: 10.1002/car

may actually enhance the perception of intimacy (McKenna *et al.*, 2002). Online relationships have been observed to migrate offline, with participants meeting face to face. Paedophiles have been known to use synchronous chat to develop relationships with children and groom them for exploitation (Chase and Statham, 2005). Although the developmental impact of exposure to pornography is less clear, it is clear that exposure to pornography and sexually explicit material is likely given its prevalence on the internet.

Technology for Online Sexual Solicitation

There is a paucity of available literature regarding the specific technologies internet predators use, including whether or not they employ those discussed in the forthcoming section. Furthermore, as reported by Finkelhor *et al.* (2000), about half the young people who are solicited do not report the incident to an adult. Thus, the full extent of technology used by predators remains largely unknown. However, given the potential gravity of online predation, we maintain that it is better to err on the side of caution and, therefore, present a wide range of internet technologies reasonably accessible to online predators. Future empirical research is clearly required regarding the nature of technology use among predators. With this caveat, we provide an overview of two technological resources that sexual predators would likely have access to and employ in online grooming.

'The full extent of technology used by predators remains largely unknown'

Website portals

It is now common practice for even non-technical individuals to publish personal information (name, home address, hobbies and photographs) on the internet, usually on a personal website (e.g. http://www.livejournal.com). This process is often freely available or requires a nominal fee. This information is routinely compiled and indexed by online services (e.g. Google) and becomes readily available through text-based queries. The publication of such material can invite abuse by sexual predators, who could use it to gain advantage when conversing online with minors by posing as individuals with similar age and interests.

Internetworked synchronous chat

This (e.g. AOL Instant Messenger) represents one of the more prevalent internet commutations technologies. With clients available for multiple platforms (including mobile phones) and interoperability between private networks, it is estimated that 52 million people had used synchronous chat as of 2002. More recent figures are unavailable, but the trend suggests increased growth of

DOI: 10.1002/car

this medium, especially among younger users of technology (Pew Internet and American Life Project, 2005). In addition to carrying text messaging, many software clients are capable of transferring voice, photos and files. Unlike email, this is an immediate and localizing technology. A user of synchronous chat often participates in multiple concurrent conversations (Greenfield and Subrahmanyam, 2003), a process which limits time for reflection and may result in a child participant unwittingly revealing personal information to other participants. Additionally, although encryption is sometimes used, data on these networks are generally not considered secure. It is theoretically possible for a child's conversation to be monitored by a sexual predator.

'It is theoretically possible for a child's conversation to be monitored by a sexual predator'

Technological Considerations for Circumscribing Online Sexual Solicitation and Access to Pornography

Technological options for protecting young people from online sexual solicitation and access to pornography are discussed in this section. These measures of protection are generally available from most retail computer outlets or consumer electronics stores. However, the consumer needs to keep in mind that technological mechanisms can be circumvented and that many children are more sophisticated than their parents in regard to technology (Thornburgh and Lin, 2004). Thus, the best line of defence may well be a concerted effort of technology-based tools and education.

Technological Means for Circumscribing Online Sexual Solicitation

Generally, technological considerations such as a firewall, anti-spyware software, wireless encryption and antivirus software will protect young people from a predator's attempt to access personal information. However, these programmess or applications cannot protect a young person from a predator who has already received a young person's contact information. Attention to a child's online activities should be the primary tool for avoiding solicitous interaction. Nonetheless, we contend that technology can offer a degree of protection by facilitating parental monitoring of a home-based computer. Software tools such as firewall security barriers, wireless encryption, antivirus, spyware detection and removal, content filters and usage tracking provide a caregiver with a means to monitor the nature of the young person's communication online (O'Reilly, 2005). While these technologies are far from perfect, they offer a means of reducing general computer security threats from outside and may deter children from engaging in activities which invite solicitation.

'Technology can offer a degree of protection by facilitating parental monitoring of a home-based computer'

DOI: 10.1002/car

Personal firewall

A personal firewall (e.g. Norton Personal Firewall), which can be installed in either the hardware or software, is a system designed to prevent unauthorized access of a private computer. All data entering the computer pass through the firewall barrier, which examines each message and blocks those that do not meet the predetermined security criteria (Internet.com, n.d.). The firewall included in Windows XP Service Pack 2 works in this manner. It is important to keep in mind that firewalls are a passive defence, preventing outside threats from entering the computer unbidden. Generally, they do not prohibit users from installing malicious code such as spyware.

Encryption of wireless network communications

If caregivers have a wireless network, some form of encryption can be protective (O'Reilly, 2005). Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) encryption is commonly available in wireless networking routers. Unencrypted wireless communications are open to eavesdropping by technically astute users and the level of skill required to do this has decreased as wireless communication is becoming more common. For this reason, we advise that unencrypted computer usage in public spaces, such as internet cafes, should be avoided. While the authors consider the prospect for sexual solicitation to be low, there is increased potential for exposure to sexual content in a hacked computer. Most computer communications, such as email and synchronous chat, are sent in plain text. Due to the perceived anonymity of computer-mediated communication, online solicitation may be more tempting. Nevertheless, in almost all cases, the benefits should outweigh the costs (von Solms and Marais, 2004).

'Unencrypted wireless communications are open to eavesdropping by technically astute users'

Privacy filtration software

Through the use of privacy filtration software (e.g. SpyAgent), caregivers can predetermine the type of information that can be transmitted to the child's computer across the internet. The software monitors and filters online communication and blocks pop-up advertisements, some of which are pornographic in nature. Privacy filtration software can also be set to impose time limits on activities, such as chatroom communication (peacefire.org, n.d.). One of the main uses of privacy filtration software is to attempt to block the dissemination of pornography. Filtration methods are described in detail in the next section.

'The use of privacy filtration software'

Another consideration is the use of monitoring applications such as keyloggers (e.g. IamBigBrother) to track children's computer

DOI: 10.1002/car

use. It is recommended that caregivers also check the browser history periodically (Dombrowski and Gischlar, 2005). The authors consider the use of such tools beneficial in drawing attention to changes in a child's online activity. Moreover, use of such may deter children from participating in unapproved activity, if they are aware that monitoring is taking place.

Technological Methods for Circumscribing Access to Pornography

Internet filtration methods

'Filters employ at least one of three methods to determine which user requests to honour'

Filtering of computer communications (e.g. NetNanny) is a primary tool of parents and caregivers in preventing exposure over the internet to inappropriate material, with an estimated 54% of families with teens employing filters (peacefire.org, n.d.). Filters employ at least one of three methods to determine which user requests to honour. 'Inclusion filtering' relies on the creation of a 'whitelist' (a list of specific sites that are to be accessible to the user); all other content is then denied. 'Exclusion filtering', conversely, relies on the existence of a 'blacklist' (sites to be denied). The third method uses 'content filtering' technology that evaluates the requested data and checks to see if its content matches descriptions (keywords, phrases, or image characteristics). As one might expect, exclusionary filtering is the most commonly used in commercial filtering tools, though most filters employ a combination of techniques (Greenfield, 2004). Filters may store the list on the machine that is being blocked or, more securely, elsewhere, usually on a remote server. Filters have become quite easy to implement and are available from several commercial sources. Some internet service providers, such as AOL, offer filtering services to their subscribers.

'Programs that compile lists tend to cast a very wide net, leading to allegations of overblocking'

Due to the volume of material on the internet, most systems employ computer programmes to compile blacklists. The identification and selection of material to block is crucial and, given the vast amount of data on the internet, manual compilation is not practical. The internet is decentralized, and no potent authorities exist capable of enforcing the naming and location of documents (Bradford, 2005). In this absence, software vendors search for internet domains and document contents for words that describe the material to be censored and solicit suggestions from concerned parties. If the blacklist criteria are too closely defined (e.g. 'foo' and 'bar'), alternative spellings or wordings (e.g. 'f00' and 'b@r' or 'foobar') may be missed (Greenfield *et al.*, 2001). As a result, programs that compile lists tend to cast a very wide net, leading to allegations of overblocking (Electronic Freedom Foundation

DOI: 10.1002/car

and Online Policy Group, 2003). Documents with metadata indicating that they relate to the University of 'Essex' or the 'Essex' Police Department may be blacklisted by filters which prevent access to pages containing the word 'sex'. Filters which block the word text containing 'ass' would limit access to information pertaining to embassies (OpenNet Initiative, 2005a,b). Manual additions and deletions are often used to fine-tune the list and improve its accuracy. However, removal of acceptable words from blacklists has proven to be an arduous process (Edelman, 2002). And, content related to health care, human rights, marginalized populations or supporting cultural pluralism often finds its way onto blacklists (Gay & Lesbian Alliance Against Defamation, 1997; Heins and Cho, 2001; Larkin, 2002).

Evasive techniques

Circumvention of filters is possible by users who wish to do so. Several sources are available online offering tools and techniques for evading the censor's eye. Many of these are provided by civil liberties organizations, concerned over the use of filtering software by governments to restrict citizens' access to outside media sources. As many of these governments rely on the same or similar software to that used to censor inappropriate material for children (OpenNet Initiative, 2005a,b), the methods recommended by civil liberties advocates can often be used to circumvent filters that limit the exposure of inappropriate content to minors.

'Evasive techniques break down into two categories'

Evasive techniques break down into two categories. The first technique is to gain administrative access to a home computer, which is often trivial due to lax security procedures, and modify the settings of the home computer web browser or internet connection. The second method involves the use of an external server through which one can route internet traffic. Such relay proxies are non-trivial to establish, but once identified as a conveyance for blacklisted content, are soon added to blacklists. However, free speech activists maintain active relay proxies and disseminate information on their configuration and use (peacefire.org, n.d.). One such relay, Tor (Dingledin *et al.*, 2001–2004), provides anonymous and encrypted access as a P2P network as well. In September 2003, the United States International Broadcasting Bureau established a similar relay to circumvent the Iranian Government's content filters (OpenNet Initiative, 2005b). Finally, relay proxies can be used to confuse content analysis filters by placing requests through a translation service (ex. http://babelfish.altavista.com/). The text of the requested page is retrieved in a nonsense language (e.g. Pig Latin), while images are passed unaltered.

'The United States International Broadcasting Bureau established a similar relay to circumvent the Iranian Government's content filters'

DOI: 10.1002/car

Summary Regarding Efficacy of Technological Protective Measures

Until filtration software is capable of addressing these issues, technology should not be relied upon as the sole method of addressing the unsuitability of internet content for children. Flaws in the design and delivery of filtering technology result in filtering products that are unable to evaluate content effectively. While technology has a place in preventing access or pornographic material, the tools available today are not sufficient to serve as the sole arbiter of suitability. In a similar vein, technological aspects of protecting children, though recommended, are certainly insufficient as a singular means of safeguarding young people. In some cases, the use of technological protective measures only protects identity theft and can provide a false sense of security that a computer is protected from intrusions such as online predators.

Safeguarding Young People: Psychological and Educational Considerations

'Technology should supplement, not replace, the actions of caregivers'

As technology is continually evolving, a technologically aware individual may be able to evade protective measures described previously. Therefore, we contend that technology should supplement, not replace, the actions of caregivers. When improperly configured or misused, the technological options we discuss can result in the curtailment of children's access to educational materials available on the internet. Additionally, these technologies are not foolproof and can often be overcome or evaded by determined individuals on both sides (children, sexual predators and disseminators of pornography) (McCraken, 2005).

'Technologies are not foolproof and can often be overcome or evaded by determined individuals on both sides'

As a result, increased emphasis should be placed upon educating young people and those responsible for their wellbeing about internet safety. When teaching children about safe internet use, developmental aspects must be considered. Communication about safety ought to be tailored to the child's developmental level in language that can be readily understood. Clearly, greater autonomy and more specific discussion should transpire with adolescents, while increased monitoring and concrete language should be provided to children below age 12. Following are a few specific suggestions for safeguarding young people from internet hazards. The effectiveness of these approaches is presently undetermined. Thus, the approaches should be considered tentative until additional empirical validation occurs. This line of discussion is especially important because young people often access the internet outside of the home environment and via mobile phone technology that is much more difficult to monitor. For instance, mobile phone

'Mobile phone technology is increasingly being used to access the internet'

DOI: 10.1002/car

technology is increasingly being used to access the internet, communicate with peers and transmit digital images (Childnet International, n.d.).

Discuss Internet Dangers

It is important for adults to discuss with children and adolescents the risks of the internet (Freeman-Longo, 2000). For instance, inappropriate material such as pornography is readily available to young people. With their caregivers, young people should be encouraged to discuss freely their concerns and curiosities about these sites, rather than wade through them behind closed doors or with peers. Moreover, children should be taught respect for their own bodies and those of others and that pornography is degrading and demeaning. This discussion should be conducted in a developmentally appropriate fashion. Given the lack of discussion that presently transpires regarding sexualized matters on the internet, Finkelhor *et al.* (2000) recommended the need for a much more open climate. Also emphasized to young people must be the extreme danger of sending personal information over the internet, including telephone number, address, family information, and photographs. In fact, some sexual predators might attempt to use this information to groom children for later sexual abuse (Cooper, 2000; US Sentencing Commission, Sexual Predators Act Policy Team, 2000; Childnet International, n.d.).

Supervise Internet Friends

Caregivers should become acquainted with their children's online friends in the same way that they monitor their children's neighbourhood friends. Any discussion about a child's online friends should serve the dual purpose of respecting the child's autonomy and safeguarding him or her from inappropriate material or communication (e.g. exchange of detailed personal information, pornography, or solicitation from a predator) (Medaris and Girouard, 2002). For instance, the dangers of meeting an internet friend offline should be clearly established. If a decision is made to meet offline, then the young person should be accompanied by an adult and should meet in a public location.

'The dangers of meeting an internet friend offline should be clearly established'

Monitor Screen Names

Those responsible for young people should ensure that the child is using a non-sexually suggestive screen name. Sexual predators might more readily target young people who use screen names that are sexually provocative (US Department of Justice, 2001).

DOI: 10.1002/car

Establish a Caregiver–Young People Internet Safety Contract

Parents or legal guardians should consider establishing with their children an internet use safety contract, which specifies in very detailed fashion the guidelines for internet use within and outside of the household. Also, the contract can be used as a means to introduce the topic of internet safety and facilitate discussion about sexualized matters. This material may be uncomfortable for some parents to discuss, but it is essential that a discussion take place (Dombrowski *et al.*, 2004; Dombrowski and Gischlar, 2005; Greenfield, 2004). A review of the contract with the child can facilitate this discussion. (A sample contract is presented in the Appendix.)

'A review of the contract with the child can facilitate this discussion'

Monitor Children's Internet Use

In the same way that parents monitor their child's decision to attend movies or select a video, parents should monitor their children's computer use. Just as most parents would not allow a child to select X-rated movies, they should remain vigilant regarding their child's internet use. In addition, parents might consider periodically reviewing the internet browser history to monitor their children's internet use. This should not be done as a means to control every action taken by the child, but rather to safeguard the child from developmentally inappropriate conversation or material. Finally, parents should consider setting the browser security feature to 'high' to reduce the probability of being exposed to pornography.

Use a Dedicated Computer in a Public Location

To facilitate monitoring of young people's internet use, caregivers ought to consider requiring children to use a dedicated computer for interaction with the internet. In addition, caregivers should consider placing the dedicated computer in a public l ocation, rather than in a secluded part of the dwelling such as a child's bedroom.

'Placing the dedicated computer in a public location, rather than in a secluded part of the dwelling'

Contact the Proper Authorities

In the UK, laws and agencies have been established for the protection of children from online grooming and pornography. The Sexual Offences Act (2003) includes regulations that can be extended to protect young people from online grooming and pornography exposure. For instance, the 2003 Act includes a section which outlaws 'grooming' (see Section 15 and also the Risk of Sexual Harm Orders). Even more progressive, in April 2006, the Home

DOI: 10.1002/car

Office will inaugurate a 'cybertipline' type 24-hour reporting centre (Centre to Tackle Net Paedophiles, 2005). Until the Centre is up and running, the UK has a tipline for reporting online child pornography (http://www.iwf.org.uk). There also is a hotline for reporting suspected online paedophile behaviour: 0800 555 111 or http://www.virtualglobaltaskforce.com/contactus/contactus.html. In the United States, an analogous reporting site is hosted by the National Center for Missing and Exploited Children (NCMEC): http://www.cybertipline.com. Similar reporting sites can be found in other countries of the world, for example, in Canada, a cybertipline that can be accessed on the web at www.cybertip.ca or via phone at 1-866-658-9022 (Government of Canada, 2005). Australia also has put some precautionary measures in place. While the country does not offer a cybertipline, a website (i.e. http://www.afp.gov.au/afp/page/Crime/E-Crime/OCSET.htm) is available that offers a means for reporting pornography and suspicious online activity. Users of the website are also encouraged to report concerns to their local police departments (Australian Federal Police, 2005).

After reporting the suspected solicitation or pornography dissemination, it is recommended that one also contact the internet service provider (ISP; e.g. AOL) to notify them of the suspicion. These steps will alert the authorities about potential online solicitation and pornography dissemination, placing them in a better position to safeguard young people from such a threat.

'It is recommended that one also contact the internet service provider'

Conclusion

The more traditional approach to protecting young people from online threats—discussion and education about the internet's dangers in a developmentally appropriate fashion—will likely prove to be most effective. Technology expands significantly on a daily basis. For example, mobile phone technology and handhelds add another dimension to both pornography dissemination and grooming (see http://www.childnet-int.org/publications/policy.aspx for more details). These devices have the technological capabilities to receive email, files, pictures and pop-up advertisements and also enable the user to surf the internet. Furthermore, these technological modalities are less able to be traced. Thus, savvy individuals can generally circumvent technological mechanisms of protection, which tend to be one step behind the adroit hacker. Therefore, psychological and educational considerations are essential and should be considered the primary measures of protection. However, added protection is offered by a combination of psychoeducational and technological protective considerations that restrict access to inappropriate materials.

'Psychological and educational considerations are essential and should be considered the primary measures of protection'

DOI: 10.1002/car

References

Australian Federal Police. 2005. http://www.afp.gov.au/afp/page/Crime/E-Crime/OCSET.htm [29 September 2005].

Bradford S. 2005. Is the Net doomed? *PC World* **23**: 111–114.

Centre to Tackle Net Paedophiles. 2005. http://news.bbc.co.uk/1/hi/uk_politics/4399183.stm [25 July 2005].

Chase E, Statham J. 2005. Commercial and sexual exploitation of children and young people in the UK—A review. *Child Abuse Review* **14**: 4–25.

Childnet International. N.d. http://www.childnet-int.org/ [5 August 2005].

Clearswift Ltd. 2003. http://www.clearswift.com/ [25 March 2005].

Clearswift Ltd. 2005. http://www.clearswift.com/news/item.aspx?ID=864 [2 August 2005].

Cooper A (ed.). 2000. *Cybersex: The Dark Side of the Force: A Special Issue of the Journal of Sexual Addiction and Compulsivity*. Brunner-Routledge: Philadelphia.

Dingledin R, Mathewson N, Syverson P. 2001–2004. *Tor* [Computer Software]. The FreeHaven Project: San Marcos, CA. Retrieved on July 22, 2005 from http://tor.eff.org/overview.html

Dombrowski SC, Gischlar K. 2005. Keeping children safe from online sexual victimization. *Communiqué* **34**: 4–6.

Dombrowski SC, LeMasney J, Ahia C, Dickson S. 2004. Protecting children from online sexual predators: technological, psychoeducational, and legal considerations. *Professional Psychology Research and Practice* **35**: 65–73.

Edelman B. 2002. *Supplemental Expert Report of Benjamin Edelman Multnomah County Public Library et al., vs. United States of America, et al.* http://cyber.law.harvard.edu/people/edelman/pubs/aclu-031302.pdf [21 July 2005].

Electronic Freedom Foundation and Online Policy Group. 2003. http://www.eff.org/Censorship/Censorware/net_block_report/net_block_report.pdf

Finkelhor D, Mitchell K, Wolak J. 2000. *Online Victimization: A Report on the Nation's Youth*. National Center for Missing and Exploited Children.

Freeman-Longo R. 2000. Children, teens, and sex on the Internet. *Sexual Addiction and Compulsivity* **7**: 75–90.

Gay & Lesbian Alliance Against Defamation. 1997. *Access Denied: The Impact of Internet Filtering Software on the Lesbian and Gay Community*. Gay & Lesbian Alliance Against Defamation: New York.

Government of Canada. 2005. http://www.cybertip.ca/PDFs/en/media_releases/CybertipPressReleaseJan24.pdf [29 September 2005].

Greenfield P. 2004. Developmental considerations for determining appropriate Internet use guidelines for children and adolescents. *Applied Developmental Psychology* **25**: 751–762.

Greenfield P, Rickwood P, Tran HC. 2001. Effectiveness of Internet filtering software products. Internet: http://www.aba.gov.au/internet/research/filtering/filtereffectiveness.pdf [20 July 2005].

Greenfield PM, Subrahmanyam K. 2003. Online discourse in a teen chatroom: new codes and new modes of coherence in a visual medium. *Journal of Applied Developmental Psychology* **24**: 713–738.

Haggstrom-Nordin E, Hanson U, Tyden T. 2005. Associations between pornography consumption and sexual practices among adolescents in Sweden. *International Journal of STD & AIDS* **16**: 102–107.

Heins M, Cho C. 2001. http://www.mega.nu:8080/ampp/internetfilters.html [21 July 2005].

Kennison P. 2005. [Review of the book *Child Sexual Abuse and the Internet:*

DOI: 10.1002/car

Tackling the New Frontier.] *International Journal of Police Science and Management* **7**: 67–70.
Larkin M. 2002. Pornography-blocking software may also block health information sites. *The Lancet*, 360. DOI: 10.1016/S0140-6736(02)11939-8
Livingstone S, Bober M, Helsper E. 2005. www.children-go-online.net [22 July 2005].
Lo V, Wei R. 2005. Exposure to Internet pornography and Taiwanese adolescents' sexual attitudes and behaviour. *Journal of Broadcasting & Electronic Media* **49**: 221–237.
McCraken H. 2005. Rule one: they're our machines. *PC World* **23**: 17.
McKenna K, Green A, Amie S, Gleason, Marci EJ. 2002. Relationship formation on the Internet: what's the big attraction? *Journal of Social Sciences* **58**: 9–31.
Medaris M, Girouard C. 2002. Protecting children in cyberspace: the ICAC task force program (*OJJDP Juvenile Justice Bulletin*). US Department of Justice: Washington, DC.
O'Connell R. 2003. *A Typology of Child Cybersexploitation and Online Grooming Practices*. University of Central Lancashire: Preston.
OpenNet Initiative. 2005a. *Internet Filtering in China in 2004–2005: A Country Study*. OpenNet Initiative: Cambridge, MA, Cambridge, UK, Toronto. Retrieved on July 19 from http://www.opennet initiative.net/studies/china ONI_China_Country_Study.pdf
OpenNet Initiative. 2005b. *Internet Filtering in Iran in 2004–2005.* OpenNet Initiative: Cambridge, MA. Retrieved on July 19 from http:// www.opennetinitiative.net/stud ies/iran/ONI_Country_Study_Iran.pdf
O'Reilly D. 2005. PC protection: 10-step security. *PC World* **23**: 119–120.
peacefire.org. (n.d.). http://www.peacefire.org/censorware [24 April 2005].
Pew Internet and American Life Project. 2005. http://www.pewinternet.org/ [3 August 2005].
Sexual Offences Act. 2003. Chapter 42. http://www.opsi.gov.uk/acts/acts2003/ 20030042.htm#aofs [2 August 2005].
Stanley J. 2001. Child abuse and the Internet. *Child Abuse Prevention Issue* **15**. Australian Institute of Family Studies, National Child Protection Clearinghouse: Melbourne.
Suler J. 2004. The online disinhibition effect. *CyberPsychology & Behavior* **7**: 321–326.
Suzuki L, Calzo J. 2004. The search for peer advice in cyberspace: an examination of online teen bulletin boards about health and sexuality. *Applied Developmental Psychology* **25**: 685–698.
Thornburgh D, Lin H. 2004. Youth, pornography, and the Internet. *Issues in Science and Technology* **20**: 43–48.
US Department of Justice. 2001. Internet crimes against children. *Office for Victims of Crime Bulletin.* US Department of Justice: Washington, DC.
US Sentencing Commission, Sexual Predators Act Policy Team. 2000. *Sentencing Federal Sexual Offenders: Protection of Children from Sexual Predators Act of 1998*. US Sentencing Commission: Washington, DC.
Viadero D. 2005. High tech preschoolers. *Education* Week **24**: 9.
von Solms B, Marais E. 2004. From secure wired networks to secure wireless networks—what are the extra risks? *Computers & Security* **23**: 633–637.
Wolak J, Mitchell K, Finkelhor D. 2003. Escaping or connecting? Characteristics of youth who form close online relationships. *Journal of Adolescence* **26**: 105–119.

Appendix

Caregiver–Young Person Contract for Safe Internet Use

Youth's responsibilities

I, _____, have read this internet safety contract together with my caregiver(s). I unde stand the rules of internet use as they have been explained to me by my caregiver(s). I will keep this contract clearly posted by my computer. If I should run into any problems or have questions while using the internet (including instant messages and chatrooms), I will contact my caregiver(s) immediately. I promise to abide by the rules listed in this contract, whether I am using the internet at home or away from home.

- I will never share my home telephone number, home address, or the name of my school over the internet.
- I will never share information about my family or myself, such as where my parents work or the names of my brothers and sisters.
- I will not share internet passwords with anyone, including my close friends.
- I will not use my real name in chatrooms; I will always use my screen name or a 'nickname'. I will choose my screen name with my caregiver(s).
- I will never meet someone I have talked to on the internet, unless my caregiver approves and comes with me to the meeting.
- I will never send pictures over the internet or upload pictures to a website without my caregivers' permission.
- I will tell my caregivers if anyone is threatening me or using bad or inappropriate language. I will always let my caregiver know if someone online makes me feel uncomfortable or afraid.
- I will always keep in mind while talking to people on the internet that they are strangers and that I need to follow the same rules for strangers on the internet that I do in person.
- I will get my caregivers' permission to sign on and download/upload material.
- I will remember that the internet rules listed above apply whether I am using the internet at home or away from home. These rules apply to *all* internet use, including computers, mobile phones and handheld devices.

Caregivers' responsibilities

I, _____, will supervise my child's internet use to ensure that he/she is using this tool responsibly and is not endangering him/herself by communicating and interacting inappropriately with strangers that he/she may meet via the internet.

- I will respect my child's need for a degree of privacy while speaking to friends and exchanging email on the internet.
- I will take the time to learn about my child's interests on the internet and will monitor his/her online activity through such means as checking the browser history.
- I will attempt to ensure my child's safety through installing safeguarding software (e.g. firewalls, virus and spyware scanners).
- I will set rules for internet use in my home, including the time and length of sessions.
- I will try to get to know my child's internet friends, just as I do his/her other friends.
- I will teach my child to use judgement while online and I will ensure that my child is educated about the hazards of internet use and how to use the internet safely. I will stress the importance of following these rules whether he/she is using the internet at home or away from home.
- I will be aware of the procedure for contacting my online service provider for advice if someone should act inappropriately with my child. In addition, if I suspect someone has been soliciting my child for sexual purposes, I will contact my local police department and the Virtual Global Task Force at http://www.virtualglobaltaskforce.com/contactus/uk.html for appropriate reporting procedures. If I suspect someone has been sending pornographic materials to my child, I will contact my local police department and the Internet Watch Foundation at 0800 555 111 or http://www.iwf.org.uk/

Caregiver(s)' signature _____

Young person's signature _____

Date _____

DOI: 10.1002/car