Professional Psychology: Research and Practice
2004, Vol. 35, No. 1, 65–73

Copyright 2004 by the American Psychological Association, Inc.
0735-7028/04/$12.00 DOI: 10.1037/0735-7028.35.1.65

Protecting Children From Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations

Stefan C. Dombrowski, John W. LeMasney, and C. Emmanuel Ahia
Rider University

Shannon A. Dickson
California State University, Sacramento

Professional psychologists should more fully understand the dangers of online sexual solicitation and ways in which to protect youth from sexual predators who use the Internet. Although the Internet has many positive aspects, one of the most pernicious aspects is its potential use for online sexual predation. The Internet represents a medium that allows sexual predators access to countless children in a relatively anonymous environment. This article reviews the general strategies of sexual perpetrators and their characteristics, as well as the online strategies and characteristics of the cyber sexual predator. Information on how to protect children from this crime through a review of technological, psychoeducational, and legal considerations is provided. A description of the relevant laws as they relate to online solicitation and practicing psychologists is also provided.

A recent national survey indicated that about one in five youth are solicited for sex over the Internet annually (Finkelhor, Mitchell, & Wolak, 2000; Mitchell, Finkelhor, & Wolak, 2001). This is an alarming statistic given the potentially deleterious impact of sexual abuse. Sexual abuse robs children of their dignity, threatens their social–emotional integrity, and places them at great developmental disadvantage (Cicchetti & Toth, 1995). Although there is no definitive post-sex-abuse syndrome, sexual abuse can have an adverse impact on a child's cognitive, physical, academic, and psychological development (Dombrowski, 2003). The outcomes of sexual abuse persist well into adulthood and often include higher levels of anxiety, depression, substance abuse, eating disorders, relationship problems, and suicidal ideation (Browne & Finkelhor, 1986; Dombrowski, Ahia, & McQuillan, 2003; Kendall-Tackett, Meyer, & Finkelhor, 1993; Oddone, Genuis, & Violato, 2001). Moreover, a significant number of prostitutes were subjected to sexual abuse while in their youth (Silverman, Reinherz, & Giaconia, 1996). As a result of the deleterious and persistent nature of sexual abuse, laws have been established for the protection of children from this insidious crime.

The Internet, however, poses challenges to those who foster the well-being of youth (Office of Juvenile Justice and Delinquency Prevention [OJJDP], 2000). It provides access to countless children and represents an efficient way for predators to "groom" and then solicit youth for future sexual abuse (Medaris & Girouard, 2002). In the United States, more than 30 million children (45% of all children younger than 18) use the Internet (*Online Risks for Youth*, n.d.). By 2005 the U.S. Department of Justice estimates that approximately 77 million children will be online (U.S. Department of Justice, 2001).

The Internet has changed the way in which many people interact. It is now a much more acceptable forum for seeking out friendships and romantic relationships, particularly among younger generations (Wolak, Mitchell, & Finkelhor, 2003). Some people who establish online relationships share deeply personal information without ever meeting. Others who communicate online sometimes meet in person and may eventually form more permanent relationships. The early stigma associated with meeting someone on the Internet and then establishing an in-person relationship has faded. Although this way of meeting can have advantages, there are also significant dangers. An individual can masquerade as a youth with similar background, age, and interests. This, in fact, is a common modus operandi of sexual predators whose goal is to gain access to youth for the purpose of sexual abuse.

Stefan C. Dombrowski received his PhD in school psychology from the University of Georgia and his MBA from the University of Connecticut. He completed a postdoctoral fellowship in child-clinical psychology at the University of California, Davis Medical Center. He is an assistant professor in the school psychology program at Rider University. His research interests include child maltreatment and the investigation of the impact of prenatal factors on later child psychological development. He also conducts research on cognitive and learning assessment issues.

John W. LeMasney received his BFA in sculpture from the University of the Arts in Philadelphia. He is the manager of the Office of Instructional Technology at Rider University and the primary instructional technologist in the Center for Innovative Instruction, a part of the Teaching and Learning Center at Rider University. His area of research is in the effects of instructional technology and how various technologies can affect the teaching and learning process in and out of the classroom.

C. Emmanuel Ahia received his PhD in counseling psychology from Southern Illinois University and his JD from the University of Arkansas. He is an associate professor in the Counseling Services Program at Rider University. His research interests include mental health law.

Shannon A. Dickson received her PsyD in counseling psychology from the California School of Professional Psychology (Alameda) and is an assistant professor in the Counseling Services Program at California State University, Sacramento. Her research interests include child maltreatment and multicultural issues.

Correspondence concerning this article should be addressed to Stefan C. Dombrowski, Department of Graduate Education and Human Services, Rider University, Memorial 202, 2083 Lawrenceville Road, Lawrenceville, NJ 08648-3099. E-mail: sdombrowski@rider.edu

The OJJDP (2000) indicated that mental health professionals should more fully understand the potential hazards of online sexual solicitation. We extend this warning even further and maintain that professional psychologists, educators, parents, and any individuals who ensure the well-being of children should also increase their understanding of the risks. Practicing psychologists are in a position to raise awareness of the risks and offer protective measures via direct relationships with child clients and their caregivers or through consultative roles via in-service presentations or workshops. One study indicated that those who should be most aware of online solicitation—counselors specifically responsible for providing treatment to sex offenders—ironically had only limited knowledge of these matters (Buttell & Carney, 2001). Furthermore, the study reported that the treatment agency did not have an organizational policy for monitoring and limiting the use of the Internet by offenders, a situation that should clearly be circumscribed.

Although the Internet has numerous hazards (e.g., pornography) for youth and there are a variety of ways in which children can be victimized, in this article we focus on increasing awareness of one subset: online sexual solicitation. We first present an overview of the characteristics of the sexual predator, followed by a review of the possible mechanisms by which sexual predators lure children. An understanding of the nature of sexual predators and general methods of sexual perpetration is necessary to effectively protect children from online solicitation: Those attempting online solicitation may employ some of the same grooming strategies. Second, we describe how the Internet is an efficient vehicle for the solicitation of youth and how sexual predators might use the Internet for such purposes. Third, we discuss ways in which to protect children from online sexual solicitation. This discussion includes both technological as well as psychoeducational approaches that should be familiar to professional psychologists who either directly counsel children and adolescents or provide consultation services to those who foster the developmental well-being of youth (e.g., schools, caregivers). Last, we review the relevant laws for professional psychologists with respect to reporting online sexual solicitation. Thus, this article provides mental health professionals with an understanding of the risks involved in online solicitation and with a means of serving as a resource to others on how to protect youth from this danger.

Characteristics of Sexual Predators

Sexual predators are a heterogeneous group, and as a result it is difficult to define a typology of the sexual predator. Historically, sexual predators have been portrayed as older, European American, middle-class men (Gudjonsson & Sigurdsson, 2000). However, few studies have examined in detail the characteristics of predators, particularly as these characteristics relate to race, ethnicity, culture, and sexual abuse (Kenny & McEachern, 2000). Recent research suggests that adult sexual predators range in age from 18 to 72, with a preponderance between 30 and 42 years of age (Elliott, Browne, & Kilcoyne, 1995). Yet sexual perpetration is not limited to adulthood. Many youth also commit acts of sexual perpetration (Miranda & Corcoran, 2000), and as many as 30%–60% of child molestation cases in the United States are committed by children under the age of 18 (G. E. Davis & Leitenberg, 1987; Fieldman & Crespi, 2002).

Both adult and child sexual predators are often characterized as less socially adept (G. E. Davis & Leitenberg, 1987; Fagan, Wise, Schmidt, & Berlin, 2002). Adult sexual predators are reported to have more sexually deviant fantasies (i.e., having sex with children; having sex with nonhuman objects; Fagan et al., 2002). Statistics indicate that sexual perpetrators of all ages are predominantly male, accounting for 85%–90% of cases of sexual perpetration (G. E. Davis & Leitenberg, 1987; Fagan et al., 2002; Ferrara, 2002). Research also indicates that adult sexual perpetrators (e.g., pedophiles) who target children under age 12 experience a high occurrence of psychiatric, substance abuse, and personality disorders (Murray, 2000). Nearly 75% experience anxiety or depression, whereas more than half experience lifetime substance abuse problems. Furthermore, 60% of pedophiles experience a personality disorder: obsessive compulsive (25%), antisocial (22.5%), narcissistic (20%), or avoidant (20%). Although sexual perpetrators may experience coexisting psychiatric disorders, there are also sexual perpetrators without such psychiatric difficulties. In the majority of cases, sexual perpetrators were themselves the victims of sexual abuse while in their youth (Becker, 1998; Elliott et al., 1995; Ferrara, 2002; Glasser et al., 2001). Despite mainstream perceptions, the typical sexual perpetrator is often someone well known to the child (i.e., uncle, relative, family friend, neighbor; Fieldman & Crespi, 2002). In this respect, the reality of sexual abuse conflicts with the highly publicized (and mainstream) perception that sexual abuse involves a stranger. Sexual perpetration by a stranger is less common, accounting for anywhere from 5% to 34% of the offenses (Elliott et al., 1995; Snyder, 2000).

The characteristics of online sexual predators are even more illusory (Finkelhor et al., 2000). There has only been one study to date that has investigated this topic. Mitchell et al. (2001) conducted a study and found that nearly 48% of online predators were under the age of 25, and nearly one quarter were female. Further, 97% of online solicitations were from strangers (Mitchell et al., 2001). Of youth who use the Internet regularly, 19% were the targets of unwanted sexual solicitation over a period of a year (Mitchell et al., 2001). The Mitchell et al. study suggests that the profile of online predators might be different from that of typical predators. However, given that the Internet allows individuals to misrepresent their identity, it is difficult to determine specific characteristics of online predators (Lanning, 2001; Medaris & Girouard, 2002; Mitchell et al., 2001).

The Grooming Process

Despite the very serious social problem of sexual abuse, there is a paucity of empirical data on how sexual abuse transpires. There are even fewer data available on the Internet grooming process. The typical information on the Internet grooming process comes in the form of pamphlets or bulletins based on actual case reports that have been compiled by governmental agencies overseeing the prosecution of Internet crimes (U.S. Sentencing Commission, Sexual Predators Act Policy Team, 2000). In this article, we present more general information on grooming, as this process seems to be consistent across modalities, whether in person or online. Accordingly, our discussion of the Internet grooming process should be considered hypothetical and subject to future empirical validation.

Sexual predators typically engage in “grooming” (Berliner & Conte, 1990), a process marked by initial prosocial contact in which the predator gains the affection, interest, and trust of children/adolescents through kind words and deeds (Conte, Wolf, & Smith, 1989). Children/adolescents of any age find this appealing, as they have a strong desire for attention, validation, and acceptance. For instance, the sexual predator might bring gifts to the child, play with the child, or just listen to the child and show interest in the child's world. In the case of online grooming, the process may advance from e-mail correspondence to the exchange of gifts or pictures. If the child/adolescent seems receptive, the predator might escalate the grooming process by initiating more overt contact. For example, the predator might present pornographic material in attempt to desensitize the child/adolescent to sexualized content and normalize sexual activities (Berliner & Conte, 1990; U.S. Department of Justice, 2001; U.S. Sentencing Commission, Sexual Predators Act Policy Team, 2000). If the child/adolescent does not seem to object or perhaps displays curiosity, the sexual predator might attempt to establish a meeting to continue the process of grooming.

As the grooming process continues, the predator tries to gain the trust of the victim while attempting to desensitize the child/adolescent to the purpose of touch. Touching may progress from borderline sexual behavior, such as a lower back rub, to more overt sexual behavior, such as fondling. Following overt sexual contact, the predator will attempt to conceal the abuse. There are a variety of strategies used to conceal sexual abuse, ranging from physical threats to psychological subterfuge. Research indicates that offenders under the age of 18 generally use physical threats and coercion to conceal abuse, whereas adult predators more often use psychological manipulation (Becker, 1998; Miranda & Corcoran, 2000). Following an act of perpetration, the adult predator might threaten the youth's sense of psychological security by indicating that the youth had willingly participated in sexual contact and will therefore be equally culpable if discovered. When caught and confronted about their actions, sexual predators rationalize their behavior by claiming that the youth either wanted sexual contact or initiated it. They also maintain that the youth has not been harmed by the abuse, often overlooking the youth's resulting feelings of fear, anxiety, and pain from the abuse (Conte et al., 1989).

Characteristics of Youth Targeted by Sexual Predators

There are certain characteristics that might predispose a youth to sexual victimization. The literature indicates that physically attractive youth with low self-esteem are often targeted for sexual abuse (Elliott et al., 1995). More typically, youth who come from dysfunctional and impoverished families are often victims of sexual abuse (Kenny & McEachern, 2000). It is noted that living in poverty makes many families susceptible to social problems of all kinds, including sexual abuse (Derezotes & Snowden, 1990).

Conte et al. (1989) were among the first researchers to provide data on the characteristics of youth most often targeted for abuse. These researchers interviewed convicted sexual perpetrators who reported that children displaying the characteristics of friendliness, openness, and persuadability were often targeted with greater frequency. According to Conte et al., perpetrators also reported targeting adolescents who experienced behavioral difficulties or emotional distress (e.g., those who were emotionally disturbed or who had a history of peer rejection or school difficulties). This is consistent with the general literature on victimization, which indicates that troubled youth who experience social alienation or depression are generally at risk for victimization of any type (Acierno, Resnick, Kilpatrick, Saunders, & Best, 1999). Perpetrators feel that maladjusted children often lack support systems in their lives and may be more amenable to attention and affection and therefore vulnerable to perpetration. Given their troubled backgrounds, these youth are also easier to discredit if allegations of abuse surface. Everson and Boat (1989), however, provided data indicating that fewer than 10% of children who allege abuse contrive stories of abuse. Although both child and adult perpetrators have been described as being less socially adept, the research indicates that predators are skilled at discerning and then manipulating vulnerable youth (Conte et al., 1989; Miranda & Corcoran, 2000). This can be perilous. Children of all ages may be susceptible to manipulation and intimidation due to a lack of emotional maturity and an inherent power differential as a result of being a minor. Those who are most vulnerable to victimization are least likely to have caregivers actively involved in their lives (Glasser et al., 2001).

How Predators Might Use the Internet

It should be noted that the mechanisms by which predators solicit youth online require further study and empirical validation, as there is limited scholarly literature on this topic. Much of what is available emerges from governmental publications that present anecdotal case reports of individuals who have been convicted or children who have experienced perpetration via online solicitation (OJJDP, 2000; U.S. Department of Justice, 2001). What follows is a description of how predators might use the Internet to solicit children. Although the literature is lacking on the specific characteristics of youth who are at risk for online perpetration, one may extrapolate the findings from the more general perpetration literature to delineate characteristics of youth who might be especially vulnerable.

The Internet provides sexual predators with access to countless children and represents a new way in which to engage in the grooming process. Nearly 30 million children (45% of youth under age 18) use the Internet in the United States (*Online Risks for Youth,* n.d.). Although the Internet initially delimits face-to-face contact, it represents an efficient, private, and economical medium for establishing numerous online relationships with children (U.S. Sentencing Commission, Sexual Predators Act Policy Team, 2000). This makes the Internet an attractive and dangerous vehicle for potential sexual abuse. Once an online relationship has been established, the predator can begin to groom children with the goal of establishing offline contact. This contact might begin with e-mail or chat room contact and then progress to phone conversations and then to face-to-face meetings. Further, presentation of pornography may occur in an attempt to normalize and desensitize the youth (Young, 1997).

Given their greater autonomy, sexual curiosity, and mobility, teenagers may be likely targets for online solicitation (Mitchell et al., 2001). These youth have a greater capacity to meet the predator at an agreed upon location. There have even been reported cases in which the predator has sent money to cover the cost of a child's transportation to a meeting (Freeman-Longo, 2000; *Online Risks for Youth,* n.d.). In addition, and consistent with the broader solicitation literature, the limited available research on online solicitation suggests that youth who seem in need of help, have poor self-images, and reveal in chat rooms that they have emotional difficulties might also be targeted more frequently (Mitchell et al., 2001). These children also seem to be more inclined to seek out and establish relationships via the Internet (Wolak et al., 2003). Thus, troubled youth who experience social alienation and symptoms of depression may be vulnerable to online solicitation (U.S. Department of Justice, 2001; U.S. Sentencing Commission, Sexual Predators Act Policy Team, 2000).

Chat rooms may be a favored solicitation medium of online predators. Within chat rooms, youth who express agreement and are somewhat passive may also be targeted frequently, although this topic deserves greater study (Mitchell et al., 2001). Internet predators might also scan chat rooms for sexually suggestive screen names and target youth who use such names. Overall, the scholarly literature on the mechanisms of online solicitation is extremely limited and requires further empirical validation. A likely scenario is that the risk factors that predispose youth to offline victimization will also contribute to a higher likelihood of online solicitation. Furthermore, adolescents, rather than children, seem to be the more likely targets of online solicitation, owing in part to their greater mobility, sexual curiosity, and autonomy (Finkelhor et al., 2000). This feature may distinguish the victims of online solicitation from victims of sexual solicitation more generally.

Mechanisms of Online Solicitation

In the following discussion we describe the technological approaches that predators might use to establish an online relationship with a child or an adolescent. Essentially, there are two ways for a predator to use the Internet to establish a relationship for the purpose of solicitation: e-mail and instant messaging (or chatting). Following initial contact, the predator might use other technological means to intensify the grooming process, such as gaining access to the youth's Web site or presenting pornographic material. However, initial communication is most easily facilitated through e-mail and instant messaging. These two means of communication are vulnerable to virtual eavesdropping by technologically aware individuals whose goal is to establish offline contact. What follows is a description of some of the ways in which an online predator might gain access to children's personal information and communication over the Internet.

Virtual Ethernet Stethoscopes: "Sniffers"

A technologically aware predator can use virtual Ethernet stethoscopes called "sniffers" to listen to chat client traffic on a particular network and therefore gather information about an unsuspecting youth. A sniffer is a software application used by hackers to listen to Internet provider traffic (Ethereal, n.d.). The term *sniffer* is a play on the notion of an ether addict. Chatting or instant messaging is a communication medium such as that used in the America Online (AOL) Instant Messenger client. The AOL Instant Messenger client allows subscribers to identify and exchange messages instantaneously with other subscribers via the Internet. A chat client is any piece of software that allows one to type messages back and forth over the Internet. Some are very simple and allow only the exchange of typewritten text. Many others are more sophisticated and allow not only the exchange of typewritten text but also the formatting of text, icon representation, secure communications, exchange of files, Short Message Service messaging, and many other features.

While eavesdropping on a child's chat client communication, the predator can gain access to a child's personal interests (e.g., hobbies; favorite music or food). Gaining knowledge of this information, the online predator might more readily establish a relationship with a child by indicating enjoyment of similar interests and activities. Initially, online predators might misrepresent themselves as having the same age or race as the youth (Baker, 2002). (There is no viable way to discern whether an individual with whom one is corresponding is a similar-aged peer or a 45-year-old predator masquerading as a peer.) After gaining the youth's trust, the predator might then inform him or her of the age or racial difference (U.S. Department of Justice, 2001). In doing so, the predator might, for instance, reframe an age difference by asking the youth whether or not he or she would be interested in having an uncle or a big brother. As part of this process, the online predator has likely been presenting or exchanging pornographic material for the purpose of normalization and desensitization of sexual material (Cooper, 2000; Young, 1997). After the online relationship has been solidified, the predator might attempt to establish offline contact (e.g., telephone or face-to-face contact) with the youth. Once this contact has been established, the youth's safety is imperiled, and he or she may be at great risk for sexual abuse (Baker, 2002).

Web Site Portals

In addition to using Ethernet sniffers to gather information about a child, a predator might also ascertain information through a Web site created by the child. For instance, Yahoo! allows for the easy creation of free Web sites (e.g., http://www.geocities.com) that can be used to display personal information such as name, e-mail address, telephone number, home address, and any other information. In fact, these Web sites may be flexibly created to include details about hobbies, group sites that deal with those interests, and specific information about the child. These sites may also be constructed free of charge, requiring only authorization, a free username, and a password from the sponsoring Web site portal (Free Webspace Directory, n.d.). If a predator ascertains the account name of a targeted child (via chat, for instance), it is easy to determine whether the child has posted any additional personal information on the Web site portal. This information, in turn, might be used as a means to facilitate communication with youth through deception by claiming similar interests (Wolak et al., 2003).

Trojan Horse and Worm Virus Infiltration

Trojan horse and worm virus attacks represent two of the most dangerous threats to computer security (Lo, 2003). The term *Trojan horse* gets its name from the legendary hollow gift horse, given to the city of Troy, in which soldiers lay waiting for the opportunity to attack. Like the legendary Trojan horse and the typical sexual predator, the Trojan virus appears desirable but is actually harmful. Trojans are usually installed secretly inside popular software that have been obtained or downloaded from the

Internet (often against copyright laws) over peer-to-peer clients (e.g., Kazaa). Many Trojans work by installing a tiny Web or other kind of server on a system and sending a message to the attacker that the system has been infiltrated and is now ready to send personal information upon request (Lo, 2003). For instance, suppose an expensive software program has been downloaded illegally through a peer-to-peer client. When an individual uses the program that has been infected with a Trojan, remote attackers can copy private information such as e-mail address, credit card information, age, address, and telephone numbers. Similarly, a worm virus can be used to access personal information contained on a computer, although it is typically used to disrupt computer systems (*Virus Encyclopedia,* n.d.). Both Trojan and worm viruses allow a third party to take over a computer remotely or retrieve stored personal information. Online sexual predators might use such viruses to ascertain information about a child and then to express similar interests and gain advantage during communication with unsuspecting youth.

How to Prevent Online Solicitation

In the following section we describe both technological and psychoeducational ways to protect youth from online perpetration. Given the insidious nature of sexual abuse, it is essential to discuss these methods with youth and to implement them in the home and within settings where children have access to the Internet. Practicing psychologists are in a position to serve as an important resource for the dissemination of such information, either directly through their counseling of youth or indirectly through consultative relationships with caregivers or systems that foster the well-being of children.

Technological Protective Considerations

Although there are specific steps that can be taken from a technological perspective to protect youth from online sexual solicitation, many of these measures can be circumvented by a motivated and technologically sophisticated sexual predator. Therefore, when attempting to protect children from online solicitation, one should include not only technological but also psychoeducational measures of protection. Professional psychologists may serve directly by informing their child clients or their clients' caregivers of these protective measures or indirectly through in-service presentations to systems that foster the well-being of children. The following are technological approaches that might be used to protect children from online solicitation:

Installation of a firewall. It is essential to install a firewall. A software or hardware firewall provides a barrier between a computer and the Internet that prevents third parties from controlling the computer. As a result, it prevents unauthorized users from gaining access to private information by restricting Internet traffic to approved activities (e.g., Norton Personal Firewall; Symantec, 2003). A firewall can be effective in preventing infiltration by a Trojan horse or a worm virus.

Installation of antivirus or anti-Trojan software. It is very important to install antivirus or anti-Trojan software to prevent a computer from being infiltrated by a Trojan horse virus or a worm virus. If antivirus software is installed and updated or if a firewall has been installed, then either can prevent the Trojan horse or worm virus from functioning (Lo, 2003; Symantec, 2003).

Installation of a key logger. A key logger is computer software that allows the storage of all characters that have been typed on a particular machine (Keylogger, n.d.). It provides a digital fingerprint of communication coming from a particular computer. Accordingly, it might be an efficient means of reviewing the type of communication patterns children are having on a computer. Questions of privacy and trust might arise, particularly among adolescents, who are at a stage of development where autonomy is paramount. However, much of this can be discussed and then put into writing in the form of a contract between the caregiver and the child/adolescent to avoid unnecessary trespassing on the youth's privacy. (A caregiver–child contract is provided in the Appendix.) A key logger may be acquired from any retail outlet that sells computer technology.

Monitoring the browser history. Another way to observe communication behavior online is through the use of the computer's Web browsers. For instance, on Microsoft Internet Explorer, this information is contained in the history section of the browser. Much of this communication is stored for several weeks, and those responsible for the well-being of children should periodically check to see what sites children are visiting.

Encryption. Another line of technological defense against predators might be through the use of encryption. If this action is used, it will be necessary to find out if there are encryption filters available for the computer's chat client. AOL Instant Messenger, for instance, allows for two-way encryption. The use of encryption will hide text from predators who are using an Ethernet sniffer to spy on a child's Internet-based communication. A potential drawback is that in order for encryption techniques to work, the intended recipient must also have encryption capabilities enabled. If both parties have encryption capabilities, then use of encryption techniques will block spying on communication but will allow the intended recipient to receive and send protected messages freely.

Privacy filtration. Through privacy filtration software, such as Netscape Nanny 5.0, personal information may be blocked from transmission over the Internet (NetNanny, 2003). The software program allows those responsible for the well-being of children to specify the information that can and cannot be transmitted. The software also provides tools for blocking intrusive pop-up ads, some of which may be pornographic, and allows for time-limit controls on Internet use.

Application tracking and usage. One can monitor the amount of time spent using particular computer programs (e.g., video games) or applications (e.g., the Internet) through the use of application tracking software (Timetrack, 2000). Application programs, such as TimeTrack, can often be downloaded free of charge from the Internet and represent an additional way to monitor children's computer use. Application tracking programs are versatile, with numerous recording and reporting options. Although they cannot directly monitor the specific online communication a child is having, they can determine how much time a child might spend within a chat room or surfing the Internet. Application tracking programs generally record at 5-s intervals the amount of time spent on particular computer programs or applications.

Chat logging. Another effective way to monitor children's online communication is through the use of chat logging. A chat logger records and saves on the hard drive the plain text communication that occurs over a chat client (eBlaster 3.0, n.d.). This way, online conversations can be monitored for appropriate content.

Psychoeducational Protective Considerations

Although several technological avenues exist for the protection of children, technologically savvy predators may be able to circumvent such protective measures. As a result, educating youth and those responsible for their well-being regarding online safety as well as monitoring Internet use are the most important components of protection from online solicitation. It is noteworthy that both education and monitoring should occur in a developmentally appropriate fashion, and professional psychologists are particularly well suited to facilitate this process. The way in which the Internet is discussed and monitored should depend on the age of the child/adolescent. Understandably, greater autonomy should be provided to adolescents, whereas increased monitoring should be used for children.

Recognizing and discussing Internet dangers. It is important to discuss with children and adolescents the risks of the Internet (Freeman-Longo, 2000). Some children (and adults) may falsely assume that information sent over the Internet is private and only received by the intended recipient. However, it is not difficult to gain access to communications sent through this medium (Cooper, 2000). One of the most important facets of protection is to instill in youth an awareness of the dangers of sending personal information over the Internet, including telephone number, address, family information, and social security number. As part of this education, it is important to discuss how some individuals might attempt to use this information to engage in sexual abuse (U.S. Sentencing Commission, Sexual Predators Act Policy Team, 2000). This discussion should be presented at a developmentally appropriate level; however, it is essential that children and adolescents be made aware of the dangers of individuals who attempt to meet them online and the strategies such individuals might employ toward this end.

Education of this type is especially important, as youth spend considerable time on the Internet outside of the home. Thus, there are limitations to the kinds of prevention suggestions that focus on the home computer. If a child visits another child's house or some public venue where Internet use is less supervised, then the dangers that have been discussed are present again. It is for this reason that prevention through psychoeducation is vital.

Supervising Internet friends. Just as it is important for caregivers to get to know their children's neighborhood friends, caregivers should also become familiar with their children's online friends. Many children establish and maintain friendships over the Internet, some of which may be unhealthy and potentially harmful (Freeman-Longo, 2000). Depending upon the age of the child/adolescent, a discussion about each online friend should be done in a manner that respects the privacy of the youth while safeguarding him or her from inappropriate communication (e.g., exchange of personal information, pornography, or other illicit material). Finally, it is important for children and adolescents to exercise caution and judgment about requests to meet potential online friends. Given the duplicitous nature of sexual predators, the predator might attempt to initiate offline contact with a child or adolescent (Medaris & Girouard, 2002). There should be a discussion about that potential danger. For children under age 16, a caregiver should supervise an offline meeting. When the child is over the age of 16, the adolescent should be instructed, at a minimum, to bring a friend or older sibling with him or her to the meeting location. In either situation, the meeting should take place in a public location in the event of any malicious intent.

Understanding and approving children's screen names. Those responsible for youth should know what screen name is being used by the children they oversee. Sexual predators scroll through networks and might target more repeatedly those youth who use sexually provocative screen names (U.S. Department of Justice, 2001). Therefore, caregivers should ensure that their children/adolescents are using screen names devoid of sexual innuendo.

Establishing a caregiver–child contract. Parents should establish with their children an Internet use contract. This contract should specify in very detailed fashion the guidelines for Internet use within the household. The intent of the contract should be to establish boundaries for the child. It should not be used to control every online behavior taken by a child. The contract itself might even be helpful for structuring and then reinforcing a possible discussion between caregivers and children regarding safe Internet use. (A sample contract is presented in the Appendix.)

Placing the computer in a public location. In an effort to monitor children's Internet use, caregivers should make sure that the computer is placed in a public location. This will provide caregivers with greater ability to monitor children's computer use.

Contacting the Cyber Tip Line. When there has been suspicion of online sexual solicitation of youth, the following toll-free telephone number provided by the National Center for Missing and Exploited Children (NCMEC) should be contacted: (800)-843-5678. The NCMEC also maintains a Web site that allows for the reporting of online solicitation. This site may be accessed at http://www.cybertipline.com. It is recommended that after reporting the suspected solicitation to the NCMEC, one should also contact the Internet service provider (ISP; e.g., AOL, Verizon, Comcast) to notify them of the suspicion. The ISP will then determine whether a temporary cessation or termination of service is warranted. These steps will alert the authorities about potential online solicitation, placing them in a better position to safeguard youth from such a threat.

Guidance to Professional Psychologists Who Evaluate or Treat Sex Offenders

Monitoring of Predators' Online Activities

Psychologists who treat or evaluate convicted or alleged sexual predators should be aware of several issues. First, sexual predators should be prohibited from using e-mail, instant messaging, or any application that could facilitate online communication with youth. The online activities of sexual predators should also be monitored to ensure that child pornography is not being viewed or exchanged. The continued involvement in online solicitation or child pornography would hamper treatment effectiveness, potentially endanger children, and perpetuate the predator's cycle of psychopathology. L. Davis, McShane, and Williams (1995) discussed ways to limit and monitor sexual predators' Internet use without impinging on their legitimate need to access the Internet.

Psychologists who assess sexual predators should attempt to determine the scope of the predator's Internet use for youth sexual victimization or involvement in pornography. If appropriate, the evaluation should contain treatment recommendations that address the predator's Internet use. Overall, psychologists evaluating or treating sexual predators who overlook the online activities of sexual predators are in danger of failing to adequately protect society by allowing the predator continued access to youth (Buttell & Carney, 2001). This oversight could potentially jeopardize a youth's psychological integrity and predispose the youth to future victimization by sexual predators (Young, 1997).

Legal Considerations

Various legislative bodies nationwide have enacted laws intended to facilitate the apprehension and prosecution of persons involved in Internet child abuse and exploitation. Child exploitation statutes such as Title 18 of the United States Code (U.S.C.), Sections 2241–2260, and 2422, for example, criminalize Internet, interstate, and international child sexual coercion, exploitation, solicitation, and abuse.[1] Evidence collected pursuant to the enforcement of these laws can be used for federal or state prosecution of predators for child abuse, exploitation, and sexual solicitation.

Of particular relevance to this article is the fact that the Protection of Children from Sexual Predators Act (1998) requires online service providers to report evidence of child pornography and exploitation to the "Cyber Tip Line" at the NCMEC. This requirement is clearly similar to 42 U.S.C. 13031, which requires the reporting of child abuse in general and by cyber professionals (e.g., Web site administrators) in particular. Although this particular law does not expressly burden psychologists and other mental health professionals with the duty to report online solicitation to authorities, it is inconceivable that failure to report would be deemed by courts to be consistent with prudent and ethical professional practice. Moreover, criminal sanctions for failure to report can be based on child abuse laws, already in existence in all states (Roach, 1998).

For example, if client Michael, age 42, seeks therapy from psychologist Dr. F. and shared with her his ongoing cyber child abuse interactions with Mindy, age 12, an accurate interpretation of New Jersey child abuse laws requires Dr. F. to report this 13031 type abuse to authorities. Therefore, each professional psychologist confronted with knowledge of a client's online sexual solicitation must consider whether or not the harm to the child victim is at the same harm threshold that existing state child abuse prevention laws seek to prevent. If indeed it is, then failure to report could neither be viewed as consistent with these laws nor in the best interest of the child. The child abuse laws of Arizona, Florida, Hawaii, Massachusetts, New Jersey, New York, and Pennsylvania are just a few examples of laws that might require psychologists to report online sexual solicitation.[2] The following actions are recommended on the basis of the mandated reporting laws of most states:

Documentation. Under child abuse laws, documentation is critical for investigation, prosecution, and clinical referral and/or intervention. Documentation should include the history of online sexual solicitation (e.g., the date and time of all known incidents; other children involved; the rewards the children were promised and/or paid for participation; an accurate sequence of events; and the identity of parents, guardians, and others who may have knowledge of the incidents).

Reporting. Immediate action must be taken to report the incidents to ISPs and law enforcement. As was mentioned earlier, an immediate call to the Cyber Tip Line at the NCMEC is consistent with the legal duty of childcare professionals to report child abuse. It should be remembered that reporting sex crimes against children is an exception to clinical confidentiality.

Care and treatment. Knowledge of any form of child sexual abuse and exploitation imposes an ethical duty on child clinical professionals to provide or initiate a process that will lead to care and treatment. If a therapeutic relationship exists between the child and a professional, failure to provide or to cause treatment to be provided may be considered client abandonment, for which the psychologist may be held accountable.

Conclusion

The cost to children and society of sexual perpetration is too great to overlook the hazards of online solicitation. In this article, we have described measures that should be taken to protect youth from this insidious crime, and these measures should be fully employed. We have also examined cyber sexual exploitation laws and reminded psychologists of the possible legal reportability of these crimes.

[1] For information on these statutes, see http://www.prevent-abuse-now.com/law2ac.htm

[2] See Ariz. Rev. Stat. Ann. § 13–3620 (West Supp. 1998); Fla. Stat. Ann. § 415.504 (West 1989); Haw. Rev. Stat. § 350–1.1 (Westlaw through 2001 3rd Sp. Sess.); Mass. Ann. Laws ch. 119 (West Supp. 1985); N.J. Stat. Ann. § 9: 6-8.10 (West Supp. 1993); N.Y. Soc. Ser. Law § 413 (West 1983); N.J. Stat. Ann. § 9: 6-8.10 (West 1993); N.Y. Soc. Ser. Law § 413 (West 1983).

References

Acierno, R., Resnick, H., Kilpatrick, D. G., Saunders, B., & Best, C. L. (1999). Risk factors for rape, physical assault, and post-traumatic stress disorder in women: Examination of differential multivariate relationships. *Journal of Anxiety Disorders, 13,* 541–563.

Baker, L. (2002). *Protecting your children from sexual predators.* New York: St. Martin's Press.

Becker, J. V. (1998). What we know about the characteristics and treatment of adolescents who have committed sexual offenses. *Child Maltreatment, 3,* 317–330.

Berliner, L., & Conte, J. R. (1990). The process of victimization: The victim's perspective. *Child Abuse and Neglect, 11,* 497–506.

Browne, A., & Finkelhor, D. (1986). Impact of child sexual abuse: A review of the research. *Psychological Bulletin, 99,* 66–77.

Buttell, F. P., & Carney, M. M. (2001). Treatment provider awareness of the possible impact of the Internet on the treatment of sex offenders: An alert to a problem. *Journal of Child Sex Abuse, 10,* 117–125.

Cicchetti, D., & Toth, S. L. (1995). A developmental psychopathology perspective on child abuse and neglect. *Journal of the American Academy of Child and Adult Psychiatry, 34,* 541–65.

Conte, J. R., Wolf, S., & Smith, T. (1989). What sexual offenders tell us about prevention strategies. *Child Abuse and Neglect, 13*(2), 293–310.

Cooper, A. (Ed.). (2000). *Cybersex: The dark side of the force: A special issue of the Journal of Sexual Addiction and Compulsivity.* Philadelphia: Brunner-Routledge.

Davis, G. E., & Leitenberg, H. (1987). Adolescent sexual offenders. *Psychological Bulletin, 101,* 417–427.

Davis, L., McShane, M. D., & Williams, F. P. (1995). Controlling computer access to pornography: Special conditions for sex offenders. *Federal Probation, 59*(2), 43–58.

Derezotes, D., & Snowden, L. (1990). Cultural factors in the intervention of child maltreatment. *Child and Adolescent Social Work, 7,* 161–175.

Dombrowski, S. C. (2003). Mandated reporting for mental health professionals: An overview. *Directions in Rehabilitation Counseling, 14,* 71–80.

Dombrowski, S. C., Ahia, C. E., & McQuillan, K. (2003). Protecting children through mandated child abuse reporting. *The Educational Forum, 67*(2), 76–85.

eBlaster 3.0 [Computer software]. (n.d.). Retrieved from www.keystroke.net

Elliott, M., Browne, K., & Kilcoyne, J. (1995). Child sexual abuse prevention: What offenders tell us. *Child Abuse and Neglect, 19,* 579–594.

Ethereal [Network protocol analyzer for Unix and Windows]. (n.d.). Retrieved January 20, 2003, from http://www.ethereal.com

Everson, M. D., & Boat, B. W. (1989). False allegations of sexual abuse by children and adolescents. *Journal of the American Academy of Child and Adolescent Psychiatry, 28,* 230–235.

Fagan, P. J., Wise, T. N., Schmidt, C. W., & Berlin, F. S. (2002). Pedophilia. *Journal of the American Medical Association, 288,* 2458–2465.

Ferrara, F. F. (2002). *Childhood sexual abuse: Developmental effects across the lifespan.* Pacific Grove, CA: Brooks/Cole.

Fieldman, J. P., & Crespi, T. D. (2002). Child sexual abuse: Offenders, disclosure, and school-based initiatives. *Adolescence, 37,* 151–161.

Finkelhor, D., Mitchell, K. J., & Wolak, J. (2000). *Online victimization: A report on the nation's youth.* Alexandria, VA: National Center for Missing and Exploited Children.

Free Webspace Directory. (n.d.). Retrieved June 12, 2003, from http://www.free-webspace.org

Freeman-Longo, R. E. (2000). Children, teens, and sex on the Internet. *Sexual Addiction and Compulsivity, 7*(1–2), 75–90.

Glasser, M., Kolvin, I., Campbell, D., Glasser, A., Leitch, I., & Farrelly, S. (2001). Cycle of child sexual abuse: Links between being a victim and becoming a perpetrator. *British Journal of Psychiatry, 179,* 482–494.

Gudjonsson, G. H., & Sigurdsson, J. F. (2000). Differences and similarities between violent offenders and sex offenders. *Child Abuse and Neglect, 24,* 363–372.

Kendall-Tackett, K. A., Meyer, L. W., & Finkelhor, D. (1993). Impact of sexual abuse on children: A review and synthesis of recent empirical studies. *Psychological Bulletin, 113,* 164–180.

Kenny, M. C., & McEachern, A. G. (2000). Racial, ethnic, and cultural factors of childhood sexual abuse: A selected review of the literature. *Clinical Psychology Review, 20,* 905–922.

Keylogger [Software]. (n.d.). Retrieved January 20, 2003, from http://www.keylogger.com

Lanning, K. V. (2001). *Child molesters: A behavioral analysis.* Washington, DC: National Center for Missing and Exploited Children.

Lo, J. (2003). *Trojan horse attacks.* Retrieved June 9, 2003, from http://www.irchelp.org/irchelp/security/trojan.html

Medaris, M., & Girouard, C. (2002). *Protecting children in cyberspace: The ICAC task force program* (OJJDP Juvenile Justice Bulletin). Washington, DC: U.S. Department of Justice.

Miranda, A. O., & Corcoran, C. L. (2000). Comparison of perpetration characteristics between male juvenile and adult sexual offenders: Preliminary results. *Sexual Abuse: Journal of Research and Treatment, 12,* 179–188.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2001). Risk factors for and impact of online sexual solicitation of youth. *Journal of the American Medical Association, 285,* 3011–3014.

Murray, J. B. (2000). Psychological profiles of pedophiles and child molesters. *Journal of Psychology, 134,* 211–224.

NetNanny [Computer software]. (2003). Retrieved January 20, 2003, from http://www.netnanny.com

Oddone, E., Genuis, M. L., & Violato, C. (2001). A meta-analysis of the published research on the effects of child sexual abuse. *Journal of Psychology, 135,* 17–36.

Office of Juvenile Justice and Delinquency Prevention. (2000). *Use of computers in the sexual exploitation of children.* Washington, DC: U.S. Department of Justice.

Online risks for youth. (n.d.). Retrieved January 8, 2003, from http://www.netsmartz.org/parents/home/rskinfo.html

Protection of Children from Sexual Predators Act of 1998, 18 U.S.C. § 3486 (West 1998).

Roach, W. H. (1998). *Medical records and the law.* Gaithersburg, MD: Aspen.

Silverman, A. B., Reinherz, H. Z., & Giaconia, R. M. (1996). The long-term sequelae of child and adolescent abuse: A longitudinal community study. *Child Abuse and Neglect, 20,* 709–723.

Snyder, H. N. (2000). *Sexual assault of young children as reported to law enforcement: Victim, incident, and offender characteristics* (Report No. NCJ 182990). Washington, DC: U.S. Department of Justice, National Center for Juvenile Justice, Bureau of Statistics.

Symantec. (2003). Norton personal firewall [Computer software]. Cupertino, CA: Author.

U.S. Department of Justice. (2001). Internet crimes against children. *Office for Victims of Crime Bulletin.* Washington, DC: Author.

U.S. Sentencing Commission, Sexual Predators Act Policy Team. (2000). *Sentencing federal sexual offenders: Protection of children from Sexual Predators Act of 1998.* Washington, DC: Author.

Timetrack [Computer program]. (2000). Retrieved January 20, 2003, from http://www3.telus.net/jz/timetrk

Virus encyclopedia. (n.d.). Retrieved from www.viruslist.com

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2003). Escaping or connecting? Characteristics of youth who form close online relationships. *Journal of Adolescence, 26,* 105–119.

Young, S. (1997). The use of normalization as a strategy in the sexual exploitation of children by adult offenders. *Canadian Journal of Human Sexuality, 6,* 285–295.

Appendix

Parent–Child Contract for Internet Safety

I, ________________, have read this contract with my mom/dad/legal guardian ______________________ and I understand the rules of Internet use in my home. I will keep this contract clearly posted by my computer. If I should run into any problems while surfing the Internet or while in a chat room, I will contact my parents and abide by the rules listed in this contract.

Child's Responsibilities

- I will never give out my home telephone number or address over the Internet.
- I will not give out any information about my family, such as where my parents work and the names of my brothers or sisters.
- I will not use my real name in chat rooms and will always use a "nickname."
- I will not tell a stranger on the Internet where I go to school.
- I will never meet someone I have talked to on the Internet unless my parents approve and come with me to the meeting.
- I will never send pictures of my family or me over the Internet without my parents' permission.
- I will not talk to anyone over the Internet who makes me feel uncomfortable; I will tell my parents right away when this happens.
- I will tell my parents if anyone is threatening me or using bad language.
- I will always keep in mind while talking to people on the Internet that they are strangers and some strangers can be bad.
- I will obey my parents' rules about being on the Internet, including obtaining their permission to sign on and download material.

Parents' Responsibilities

I _______________________ will supervise my child while he or she is on the Internet to ensure they are using this tool responsibly and not endangering themselves by communicating inappropriately with strangers they may meet over the Internet.

- I will not use this contract as a way to control every action taken by my child on the Internet.
- I will respect my child's need for a degree of privacy while speaking to friends on the Internet.
- I will spend time with my child and learn about what interests him or her on the Internet.
- I will be aware of the procedure for contacting my online provider for advice should someone appear to be bothering my child. I will also contact the Cyber Tip Line at (800)-843-5678 or http://www.cybertipline.com if I suspect someone has been soliciting my child for sex or sending pornographic material to my child.
- I will teach my child to use judgment while online and I will ensure that my child is educated about the hazards of Internet use and how to safely use the Internet.

Parent's Signature ____________________________________
Child's Signature ____________________________________
Date ___________

Received March 18, 2003
Revision received June 20, 2003
Accepted July 25, 2003 ■