



Online Solicitation of Children

A Report Regarding the Use of the Internet to Facilitate the Commission of Sex Crimes
Including Recommendations for Ensuring Child Safety

Prepared for the
Texas Legislature and the Office of the Governor, Criminal Justice Division
Pursuant to Section 8, Senate Bill 912, 79th Regular Session, 2005

September 1, 2006

Council on Sex Offender Treatment
1100 West 49th Street
Austin, Texas 78756

Table of Contents

Background	Page 3
Executive Summary	Page 3
General Internet Information	Page 4
Victims of Internet Crimes	Page 4
Demographics of an Internet Offender	Page 5
Identifying Internet Offenders	Page 6
How Sex Offenders Select Victims	Page 7
Child Pornography	Page 8
Child Pornography on the Internet	Page 8
Using Child Pornography to Groom Children	Page 10
Reporting Internet Crimes	Page 12
General Recommendations	Page 13
Specific Recommendations/General Terms	Page 15
General Recommendations for Internet Safety	Page 15
Chat Programs or Instant Messaging (IM) Recommendations	Page 17
Online Language	Page 18
Finding a Child's Online Blog	Page 19
Preventing Access to Blogs	Page 19
Internet Game Recommendations	Page 20
Music Downloading	Page 20
Finding and Reporting Child Pornography	Page 20
What to Do If You Are Being Cyberstalked	Page 20
Characteristics of Youth Who Form Close Online Relationships	Page 21
Warning Signs That a Child May Be at Risk	Page 21
Resource Websites	Page 22
Safe Sites for Children	Page 24
Internet Blocking, Filtering, and Usage Tracking Software	Page 24
References	Page 26
Appendix A (Florida's Cyberstalking Law)	Page 30
Appendix B (Court Cases)	Page 31
Appendix C (Online Lingo)	Page 31

Questions or comments regarding this report may be directed to
Allison Taylor, Executive Director, Council on Sex Offender Treatment
1100 West 49th Street
Austin, Texas 78756
E-mail: csot@dshs.state.tx.us
Phone: (512) 834-4530
Fax: (512) 834-4511

Online Solicitation of Children

A Report Regarding the Use of the Internet to Facilitate the Commission of Sex Crimes Including Recommendations for Ensuring Child Safety

Background

Section 8 of Senate Bill 912 (79th Texas Legislative Session, 2005) requires the Council on Sex Offender Treatment to study the ways in which sexually violent predators, as defined by Section 841.002, Health & Safety Code, and other persons who commit sexually violent offenses, as defined by Article 62.01, Code of Criminal Procedure, use the Internet to meet or otherwise establish contact with potential victims. The bill required that not later than September 1, 2006, the Council on Sex Offender Treatment shall report the results of the study to the criminal justice division of the governor's office and to the legislature, and shall include with the report recommendations for ensuring the safety of residents of this state from sexually violent predators or offenders who use the Internet to facilitate the commission of sex offenses.

Executive Summary

Sexual exploitation can result in numerous physical and psychological consequences for children that may be multiplied for victims of child pornography because they face a lifetime of possible revictimization through the continued distribution of videos, photographs, or computer images depicting their exploitation (Klain, 2001). The mass media continues to feed into the stereotype that all Internet offenders are "predators" or "pedophiles". According to ABC World News Tonight in June 2006, there are approximately 563,000 registered sex offenders nationally. However, decades of research indicates that only ten percent (10%) of sex offenders are truly predatory in nature.

This is not to discount that Internet victimization is one of the most dangerous Internet threats, but society must be cautious in using such characteristics without empirical data to support such a homogenous label. In the National Juvenile Online Victimization (N-JOV) study, approximately seventy-eight percent (78%) of cases, the offender was one of the victim's family members, second generation family member such as grandparents, uncle or aunt, or stepparents or parent's intimate partner.

Children exploring the Internet for education and entertainment are at risk of encountering sexually explicit material, sexual exploitation, and Internet offenses while remaining undetected by parents. The Internet has become a conduit for sexually explicit material and offenses against children. Children are extremely vulnerable to victimization due to their curiosity, naiveté, and trusting nature. These crimes present law enforcement with many complex problems due to the fact that they transcend jurisdictional boundaries and often involve multiple victims in multiple states and countries. Internet crimes must be pursued vigorously by law enforcement.

The greatest obstacle facing law enforcement is that children and parents do not report the majority of Internet crimes. In situations where the abuse is a parent, a relative, or acquaintance, the abuse may be more likely to come to light inadvertently as a result of inquiries by social welfare and reports from neighbors, rather than as a result of police inquiries into online crime (Wolak, 2005, in press). Community involvement, parental supervision, and early intervention and prevention programs on Internet safety are essential in protecting children from online solicitation and exposure to pornography.

General Information

The computer age presents complex challenges for law enforcement, victim services, parents, legislators, and the community. The proliferation of computer technology obviously has enhanced our lives in many ways, such as enabling improved productivity and efficiency at work, school, and home (U.S. Department of Justice, 2001). Unfortunately, this technology is not without potential threats and harm for criminals to prey upon innocent victims. According to ABC World News Tonight in June 2006, there are approximately 563,000 registered sex offenders nationally. End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (ECPAT) International reports violence and harms against children and young people in cyberspace include: the production, distribution, and use of materials depicting child sexual abuse; online solicitation; exposure to materials that can cause psychological harm, lead to physical harm, or facilitate other detriments to a child; and harassment and intimidation.

Today the Internet has approximately two hundred (200) million users worldwide who can communicate with each other (ECPAT International 2002). Children of all ages are browsing the Internet. Forty-five (45%) of children in the United States, more than thirty (30) million of whom are younger than eighteen (18) use the Internet (Pew Internet & American Life Project, 2001). By 2005, it was estimated that there are seventy-seven (77) million children online (Youth Internet Safety). Approximately one hundred three (103) million people use instant messaging (IM) programs such as AOL's AIM, Microsoft's MSN Messenger, and others (Austin American Statesman, 2006). MySpace.com reports more than eighty-five (85) million members (New York Reuters, 2006) and the number of visitors to MySpace went from 4.9 million in 2005 to currently over sixty-seven (67) million (Kornblum, 2006). Like most new technological developments, this brings both positive and negative implications, especially for parents and their children (NetSmartz, 2006).

A 2005 survey of 1,500 youths conducted by the Crimes Against Children Research Center found a decrease in the proportion of online youths that received online sexual solicitations from one (1) in five (5) in 2000 to (1) in seven (7) in 2005. However, the study found a pronounced increase from twenty five percent (25%) in 2005 to thirty-four percent (34%) in 2006 of Internet users age ten (10) to seventeen (17) who were exposed to unwanted sexual material. Increases in unwanted exposure to sexual material were seen across every age group. Four percent (4%) of youths reported that online solicitors had requested nude or sexually explicit photographs of themselves. Solicitations from offline friends and acquaintances increased from three percent (3%) in 2000 to fourteen percent (14%) in 2005. Four percent (4%) of all youth Internet users received aggressive sexual solicitations in which the solicitor asked to meet the youth in person, called the youth on the telephone, or sent the youth offline mail, money, or gifts (Wolak, 2006).

Victims of Internet Crimes

Until the rise of the Internet, the subjects of sexual abuse images were mostly females. But in recent years, many more boys are featured in abuse images available online (Cooper, 2005). Children are easy targets for cyberstalkers to sexually victimize them.

The N-JOV study found that the victims of family offenders tended to be younger than acquaintance victims (82% were under 12). Almost all of the family member victims were female (93%), non-Hispanic Caucasians (95%), and were children aged 6-12 (45%). By contrast, almost half the acquaintance victims were male (49%) and seventy-one percent (71%) of the acquaintance victims were teens. Coercion was more commonly used in family cases (63%) as compared to thirty percent (30%) in acquaintance cases.

In a 2005 survey of 1,500 youths conducted by the Crimes against Children Research Center, seventy percent (70%) of girls were targeted for sexual solicitation and thirty percent (30%) were boys. Eighty-one (81%) were ages fourteen (14) or older and three percent (3%) were eleven (11) years old (Wolak, 2006).

In a 2006 survey conducted by the National Center for Missing and Exploited Children and Cox Communications, fourteen percent (14%) of children have actually met face-to-face with a person the child had known only online. Thirty percent (30%) have considered meeting someone the child has only communicated with online. Seventy-one percent (71%) reported receiving messages online from a person the child did not know and forty-five percent (45%) were asked for personal information by a person the child did not know. Of that forty-five percent (45%), forty percent (40%) of children replied to chat when the child received online messages from a person they did not know.

Some children are especially at risk due to a range of vulnerability-enhancing factors common to all environments (ECPAT, 2005). They are in socially and economically difficult situations, have experienced sexual abuse and exploitation, are lonely, or feel alienated from their parents. Others have low self-esteem, feel awkward, are confused about their personal identity and sexuality, and lack confidence. Gender is also seen to be a risk factor, with seemingly more girls than boys appearing to be harmed through cyberspace interactions (although boys are increasingly featured in pornographic images circulating online) (ECPAT, 2005).

Demographics of an Internet Offender

Sex offenders and child pornographers are a heterogeneous mixture. Before the advent of the Internet, between one-fifth and one-third of people arrested for possession of child pornography were also involved in actual abuse (Dobson, 2003). The majority are male and come from all socio-economic and racial backgrounds. Many are skilled in technology. Not all fit the clinical classification of “pedophilia” (Subgroup Against Sexual Abuse, 2005). The mass media continues to feed into the stereotype that all Internet offenders are “predators” or “pedophiles”. This is not to discount that Internet victimization is one of the most dangerous Internet threats but society must be cautious in using such characteristics without empirical data to support such a homogenous label. We have to remember that in a previous generation, campaigns to prevent child molestation characterized the threat as “playground predator” or “stranger danger” so that for years the problem of youth, acquaintance, and intra-family perpetrators went unrecognized (Wolak, 2000).

In the N-JOV study, in almost half the cases (44%), the offender was one of the victim’s family members: most commonly a second degree relative such as grandparents, uncle or aunt (18%) or stepparents or parent’s intimate partner (16%). In the remainder of cases, the offender was an acquaintance including neighbors or community members (16%), friends or relatives of the victim’s peers (12%), and teachers (9%).

In Wolak’s 2000 study, adults were responsible for twenty-four percent (24%) of sexual solicitations and thirty-four percent (34%) of aggressive solicitations. In twenty-four percent (24%) of solicitations, the victims were not aware if the perpetrator was a youth or an adult. Forty-eight percent (48%) of sexual solicitations were made by juveniles. Sixty-seven percent (67%) of solicitations came from males, nineteen percent (19%) from females, and thirteen percent (13%) unknown. Thirteen percent (13%) of youths knew where the solicitor lived.

In a 2005 survey of 1,500 youths conducted by the Crimes against Children Research Center, the perpetrators were largely male (73%). Of the females who made aggressive sexual solicitations sixty-four percent (64%) were younger than eighteen (18) and thirty-six percent (36%) were eighteen (18) to twenty-four (24). The survey found an increase in the proportion of adult solicitors from twenty-four percent (24%) in 2000 to thirty-nine percent (39%) in 2005. Youths met eighty-six percent (86%) of perpetrators online and seventy-nine percent (79%) of all solicitations occurred on the youth's home computer. Eighty-six percent (86%) of youths received an aggressive solicitation in chatrooms and instant messages. Of the solicitations thirty-one percent (31%) were aggressive in which the solicitor made, or attempted, offline contact with the youth (Wolak, 2006). In the 2000 survey there were no reports of sexual assault as a result of the online sexual solicitation. However, in the 2005 survey of 1,500 youth, two victims were sexually assaulted by an online solicitor (.001333%).

In an analysis of 600 cases of child sexual abuse in which the Internet played a role, either the offender-victim relationship was initiated or conducted online, the case involved the online sharing or distribution of child pornography, or the case involved child pornography stored on a computer or digital media. One hundred twenty six (126) cases involved a face-to-face relationship between the offender and the victim prior to any use of the Internet in committing abuse. N-JOV data indicated that the Internet was involved in eighteen percent (18%) of all sex crimes against minors and that nearly half of the eighteen percent (18%) were committed by acquaintances or family members, with a total of at least 460 arrests a year (Wolak 2005). This study found ninety-five percent (95%) were non-Hispanic Caucasians and forty-seven percent (47%) were twenty-six (26) or older. Thirty-five percent (35%) were married and over a third lived in small towns. Eighty percent (80%) were employed full time and fifty-one percent (51%) had incomes ranging from \$20,000-\$50,000 per year.

Identifying Internet Offenders

There is no one type of Internet child pornography user, and there is no easy way to recognize an offender. In the 2005 Wolak survey, solicitors did not match the stereotype of the older male "Internet predator". Many were identified as other youth and some were female (Wolak, 2006). Having a preconceived idea of a child sex offender can be unhelpful and prove a distraction for investigating police (Simon, 2000). Those convicted of sexually abusing children will not necessarily seek out or collect pornography, with one study putting the number of offenders who do so at around ten percent (10%) (Wortely, 2000).

This explosion of computer use, and the ease with which identities can be concealed on-line, has offered obvious opportunities to those who produce and consume pornography and those who seek to exploit vulnerable populations for sexual gratification (Alexy 2005). The Internet technology affords perpetrators a foundation for repeated, long-term victimization of a child. These crimes present law enforcement with many complex problems due to the fact that they transcend jurisdictional boundaries and often involve multiple victims in multiple states and countries.

N-JOV data reflected that the most common use of the Internet with family (70%) and acquaintance (65%) offenders was for seduction or grooming of victims either through online conversations or sharing of pornographic images. Forty-nine percent (49%) of family offenders and thirty-nine percent (39%) of acquaintance offenders produced pornographic images of their victims, which they stored or disseminated using the Internet. Forty-three percent (43%) used the Internet to arrange a face-to-face meeting. Relatively small numbers of offenders (2-4%) used the Internet as an inducement to enter the offender's home and use it to advertise or sell victims online. Seventy-five percent (75%) of these cases involved

some form of sexual contact and forty-five percent (45%) involved intercourse or other penetration. In a quarter of these cases, the sexual contact continued for over a year before being reported to the police.

How Sex Offenders Select Victims

A greater number of sex offenders are using the Internet searching for potential child victims through “kid only” or “kid friendly” chat rooms, online games, and instant messenger. The “set-up” for victimization requires long-term thought and planning. But a distinctive aspect of interaction in cyberspace that facilitates the grooming process is the rapid speed with which communication can become intimate (Wolak, 2005). Chat rooms can be frequented by sex offenders that groom and manipulate their victims by playing on the emotional immaturity of children in virtual anonymity. The goal of the “set-up” is to gain control over the victim. The length of time spent during the “set-up” varies upon the vulnerability of the child. The longer an offender knows a child the better they are at “zeroing” in their grooming tactics and strategies.

Grooming is a term used to describe the process of desensitizing and manipulating the victim(s) and/or others for the purpose of gaining an opportunity to commit a sexually deviant act [Title 22, Texas Administrative Code, Chapter 810.2(b)(15)]. Grooming inflicts psychological harm on the child. In teen chat rooms, the activities that precede the process of initiating direct contact with a child may simply involve the offender providing a description of themselves to all of the users of the public chat room so that the offender is masquerading as a particular kind of child, of a particular age, in the hope of attracting an equivalent age and the same or opposite sex child (i.e. 14/m/tx) (O’Connell, 2001). A sex offender may begin victim selection by observation in which an offender may “lurk” in chat rooms or massive multiplayer online games listening to conversations between children. An offender may search public profiles that include information such as name, age, location, hobbies, interests, and photographs. The offender will then wait for a child’s response and determine if they will initiate a conversation. After selecting a victim, the offender will introduce him or herself by instant message (IM) or by a private message to the child. Additionally, victim selection can involve viewing the child’s public profile. A victim’s information may be obtained through an Internet service provider request or a URL a child must provide in order to create their own website.

In the initial stages of grooming, the offender will suggest that the child move from a public domain to a private chat room or IM for an exclusive one-to-one conversation. The offender will engage in conversations related to school, home, hobbies, parental relationships, or interests of the child. The offender will gather information regarding the likelihood of activities being detected. The offender will manipulate the child to create an illusion of being the child’s best friend. The interactions take on the characteristics of a strong sense of mutuality (i.e. a mutual respect club comprised of two people that must ultimately remain a secret from all others) (O’Conner, 2003). During these interactions, the child is praised, made to feel special, and very positive conversations are tailored to the age of the child. Gifts or money may be offered to the child. Sadly, sex offenders tend to target children who are neglected or come from dysfunctional homes. For these children, the sex offender offers an alternative relationship that makes the child feel special and loved (Kim, 2004).

“Choose children who have been unloved. Try to be nice to them until they trust you very much and give them the impression that they will participate with you willingly. Use love as a bait. Give him or her the illusion that she is free to go with it or not. Tell him or her that they are special” (Salter, 2003).

The offender introduces the idea of trust, affection, and loyalty but it is based on deception and manipulation. This grooming tactic provides a forum to move into the next stage of victimization. The offender will begin to exploit social norms and test the child's boundaries. The offender could ask the child "have you been kissed?", "have you ever been skinny dipping?", or "do you wear a bikini?" If the child does not respond negatively to the boundary violation, it is tantamount to accepting the behavior or language. During boundary violations, the offender has positioned the child into believing that they share a deep sense of mutual trust.

Offenders who intend to maintain a relationship with a child will progress carefully and methodically into sexually explicit language. The nature of the conversations will progress from mild conversations (i.e. "I love you" or "I want to kiss you") to extremely explicit (i.e. masturbation or oral sex). The target child may be drawn into producing pornography by sending photos, using a web-cam or engaging in sexual discussions (ECPAT, 2005). To silence the child and ensure their continued compliance in sexual exploitation, the offender may use a variety of tactics including rewards, violence, threats, bribery, punishment, coercion, peer pressure, and fear (Klain, 2001). Research indicates that this pattern of conversations is characteristic of an online relationship that may progress to a request for a face-to-face meeting.

Child Pornography

Under federal law, child pornography (Wolak, 2003) is defined as a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, photograph, film, video, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where it

- depicts a minor engaging in sexually explicit conduct and is obscene, or
- depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, and such depiction lacks serious literary, artistic, political, or scientific value (18 U.S.C §1466A and 18 U.S.C. §2256)

Sexually explicit conduct includes various forms of sexual activity such as intercourse, bestiality, masturbation, sadistic or masochistic abuse, and lascivious exhibition of the genitals. It is illegal to possess, distribute, or manufacture these images.

Pornography and Child Pornography on the Internet

Both adult and child pornography has saturated the Internet due to the lack of censorship by the industry. The Internet provides the social, individual, and technological circumstances in which an interest in child pornography flourishes (Taylor, 2003). Cyberspace is host to more than one (1) million images of tens of thousands of children subjected to sexual abuse and exploitation (Howe, 2005). Of the estimated 24.7 million Internet users between the ages of ten (10) and seventeen (17), approximately 8.4 million youths received unwanted exposure to sexual material (Wolak, 2006).

It is estimated there are fourteen (14) million pornography sites (Costello, 2001) that house an estimated one (1) million pornographic images of children (Wellard, 2001) and two hundred (200) new images posted daily (Wortley, 2006). Of the thousands of images in the Interpol-managed database, only 320 children have ever been located (Taylor, 2003). It has been estimated that there are between 50,000 to 100,000 pedophiles involved in organized pornography rings around the world and that one-third of these

operate from the United States (Jenkins, 2001). The production and distribution of abuse images of children is estimated in the U.S. from a three (3) billion to a twenty (20) billion dollar business annually (ECPAT, 2005). Of this material fifty-five percent (55%) is reported generated from the United States and twenty-three percent (23%) from Russia (Council of Europe, 2005).

Child pornography is the second highest category, after indecent exposure, of sexual re-offense behavior (Bullens, 2005). The vast majority of children who appear in child pornography have not been abducted or physically forced to participate. In most cases the child knows the producer and it may even be their father who manipulates the child into taking part by more subtle means (Wortley, 2006). Most children feel a pressure to cooperate with the offender and not to disclose the offense, both out of loyalty to the offender and a sense of shame about their own behavior.

Physical contact between a child and a perpetrator does not need to occur for a child to become a victim or for a crime to be committed. Innocent pictures or images of children can be digitally transformed into pornographic material and distributed across the Internet without the victim's knowledge (U.S. Department of Justice, 2001). Digital graphic software (i.e. Photoshop, Illustrator, Microsoft PhotoEditor) allow offenders to edit "innocent" pictures. After a picture is scanned into a computer, these image-editing programs can be used to put several photos together or to distort pictures and create a believable image of a reality that never existed. This process is called "morphing". In some countries, morphed images or pictures are not illegal. Offenders may claim in court that a picture is morphed, no matter how disturbing, is not a picture of a real child or a situation which actually took place, and thus is not illegal.

In April 2002, the United States Supreme Court found that provisions of the Child Pornography Act (CPA), which prohibited the depiction of virtual and simulated child pornography, were invalid under the First Amendment of the U.S. Constitution. The Court found that in the absence of a "real" child, the Court could see no "direct link" between such images and the sexual abuse of children. The Court's majority could not see a substantial risk of producers of child pornography using virtual images of children. Additionally, children can be exposed to "virtual" pornography. Virtual pornography is legal the United States and in some other countries.

In the 2005 Wolak study, almost all of the arrested child pornography possessors (91%) used home computers to access child pornography and almost one (1) in five (5) arrested (18%) used a home computer in more than one (1) location to access child pornography. Additionally, Wolak found that in fourteen percent (14%) of child pornography investigations, the offenders not only had possessed pornography but had sexually victimized children and two percent (2%) possessed pornography and attempted to sexually victimize children. Eighty-four percent (84%) of the investigations involving child pornography did not detect concurrent child sexual victimization or attempts at victimization (Wolak, 2005). According to the United States Postal Inspection Service, forty percent (40%) of child pornographers investigated have sexually molested children. From January 1997 through March 2004, 1,807 child pornographers were arrested and 620 (34%) of these offenders were confirmed child molesters (Kim, 2004).

In the Seto study of 685 sex offenders referred between 1995 and 2004 for assessments of their sexual interests, two hundred ten (210) were child pornography offenders. Twenty-four percent (24%) had prior contact sexual offenses and fifteen percent (15%) had prior child pornography offenses. Child pornography offenders who had committed a prior or concurrent contact sexual offense were the most likely to offend again, either in general or sexually (Seto, 2006). Child pornographers showed greater

sexual arousal to children than to adults and differed from groups of sex offenders against children, and sexual offenders against adults (Seto, 2006).

Moe products (book, images, and games) are related to *anime* and *manga*. The meaning of *moe* refers to a fetishist sexual attraction that some players have to computer games. *Anime* and *manga* refers to a fetish sexual attraction for female characters, which may be depicted in pornographic and erotic contexts within games, animations, and illustrations. *Moe* web pages can link to other web pages containing images, stories, and conversations in which very young characters are the objects of sexual violence, abuse, and fantasy. Games further promote virtual interactions. It is estimated that *moe* products generated \$800 million dollars in 2003 (ECPAT, 2005). In the U.S., the number of online gamers has increased fifty-two percent (52%) to seventeen (17) million people since 2000. Almost ninety percent (90%) of adolescents use the Internet and eighty percent (80%) play games online (Lenhart, 2005).

Although most Internet pornography is created offline, technology has evolved to create “real” life pornography that can be viewed in real time, using web-cameras, phone cameras, digital cameras, and streaming video. A user can be notified of the date and time to log on the computer to view a child being sexually abused. The advent of mini-cameras has allowed for pictures and videos to be created without the subject’s knowledge. The user may pay money or exchange images with the direct abuser (Palmer, 2004).

These illegal images can be presented in various forms including print media, videotape, film, compact disc, read-only memory (CD-ROM), or digital versatile technology (DVD) (Klain, 2001) and can be transmitted through computer bulletin-board systems (BBS), USENET Newsgroups, Internet Relay Chat, web-based groups, peer-to-peer technology, and an array of constantly changing world wide web sites.

Using Child Pornography to Groom Children

Children can be exposed to pornography through spam or potential abusers. The accessibility of pornography online, the ease and perceived anonymity of transmission, and the environment of “virtuality” itself makes the use of pornography in online grooming easier for an abuser (ECPAT, 2005). Pornography is a tool for inducting and socializing a child into behaviors that reflect the content of the pornographic materials. Sex offenders frequently use pornography as a tool to assist them in the grooming process (Kim, 2004).

Children exploring the Internet for education and entertainment are at risk of encountering sexually explicit material, sexual exploitation, and offenses against children while remaining undetected by parents. Children are extremely vulnerable to victimization due to their curiosity, naiveté, and trusting nature. The Internet has become a conduit for sexually explicit material and offenses against children. In 2006, Wolak reported fifty-four percent (54%) of boys and forty-six percent (46%) of girls received unwanted exposure to sexual material. Ninety percent (90%) of all solicitations happened to teenagers (ages 13 to 17). Eighty-six percent (86%) received images of naked people and fifty-seven percent (57%) received pictures of people having sex and/or violent or deviant images. Lastly, eighty-three percent (83%) of unwanted exposures occurred when youth were surfing the web and eighty-nine percent (89%) of incidents the senders were unable to be identified (Wolak, 2006).

Sex offenders use pornography to escalate the relationship with the child. According to the Klain study, the most common purposes for which offenders use child pornography are:

- Pornography creates a permanent record for sexual arousal and gratification.

- Pornography lowers the child's inhibitions to engage in sexual behavior (Kelly, 1992).
- Pornography may be used to teach children how to behave, pose, or re-enact scenes.
- Pornography may be used to blackmail child victims by threatening to show the photographs, videos, or other depictions to parents, friends, or teachers. The threat becomes more potent because the child may fear punishment by the criminal justice system.
- Pornography created to sell for profit or trade between individuals. The Internet's anonymity, enhanced by increasingly sophisticated encryption technology, facilitates the increasing demand for child pornography.

Repeated exposure to adult and child pornography is deliberately used to diminish the child's inhibitions, break barriers to sexual arousal, desensitize the child that sex is normal, and arouse the victim. Children depicted in pictures are often smiling or have neutral expressions, a factor that appears to be designed to represent the children as willing participants in sexual or degrading acts (O'Connell, 2001). There is a recent trend for pictures to be taken in domestic settings such as a kitchen or bedroom, thus further "normalizing" the activity for children who view images (Queensland Crime Commission, 2000).

It has been reported that children under ten (10) who have been exposed to sexually exploitative material have themselves become users of it (Stanley et al, 2003). Eight percent (8%) of youths admitted to going voluntarily to X-rated sites (Wolak, 2000). Children at most risk of being violated through pornography productions are within the home and family (ECPAT, 2005). The child knows their abuser as a parent, a relative, a guardian, or an acquaintance. In these situations, the abuse may be more likely to come to light inadvertently as a result of inquiries by social welfare and reports from neighbors, rather than as a result of police inquiries into online crime (Wolak, 2005. in press).

Reporting Internet Crimes

The impact of online child victimization (i.e. solicitation and harassment) is not completely understood. Family dynamics often play a significant role in children's denial of a crime and their willingness to participate in the investigation and prosecution. A child's ability to acknowledge and accept the crime can be linked to family values, peer pressure, and feelings of guilt, shame, and embarrassment (U.S. Department of Justice, 2001). Only three percent (3%) of all incidents of predators harassing children on the Internet is reported (ProtectKids.org). The Crimes against Children Research Center found less than ten percent (10%) of sexual solicitations and only three percent (3%) of unwanted exposure episodes were reported to authorities such as a law-enforcement agency, an Internet service provider, or a hotline. In 2005, only one (1) incident out of more than 500 incidents of sexually explicit material was ever reported to an Internet service provider (Wolak, 2006).

NetSmartz reported that only seventeen percent (17%) of youth and approximately ten percent (10%) of parents could specifically name an authority, such as the Federal Bureau of Investigations, CyberTipline, or Internet service provider, to which they could make a report. NetSmartz found thirty-three percent (33%) reported that their parents or guardians knew "very little" or "nothing" about what the child did on the Internet. Twenty-two percent (22%) reported that their parents or guardians have ever discussed Internet safety with the child. Only twenty-five percent (25%) of youth who encountered a sexual approach or solicitation told a parent (Youth Internet Survey). Twenty-five percent (25%) of the youths reported receiving unwanted exposures to sexual material (Wolak, 2003).

In a 2001 study in Australia of 310 Internet-using households where there was at least one child under eighteen (18) years of age, forty-four percent (44%) of the children who had been exposed to undesired Internet content had reported this experience to a parent (ABA, 2001). These studies indicate that often children keep "cyber-friendships" a secret from their parents.

Wolak's study in 2005 indicated an increase in parental or guardian knowledge regarding where to report incidents of children being exposed to sexually explicit material from thirty-one percent (31%) in 2000 to thirty-five percent (35%). However, the proportion of youth who knew where to report being exposed to sexually explicit material declined from 2000 (24%) to 2005 (18%) respectively. Half of these youth (50%) who stated they knew where to report the incident could actually name a place to report unwanted Internet incidents.

General Recommendations

- 1. Focus on specifically designed awareness, educational, and reporting campaigns that address sexual exploitation in cyberspace.** Ninety percent (90%) of parents and guardians are extremely concerned about their children being exposed to sexually explicit material but yet only one (1) incident out of more than 500 incidents of sexually explicit material was ever reported to an Internet service provider (Wolak, 2006). Programs should be comprehensive and flexible to be updated with the evolving technology. Internet users need to be informed about the existence of resources to assist parents. Awareness programs need to focus on the diversity of threats children can experience both sexual and non-sexual.
- 2. Parents and professionals who come in contact with children at risk of exploitation should receive training to recognize sexual exploitation. Youth services programs or agencies should receive comprehensive training on online sexual exploitation and appropriate responses to suspected cases.** Teachers, counselors, and staff members in school settings should receive comprehensive training on online sexual exploitation and appropriate responses to suspected cases.
- 3. Texas law could be strengthened in the area of cyberstalking, as has been done in Florida.** Texas Penal Code 42.07 (Harassment) includes references to electronic communication including instant messaging, but Texas Penal Code, 42.072 (Stalking) does not specifically mention cyberstalking. Under 18 U.S.C. 875(c), it is a federal crime, punishable by up to five (5) years in prison and a fine of up to \$250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person or another. Although 18 U.S.C. 875 is an important statute, it is not an all purpose anti-cyberstalking statute. It only applies to actual threats and would not apply to a situation where a cyberstalker engaged in a pattern of conduct to harass or annoy another. Certain forms of cyberstalking may be prosecuted under 47 U.S.C. 223., in which the perpetrator does not reveal his or her name but only applies to direct communications between the perpetrator and the victim. Thus, this statute would not apply to a cyberstalker that harasses or terrorizes another by posting messages on a bulletin board or in a chat room. 18 U.S.C. 2425 makes it a federal crime to use any means of interstate or foreign commerce to knowingly communicate with a person with the intent to solicit or entice a child into unlawful sexual activity. While this statute provides important protections, it does not reach harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes. See Appendix A for the text of a Florida law that addresses cyberstalking and harassment.
- 4. Continue aggressively identifying, investigating, and prosecuting Internet solicitation and child pornography through undercover operations and using multi-jurisdictional and multi-disciplinary approaches.** In the June 2006 U.S. Supreme Court decision, the court upheld that parolees can routinely be searched by law enforcement as a condition of release (Samson v. California No.04-9728).
- 5. Enhance efforts to identify children exploited through pornographic images circulated online.**
- 6. Law enforcement should investigate child pornographers to determine if the offender has had contact victims.**
- 7. Protocols for computer searches in non-sex crimes should account for the possibility of child pornography.** Five percent (5%) of child pornographers came to the attention of law enforcement through investigations not involving sex crimes (Wolak, 2000).

8. **Probation and parole should regularly search offender's computers with management software solutions.** Nearly one (1) in four (4) sex offenders under supervision access pornography online despite treatment and supervision restrictions (Bullens, 2005). Supervision agencies cannot restrict offender's computer use or Internet access as a condition of probation or parole. In *U.S. v. Sofsky*, 287F.3d 122 (2nd Cir. 2002) decision, probation and parole can no longer restrict an offender from having a computer or access to the Internet for a legitimate purpose. In *U.S. v. Lifshitz* 369 F.3d 173 (2nd Cir. 2004), the scope and nature of active monitoring can no longer be indiscriminate and software monitoring can be justified by the special needs of the probation system. Lifshitz stated that an offender's computer can be conditioned on his submission to software monitoring of his computer as long as the scope of the search is limited to the least intrusive means and not overbroad (Bullens, 2005). If access to child pornography is indicated, then law enforcement would need to run a forensic-evidence based program to extract the images for the prosecution.

9. **Probation and parole officers should be trained on Internet crimes and management software.**

10. **Internet service providers (ISP) should be encouraged to enhance software for filtering and blocking illegal, violent, or abusive material.** Internet service providers, search engines, and web businesses should be encouraged to aim awareness and prevention messages about online solicitation and child pornography.

11. **Enhance Internet accountability regarding sexually explicit material.** ISPs should be legally responsible to report child pornography among various jurisdictions. In the U.S., ISPs are legally required to report known illegal activity on their sites, but they are not required to actively search for such sites (Stanley, 2001). Encourage ISPs to develop systems in which the public can view incidents of customers exposed to sexually explicit materials or online solicitation.

12. **ISPs and mobile phone networks should be encouraged to strengthen their procedures for user verification.** ISPs and mobile phone networks exercise little control over verifying the identities of people who use Internet accounts. This problem with anonymity is likely to increase as the access to the Internet via mobile phones increases (Wortley, 2006).

13. **Telecommunication sectors (public and private) should be encouraged to adopt child protection standards and mechanisms for self-regulation.** Coordination models between states must be seen to effectively reduce online solicitation and child pornography.

14. **Continue researching online solicitation, child pornography, and the developmental impact of unwanted exposure to pornography and online solicitation of child victims.**

Specific Recommendations

General Terms

- **Anime** is the Japanese version of animation.
- **Blam** is the spamming of weblogs.
- **Blog** is a slang term for a web log or an online diary (i.e. MySpace, Xanga, Yahoo, AOL, LiveJournals).
- **Cyberspace** is used to distinguish the physical world from the digital or computer-based world.
- **Cyberstalker** is the use of the Internet or other electronic means to stalk someone, which may be a computer crime or harassment. The term is used interchangeably with online harassment and online abuse. The anonymity of online interaction reduces the chance of identification and makes cyberstalking more common than physical stalking. Cyberstalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites (i.e. blogs and Indymedia), and email. Another contributing issue with cyberstalking is that it is simple to do a Google search for someone's alias, real name, or email address (Wikipedia 2006).
- **Encryption** is the scrambling of data into a secret code that can only be read by software set to decode the information.
- **Instant messengers (IM)** or chat programs are technologies that notify a user when a friend is online and allows them to communicate with each other in real time.
- **Manga** are Japanese comics.
- **Moe** refers to a fetishist sexual attraction that users of computer games, anime and manga have for female characters, who may be depicted in pornographic and erotic contexts within games, animations, and illustrations.
- **Morph** is to modify or create an image using computer software.
- **Person to person (P2P)** are file transfer programs for music and picture files on the computer (i.e. Kazaa, Napster, Bearshare, Limewire, and Morpheus).
- **Parental controls** are tools that allow adults to prevent their children from accessing certain Internet content.
- **Phishing** is a method used by fraudsters who send spam or pop-up advertisements to lure personal or financial information.
- **Spam** is the abuse of electronic messaging systems to send unsolicited, bulk messages. While the most widely recognized form of spam is e-mail spam, the term is also applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, and mobile phone messaging spam. E-spam is the most common form of spamming and involves sending identical or nearly identical unsolicited messages to a large number of recipients.
- **Spim** is spam received during instant messaging.

General Recommendations for Internet Safety

- Create and set clear rules for the child and enforce the rules.
- IMMEDIATELY CONTACT law enforcement if the child reports inappropriate language, inappropriate material, being solicited, threatened, stalked, or a person requests to meet the child in person.
- ENSURE that the child does not give out any personal information about themselves or the adult such as their name, home address, birthday, age, sex, phone number, sports team, favorite places to play, school name, school address, teacher's name, parent's name, telephone number, friend's screen name, email address, screen name, password, email address, or even feelings. Sex

offenders often target children who are vulnerable, lonely, sad, and have low self-esteem. Children crave attention and affection but lack caution and self-preservation skills. Protecting personal information is vital to protecting a child from becoming victimized. In 2000, eleven percent (11%) of youths posted their real name, telephone number, home address, or school name online. By 2005, thirty-four percent (34%) of youths posted personal information (Wolak, 2006).

- Ensure that the child does not post or send out any pictures of themselves or their family or friends on an online profile, blog, IM, email, chat room, or website.
- Assist the child in choosing appropriate screen names and email addresses that do not identify or reveal personal information. The following are considered inappropriate screen names: jacob9, soccerfan, littlesally, doglover, Xmanfan, and jamestx.
- If the child has given out personal information, it is extremely difficult to remove the information. Contact the Internet service provider or the site where the personal information was posted and ask the provider or site how the information can be deleted.
- If a child has given out their password to another person, go to the change password feature on the website. If the website does not have this feature, contact the Internet service provider or website directly to have the password changed.
- Keep the computer in a room that will allow the child to constantly be monitored. Position the screen so it is visible to an adult. Do not allow the child to have the computer in their bedroom.
- Ask questions regarding with whom the child is communicating, the files the child is downloading or sending, the content of the blog, and the games the child plays and with whom the child is playing. Nearly three (3) out of ten (10) parents do not know or are not sure if their teen talks to strangers online (NCMEC, 2005).
- Educate the child on the threats and dangers of the Internet. Talk frankly with the child about inappropriate language, inappropriate material, and invasion of privacy. Adults should be specific about the rules if the child is allowed to access chat rooms. A 2006 survey by the National Center for Missing and Exploited Children revealed that when parents and guardians talk to their children about Internet safety, the child's exposure to potential threats decline and the child makes safer online decisions.
- A child can easily be exposed to adult pornography and thus it is extremely important to provide open lines of communication between the adult and child. One of the main reasons that children do not report the inappropriate content they find online is fear of punishment from the parents (NetSmartz, 2006).
- Educate the child to report inappropriate language, inappropriate material, or if someone wants to meet the child in person. Educate the child to never respond to inappropriate language or suggestive emails or IM.
- Monitor the games the child is playing and with whom the child is playing the game.
- Ensure that the child does not share files, open attachments, or click on links from strangers. Teach the child never to accept gifts from someone online unless the adult has given permission. Control the information flow the child sends and receives.
- Ensure that the child does not access *moe* web sites.
- Always scan emails, files, attachments, and IM for viruses prior to downloading the item.
- Encourage the child to delete any emails or IMs from anyone they do not know.
- Internet accounts should be in the adult's name with the adult having the primary screen name and controlling passwords. Change passwords so the child cannot log on without the parent. Children should not complete a profile for a service provider.
- Install retail spyware that will log keystrokes and identify what the child is watching and update the software regularly.

- Install parental control programs and update the software regularly (i.e. Guardian Monitor, Tattletale, eBlaster, CYBERSitter, CyberParol, and/or NetNanny). These programs will monitor the child's activity.
- Update computer software. Most IM vendors regularly provide software updates as an added security feature.
- Install updated pop-up blockers and anti-spam programs and update them regularly. Filters are not a guarantee that a child will not be exposed to inappropriate material nor are filters a substitute for supervision of a child while on the Internet.
- Learn how to spot a bogus phishing message and what to do if the child has responded to a phishing email with the child's or the adult's personal information.
- Supervise email accounts and use services such as KidMail, Kid Safe Mail, and Safe2Read. These services are an essential portion of email protection.
- To avoid a child providing personal information online, utilize the feature (i.e. ID Block, Privacy Control, or Privacy Protection) found in full-function firewalls (i.e. Panda Platinum Internet Security, Norton Personal Firewall, Keiro Personal Firewall, and ZoneAlarm Pro). The feature allows the user to enter personal information and then the information is stored and encrypted. If the firewall detects any of the information being sent out the transmission is then blocked.
- Restrict Internet access and remove the Internet cable when an adult cannot supervise the child.

Chat Programs or Instant Messaging (IM) Recommendations

- Ensure that the child does not reveal ANY personal information over IM.
- Make sure that the child(s) IM screen name is not giving out personal information (i.e. avoid screen names that include your child's real name, birthday, or age).
- Some IM programs allow the creation of personal profiles. Common profile items include a real name, city, state, age, and gender. It is not necessary to create these profiles if the child only uses IM with established offline friends.
- Avoid clicking into links or files in IM. IM receives spam messages also known as spim. Spim often have the same characteristics of e-mail spam. A spim message may say "Hey check out my new site" followed by a link. A child may open spam or spim without knowing that they should be skeptical and can be dangerous. Spam or spim invariably is linked to pornography and pornographic websites serving deceptive spyware downloads. These messages may directly link to malicious files.
- Ensure that the child does not try to win or buy anything on the Internet without the parent's permission.
- Avoid allowing the child to download or exchange "person to person" files for music or pictures. Despite copyright law, P2P programs utilize an "open port" giving the computer access to other users which can be dangerous if not monitored by a proper firewall.
- Restrict children to only IM with friends in a "buddy" list. The most common used messaging programs provide features that can block messages from everyone but those on the buddy list.
 - AOL Instant Messenger (AIM). Click on My AIM > > Edit Options > > Edit Preferences. Select Privacy Tab. Under "Who can contact me," and select "Allow only users on my Buddy List."
 - Yahoo Messenger. Click on Messenger > > Preferences. Under Category, select "Ignore List". Then select "Ignore anyone who is not on my Messenger List". Then click OK. Make sure that only friends are in the child's list of contacts.

- MSN Messenger. Click on Tools > > Options. Select Privacy from the menu. Under “Allow and block lists”, mark the checkbox labeled “Only people on my Allow List can see my status and send me messages”. Then click OK. Make sure that your child’s friends are included on the contact list.

Online Language

Ninety-five percent (95%) of parents could not identify common chat room lingo that teenagers use to warn people they are chatting with that their parents were watching (NCMEC, 2005). Ninety-two percent (92%) of parents did not know the meaning of A/S/L (Age/Sex/Location) (NCMEC, 2005). Parents should watch for the following questionable abbreviations:

- 53x means “sex”
- 121 means “one to one”
- A/S/L means age, sex, location. Watch for personal information being exchanged (i.e. 14/m/tx). This is a 14 year old male from Texas.
- CYBER used as a verb and means “cybersex”
- CONNECT means “to talk privately”
- DIKU means “do I know you”
- ESAD means “eat sh*t and die”
- F2F, FTF means “face to face” or “let’s meet F2F”
- FOAD means “f*ck off and die”
- GP means “go private”
- H4U means “hot for you”
- H&K means “hugs and kisses”
- ILU means “I love you”
- IWALU means “I will always love you”
- KOC means “kiss on the cheek”
- KOL means “kiss on the lips”
- LTR means “long term relationship”
- LMIRL means “lets meet in real life”
- LUWAMH means “love you with all my heart”
- LU means “love you”
- MOSS means “member of the same sex”
- MOTOS means “member of the opposite sex”
- MUSM means “miss you so much”
- NIFOC means “naked in front of the computer”
- OLL means “online love”
- P2P means “person to person”
- P911 means “my parents are coming”
- PA means “parent alert”
- PAL means “parents are listening”
- PANB means “parents are near by”
- PM means “private message or one on one chat”
- POS means “parent over shoulder”
- pr0n is an alternate spelling for porn or pornography

- PDA means “public display of affection”
- RL, IRL means “in real life as in “wants to see you IRL”
- SWAK means “sealed with a kiss”
- TOY means “thinking of you”
- WIBNI means “wouldn’t it be nice if”
- WTGP means “want to go private”
- WUF means “where are you from”
- WTF means “what the f*ck”

Acronyms and words used in daily IM or discussion boards

- AFAIK means “as far as I know”
- BTW means “by the way”
- CUL means “see you later”
- HHOK means “ha ha only kidding”
- IANAL means “I am not a lawyer”
- IIRC means “if I remember correctly”
- IMHO means “in my humble opinion”
- KEWL means “cool”
- OMG means “oh my god”
- OTOH means “on the other hand”
- WUT^2 “what up with you too”

See Appendix C for additional online chat abbreviations provided by the National Center for Missing and Exploited Children.

Finding a Child’s Online Blog (from Kim Komando)

- MySpace. Go to www.myspace.com and click on the search tab. Enter the child’s name in “Find Someone You Know”. Then click “find”. If the child’s name does not appear, return to “Find Someone You Know”. Click on “Select search by option” and then select “Email”. Enter the email address and click find. This is a free search.
- LiveJournal. Requires the user to set up an account and the user may search the site by Google. If the user establishes a “free” account, go to <http://www.livejournal.com> and click “Search > > Advanced”. Select your county, state, and city. Do not select anything under Journal Update Time. Enter your child’s age into both boxes. Leave the Interest and Under has Friend blank. Then click search.
- Xanga (<http://www.xanga.com>). Requires only paid members to search the site.
- Facebook (www.facebook.com) is only available to students and is an email address ending in “.edu”.
- Google. This site can search other sites by entering “site:myspace.com” or “site:xanga.com”. Instructions can be found at http://www.google.com/advanced_search?hl=en

Preventing Access to Blogs

If user has Internet Explorer, the user can block any blog sites. To block a site, open Internet Explorer and click on Tools > > Internet Options. Click the Content icon and then Enable. Click the General icon and

then click Create Password. Click OK. In Content Advisor click Approved Site icon. The user then will type in the sites the user wants to block. In “Allow this Web site”, the user will type the entire address of sites to block. The user then will click the Never bar. Then click OK on the next window.

Internet Game Recommendations

Online games potentially provide a new platform where children and young people will be exposed to solicitations and potentially harmful interactions with other people online (ECPAT, 2005).

- Most personal computers have a “multiplayer” function. Xbox and Playstation have online capabilities for multiplayer using voice chat similar to a telephone party line. Massive Multiplayer Online Roleplaying Games (MMORPG) is an online community and propagates interpersonal connections in settings that can become very intimate and personal information can be exchanged similar to IM.
- Only allow the child to play games with “real” friends the child knows.
- Remind the child never to give out any personal information even character names when playing.
- Remind the child never to move from the game into a private online location.
- Xbox 360 is equipped with parental controls and can be accessed at Xbox Web site.

Music Downloading

- Ensure that the child is downloading music from a legitimate source. Duplicating copyrighted materials without authorization can lead to prosecution and financial penalties.
- Titles 17 and 18 of the U.S. Code protects copyright owners from the unauthorized reproduction, adaptation, or distribution of sound recordings, as well as certain digital performances to the public. The penalties depend upon whether the infringing activity is for commercial advantage or private financial gain. Under U.S. copyright, “financial gain” includes bartering or trading anything of value, including sound recording. The online infringement of copyrighted music can be punished by up to three(3) years in prison and \$250,000 in fines. Repeat offenders can be imprisoned up to six (6) years (Recording Industry Association of America 2003).
- The recording industry has two copyrighted works:
 - The copyright in the musical composition (i.e. the actual lyrics and notes on the paper.) This is owned by the songwriter or music publisher.
 - The copyright in the sound recording (i.e. the recording of the performer singing or playing the given song.) This is owned by the recording studio or company.

Finding and Reporting Child Pornography or Online Solicitation

If the computer is on, leave it on. If the computer was turned off, leave the computer off. Do not show the material to anyone and IMMEDIATELY call 911.

What To Do If You Are Being Cyberstalked (U.S. Department of Justice, 2006)

If you are receiving unwanted contact, make clear to that person that you would like him or her not to contact you again.

Save all communications for evidence. Do not edit or alter them in any way. Also, keep a record of your contacts with Internet system administrators or law enforcement officials.

You may want to consider blocking or filtering messages from the harasser. Many e-mail programs such as Eudora and Microsoft Outlook have a filter feature, and software can be easily obtained that will automatically delete e-mails from a particular e-mail address or that contain offensive words. Chat room contact can be blocked as well. Although formats differ, a common chat room command to block someone would be to type: /ignore <person's screen name> (without the brackets). However, in some circumstances (such as threats of violence), it may be more appropriate to save the information and contact law enforcement authorities.

If harassment continues after you have asked the person to stop, contact the harasser's Internet Service Provider (ISP). Most ISP's have clear policies prohibiting the use of their services to abuse another person. Often, an ISP can try to stop the conduct by direct contact with the stalker or by closing their account. If you receive abusive e-mails, identify the domain (after the "@" sign) and contact that ISP. Most ISP's have an e-mail address such as abuse@(domain name) or postmaster@(domain name) that can be used for complaints. If the ISP has a website, visit it for information on how to file a complaint.

Contact your local police department and inform them of the situation in as much detail as possible. In appropriate cases, they may refer the matter to state or federal authorities. If you are afraid of taking action, there are resources available to help you. Contact the National Domestic Violence Hotline, 800-799-SAFE (phone), 800-787-3224 (TDD), or a local women's shelter for advice and support.

Characteristics of Youth Who Form Close Online Relationships (NCMEC, 2005)

- Sixteen percent (16%) of girls and twelve (12%) of boys have close online relationships.
- Girls aged fourteen (14) to seventeen (17) were twice as likely as girls ten (10) to thirteen (13) to form close online relationships.
- High parent-child conflict and being highly troubled were associated with close online relationships. Girls with high levels of parent-child conflict report yelling, nagging, and privileges by parents at higher levels than other girls. The highly troubled girls had levels of depression, victimization, and troubling life events at higher levels than other girls.
- Boys who had low communications with their parents, and who also reported that their parents were less likely to know where and who they were with were the most strongly associated with close online relationships.
- Girls and boys who reported high levels of Internet use and home Internet access were more likely to report close online relationships.
- Youths with problems were most likely to attend a face-to-face meeting with people they first met online.

Warning Signs that a Child may be at Risk

- Excessive use of online services especially during the late night hours
- Unsupervised time in unmonitored chat rooms
- Mood swings and withdraws
- Greater desire to spend time with people online than with "real life" people
- Unexplained files downloaded (i.e. .jpd, .gif, .bmp, .tif, .pcx, .mov, .avi, .wmv, or .mpg)

- The child minimizes or closes the screen if someone approaches
- Receives unexplained gifts, money, and computer equipment (i.e. webcam, digital camera, mini camera, etc.).

National Resource Websites

Child Exploitation and Obscenity Section (Section of the Department of Justice)

www.usdoj.gov/criminal/ceos/childporn.html

Crimes Against Children Research Center

www.unh.edu/ccrc/index.html

CyberAngels

<http://www.cyberangels.org/>

Cyberstalking Laws

<http://www.ncsl.org/programs/lis/cip/stalk99.htm>

ECPAT International (End Child Prostitution, Child Pornography, and Trafficking of Children for Sexual Purposes)

<http://www.ecpat.net>

Federal Trade Commission Internet Privacy Section for Kids

<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/kidz.htm>

FBI Investigations into child exploitation via the Internet

www.fbi.gov/hq/cid/cac/innocent.htm

FBI Internet Safety Tips for Kids

<http://www.fbi.gov/kids/crimepre/internet/internet.htm>

Internet Crimes Against Children (Office of the Juvenile Justice and Delinquency Prevention)

<http://www.ojjdp.ncjrs.org/programs/index.html>

Internet Fraud Complaint Center

<http://www.ic3.gov>

Internet Watch Foundation

<http://www.iwf.org.uk>

Missing: An educational Kit about Internet Kidnapping

<http://livewwwires.com/>

National Center for Missing and Exploited Children Cyber Tipline

- To report child pornography, enticement of a child, child prostitution, and unsolicited obscene material sent to a child
www.cybertipline.com

- To misleading domain names or report concerns about obscenity not accessed by children
www.obscenitycrimes.org.

National Cyber Security Alliance
<http://www.staysafeonline.info/>

NetSmartz Kids
<http://www.netsmartz.org/>

Parents Safety-Net Test
www.incredibleinternet.com

ProtectKids.org
<http://www.protectkids.org/>

Snope-Informs about Internet hoax-debunking sites
www.snope.com

Staysafe
<http://www.staysafe.org>

Safe Kids Program
<http://www.safekids.com/>

Safe Online Outreach Society
<http://www.safeonlineoutreach.com/>

Take Charge
www.cox.com/TakeCharge

Texas Office of the Attorney General
<http://www.oag.state.tx.us/internet/inbhome.shtml>

U.S. Government
<http://onguardonline.gov/index.html>
FTC: <http://www.ftc.gov/infosecurity/>

U.S. Postal Inspection Service, U.S. Customs Service, FBI, and NCMEC
For an online for to report suspected child suspected sexual exploitation
www.missingkids.com/cybertip

Yahoo's Safety Site
<http://yahooligans.yahoo.com/parents/>

Fun and Safe Sites for Children

Disney's Internet Safety for Kids

http://disney.go.com/legal/internet_safety.html

Fact Monster

<http://www.factmonster.com/>

Kidsites

<http://www.kidsites.com/>

SafeKids

<http://www.safekids.com/>

SafeTeens

<http://www.safeteens.com/>

Sesame Street

<http://sesameworkshop.org/>

Web Wise Kids

www.webwisekids.com

Internet Blocking, Filtering, and Usage Tracking Software

BESS

www.bess.net

Children's Internet Browser

<http://www.chibrow.com>

Cyber Patrol

www.cyberpatrol.com

Cyber Sentinel from Security Software Systems

www.securitysoft.com

Cyber Snoop

www.pearlsw.com

CyberSitter

www.cybersitter.com

KidDesk

www.edmark.com/prod/kdis

N2H2

www.n2h2.com

Net Nanny

www.netnanny.com

Net Shepherd

www.netshepherd.com

Recreational Software Advisory Council

www.icrg.org

Safe Surf

www.safesurf.com

Surf Money

www.surfmonkey.com/default.asp

Surf Watch

www.surfwatch.com

The Internet Filter

www.turnercom.com/if/index.html

X-Stop

www.xstop.com

References

- Alexy, E.; Burgess, A.; & Baker, T.; (2005) *Internet Offenders: Traders, Travelers, and Combination Trader-Travelers*. Journal of Interpersonal Violence 804-812 (July 2005)
- Bullens, M., (2005) Computer and Internet Monitoring: Key Factors in Developing an Implementation Strategy for Probation and Parole. Sexual Assault Report, Page 72-74 May/June.
- Cooper, S., Estes, R., Giardino, A., Kellogg, N., & Vieth, V., (2005). *Medical Analysis of Child Pornography*. Medical and Legal Aspects of Child Sexual Exploitation. Saint Louis: GW Medical Publishing. P. 223
- Council of Europe. (2005, in press) Organised Crime Situation Report 2005. Provisional Report. Strasbourg: Directorate General of Legal Affairs, Council of Europe
- Costello, T., (2001). *Gambling's Great Web of Lies*, The Age, 3. April, page 15
- Cox Cable Take Charge Retrieved 2006 from http://www.cox.com/TakeCharge/parents_internet.asp
- Dobson, A. (2003). *Caught in the Net*. Care and Health, February, 13 pp.6-9
- ECPAT International, (2002). *Protecting Children Online: A ECPAT Guide*. Retrieved 2006 from <http://www.ecpat.net>
- ECPAT International, (2005). *Violence Against Children in Cyberspace*. Retrieved 2006 from <http://www.ecpat.net>
- Federal Bureau of Investigations press release, retrieved from <http://www.fbi.gov/pressrel/pressrel102/cm031802.htm> on 2006 Perrien, Hernandez, Gallop, & Steinour, 2000
- Howe, A. (2005) Proceedings of the Standing Senate Committee on Legal and Constitutional Affairs. Issue 17. Evidence for June 23, 2005. Ottawa Canada. Retrieved from http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/lega-e/17evb-e.htm?Language=E&Parl+38&Ses=1&comm_id=11
- Jenkins, P. (2001) *Beyond Tolerance: Child Pornography on the Internet*. New York: New York University Press.
- Keef, B., (2006) *Hackers Targeting Internet Chatters*: Austin American Statesman, Friday, June 9, 2006
- Ketchum Global Research Network. Parents' *Internet Monitoring Study*. National Center for Missing & Exploited Children and Cox Communications, 2005

Kim, C.; (2004) *From Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children*. Child Sexual Exploitation Update. Volume 1, Number 3, American Prosecutors Research Institute. Retrieved 2006 from http://www.ndaa-pri.org/publications/newsletters/child_sexual_exploitation_update_volume_1_number_3_2004.html

Klain, E., Davies, H., & Hicks, M., (2001) *Child Pornography: The Criminal Justice System Response*. American Bar Association Center on Children and the Law for the National Center for Missing & Exploited Children, March

Komando, Kim; Retrieved 2006 from <http://www.komando.com/>

Kornblum, Janet. (2006) “*Teens Hang Out at MySpace.*” USA Today. January 8, 2006, http://www.usatoday.com/tec/news/2006-01-08-myspace-teens_x.htm?csp=34

Lenhart, A., Madden, M. & Hitlin, P., (2005). *Teens and Technology: Youth Are Leading The Transition To A Fully Wired and Mobile Nation*. Washington: Pew Internet & American Life Project.

McCathy, J.:(2002) *Possession of Child Pronography Food for Fantasy, Fuel for Molestation, or Deviant Curiosity?* Sex Offender Law Report Volume 6, Number 3 April/May 2005

More Online, Doing More. Washington, DC: The Pew Internet & American Life Project, 2001, page 2

Reuters, New York (2006) *MySpace Bolsters Defenses, Faces Sex Predator Suit*, Updated June 20, 2006 8:20 PM ET.

O’Connell, R., (2003). *A Typology of Cyberexploitation and On-line Grooming Practices*: University of Lancashire, Cyberspace Research Unit, <http://fkbko.net>

O’Connel, R., (2001). *Paedophiles Networking on the Internet*. In C.A.Arnaldo (ed.), *Child Abuse on the Internet: Ending the Silence*, Berghahn Books and UNESCO, Paris pages 65-79

Palmer, T., & Stacey, L., (2004). *Just One Click: Sexual Abuse of Children and Young People through the Internet and Mobile Phone Technology*. UK: Barnardos, page 28. February.

ProtectKids.org. Retrieved 2006 from <http://www.protectkids.org/>

Queensland Crime Commission and Queensland Police Service (2000). *Child Sexual Abuse in Queensland: The Nature and Extent: Volume 1*. Project Axis

Recording Industry Association of America 2003. Retrieved 2006 from <http://www.riaa.com/issues/piracy/penalties.asp>

Salter, Anna, (2003) *Predators 66* (Basic Books 2003)

Seto, M., & Eke, A., (2005) *The Criminal Histories and Later Offending of Child Pornography Offenders: Sexual Abuse: A Journal of Research and Treatment*, Volume 17, No. 2, April

Seto, M., Cantor, J., & Blanchard, R., (2006). *Child Pornography Offenses Are a Valid Diagnostic Indicator of Pedophilia*: Journal of Abnormal Psychology. 115(3), Aug 2006, 610-615

Simon, L., (2000). *An Examination of the Assumption of Specialization, Mental Disorder, and Dangerousness in Sex Offenders*. Behavioral Science and the Law. 18:276-308.

Stanley, J., & Kovacs, K., (2003) *Child Abuse and the Internet*. Ninth Australasian Conference on Child Abuse and Neglect. Sydney: 25 November 2003

Stanley, J., (2001) *Child Abuse and the Internet*. National Child Protection Clearinghouse, No. 15 Summer. Melbourne: Australian Institute of Family Studies.

StaySafe.org Retrieved 2006 from <http://www.staysafe.org/>

Stopping Child Pornography: Protecting our Children and the Constitution: Before the Senate Committee on Judiciary, 107th Congress (2002) statement of Ernie Allen, Director, The National Center for Missing and Exploited Children

Taylor, M. & Quayle, E. (2003) *Child Pornography-An Internet Crime*. Hove and New Yor: Brunner-Routledge.

U.S. Department of Justice, Office of Justice Programs, Office for Victims of Crime, *Internet Crimes Against Children*. OVC Bulletin, December 2001

U.S. Department of Justice (2006) *Cyberstalking: What is Cyberstalking?* Retrived 2006 <http://www.cyberguards.com/CyberStalking.html>

Wellard, S. (2001). *Cause and Effect*. Community Care, 15-21, March, pages 26-27

Wikipedia. Retrieved 2006 from <http://en.wikipedia.org>

Wolak, J.; Mitchell, K.; & Finkelhor, D.; (2000). *Online Victimization: A Report on the Nations Youth*. Crimes Against Children Research Center, National Center for Missing and Exploited Children. June

Wolak, J.; Mitchell, K.; & Finkelhor, D.; (2003) *Internet Sex Crimes Against Minors: The Response of Law Enforcement*. Alexandria, Virginia: National Center for Missing and Exploited Children, November page vii

Wolak, J. (2005). ECPAT International Roundtable Meeting on Violence Against Children in Virtual Settings. Presentation. Bangkok, Thailand, June 12-13

Wolak, J.; Mitchell, K.; & Finkelhor, D.; (2005) *Child-Pornography Possessors Arrested in Internet-Related Crimes*. U.S. National Center for Missing and Exploited Children.

Wolak, J.; Mitchell, K.; & Finkelhor, D.; (2005) *Internet and Family and Acquaintance Sexual Abuse: Child Maltreatment* 49-60 February

Wolak, J., Finkelhor, D., & Mitchell, K., (2005, in press) *The Varieties of Child Pornography Production*. U.S. Crimes Against Children Research Center, University of New Hampshire. page 23.

Wolak, J.; Mitchell, K.; & Finkelhor, D.; (2006) *Online Victimization of Youth: Five Years Later*. National Center for Missing and Exploited Children

Wortley, R. & Smallbone, S., (2006) *Child Pornography on the Internet*. Office of Community Oriented Policing Services and U.S. Department of Justice. May 2006. Retrieved 2006 from <http://www.cops.usdoj.gov/mime/open.pdf?Item=1729>

Wortley, R. & Smallbone, S., (2000). *Child Sexual Abuse in Queensland: Offender Characteristics and Modus Operandi*. Brisbane: Queensland Crime Commission.

18 U.S.C. §1466A and 18 U.S.C. §2256

APPENDIX A

Florida Statutes

Title XLVI. Crimes.

Sec. 784.048 Stalking; definitions; penalties.

(1) As used in this section, the term:

(a) "Harass" means to engage in a course of conduct directed at a specific person that causes substantial emotional distress in such person and serves no legitimate purpose.

(b) "Course of conduct" means a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose. Constitutionally protected activity is not included within the meaning of "course of conduct." Such constitutionally protected activity includes picketing or other organized protests.

(c) "Credible threat" means a threat made with the intent to cause the person who is the target of the threat to reasonably fear for his or her safety. The threat must be against the life of, or a threat to cause bodily injury to, a person.

(d) "Cyberstalk" means to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose.

(2) Any person who willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person commits the offense of stalking, a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(3) Any person who willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person, and makes a credible threat with the intent to place that person in reasonable fear of death or bodily injury of the person, or the person's child, sibling, spouse, parent, or dependent, commits the offense of aggravated stalking, a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(4) Any person who, after an injunction for protection against repeat violence, sexual violence, or dating violence pursuant to s. 784.046, or an injunction for protection against domestic violence pursuant to s. 741.30, or after any other court-imposed prohibition of conduct toward the subject person or that person's property, knowingly, willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person commits the offense of aggravated stalking, a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(5) Any person who willfully, maliciously, and repeatedly follows, harasses, or cyberstalks a minor under 16 years of age commits the offense of aggravated stalking, a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(6) Any law enforcement officer may arrest, without a warrant, any person he or she has probable cause to believe has violated the provisions of this section.

(7) Any person who, after having been sentenced for a violation of s. 794.011 or s. 800.04, and prohibited from contacting the victim of the offense under s. 921.244, willfully, maliciously, and repeatedly follows, harasses, or cyberstalks the victim commits the offense of aggravated stalking, a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(8) The punishment imposed under this section shall run consecutive to any former sentence imposed for a conviction for any offense under s. 794.011 or s. 800.04.

History.--s. 1, ch. 92-208; s. 29, ch. 94-134; s. 29, ch. 94-135; s. 2, ch. 97-27; s. 23, ch. 2002-55; s. 1, ch. 2003-23; s. 3, ch. 2004-17; s. 3, ch. 2004-256.

APPENDIX B

Recent Court Cases Regarding Internet Restriction and Probation

New York v. Fisher (1982). Child pornography was not protected by the First Amendment. Child pornography separated from obscenity laws, to be judged on a different standard.

Osborne v. Ohio (1990). Private possession of child pornography ruled to be illegal.

United States v. Sofsky 287 F.3d 122 (2nd Cir. 2002) Probation and parole can no longer restrict an offender from having a computer or access to the Internet for legitimate purposes

Ashcroft v. Free Speech Coalition (2002). Virtual images ruled not to be pornography and “appeared to be a minor” ruled to be too broad.

United States v. Freeman No. 01-3475F.3d (3rd Cir. 2003) A special condition forbidding him from possessing any computer in his home or using any online computer services without written approval of the probation officer is overly broad and it involves a greater deprivation of liberty than is reasonably necessary to deter future criminal conduct.

United States v. Scott (7th District January 2003) Special conditions overturned

United States v. Zinn (11th Cir. February 2003) Special conditions upheld and ruling on the polygraph

United States v. Lifshitz 369 F.3d 173 (2nd Cir. 2004) The Fourth Amendment normally offers protection against searches of home computers, the “search” of a cybercrime probationer’s computer by monitoring software can be justified by the “special needs” of the probation system, so that a offender’s probation can be conditioned on his submission to the software monitoring as long as the scope of the search is limited to the least intrusive means and not overbroad if that is avoidable.

APPENDIX C (attached)

Online Lingo

Provided by National Center For Missing and Exploited Children (.pdf file)