ONLINE SEXUAL EXPLOITATION OF CHILDREN

The International Association of Computer Investigative Specialists
Robert J. O'Leary
Robert D'Ovidio

Overview of Issues of Online Sexual Exploitation of Children in the United States

The effects of computers on society have, unfortunately, not been entirely positive. Computers and related networking technologies have created new opportunities for crime, including crime involving the sexual exploitation of children. The connection between the Internet and the sexual exploitation of children has caught the attention of the mass media.[1] Newspaper headlines such as *Chat Site Showed Live Molestation*[2] and *Wonderland Paedophiles are Sentenced*[3] tell stories of live child molestations streamed in real-time through a chat room and a global network of predators with a child pornography library containing 750,000 explicit images.

Online victimization studies speak to the widespread concern parents have for the safety of their children, who increasingly rely on the Internet for education, entertainment, and socialization. According to the National Center for Missing and Exploited Children, approximately 1 in 7 Internet users between the ages of 10 and 17 fall victim to unwanted online sexual solicitation.[4] Of particular concern for parents and government officials is that the solicitations and ensuing adult/child relationships originating in cyberspace can lead to a physical-world relationship where the child is sexually abused. The online sexual exploitation of children is also made apparent by official crime statistics[5] and the creation of specialized investigative units within law enforcement agencies to fight this type of criminal activity.[6]

Despite the attention being paid to the online exploitation of children, the magnitude of the problem is still unknown. Victimization research is likely hampered by the unwillingness of children to report online encounters of a sexual nature for fear of embarrassment and parental scrutiny of future Internet activity. Official crime statistics likely under represent the magnitude of the problem due to the lack of a centralized system to record related complaints within and across law enforcement agencies. A lack of awareness among parents and children on where to report unwanted online sexual encounters also highlights the problem of using official crime statistics to gauge the extent of the problem. Data from a 2005 survey by the National Center for Missing and Exploited Children on Internet crimes against children show that 65% of parents and 82% of children were not aware of where they could report an unwanted online sexual encounter.[7]

The following document is divided into five sections. The first section describes the types of online activities encompassing the sexual exploitation of children. The second section offers background characteristics of victims and perpetrators. The third section highlights challenges faced by law enforcement officials and government policymakers in dealing with the online sexual exploitation of children. The fourth section recommends research to assist law enforcement, parents, and educators in responding to and preventing the online sexual exploitation of children. Lastly, the fifth section identifies existing resources that can be used to assist with investigations into the online sexual exploitation of children, train law enforcement professionals on related investigative and forensic methodologies, and increase awareness of the problem among children, parents and teachers.

Types of Online Sexual Exploitation of Children

The online sexual solicitation of children involves sexually-oriented interactions over the Internet; the production, collection, and distribution of child pornography; unwanted exposure of children to pornography; and child-sex tourism and prostitution. Each type of online exploitation directly or indirectly results in sexual contact between adults and children, and should, therefore, receive equal focus of law enforcement and preventive efforts.

Online Enticement of Children for Sexually-Oriented Interactions

The enticement of children over the Internet for sexually-oriented interactions occurs through various methods of contact, including chat rooms, instant messengers, and email. The types of solicitations can be differentiated by the degree to which the encounter involves sexually explicit discourse and actions. Predators often begin the courtship with an online encounter involving no or a subtle mention of sex. The goal of this initial encounter is to gain the trust of the targeted victim and usually involves the predator seeming to take interest in the victim's likes and dislikes. Encounters then escalate to include discussions of an overt sexual nature and will sometimes involve the predator sending pornography to the victim. Often, the predator will ask the victim to forward a picture of him or herself. The encounters can escalate further in cyberspace to include voice and video chat.

Once the predator feels the victim's trust has been earned, the relationship is likely to spill over into the physical world. Physical world encounters include gifts and letters sent through postal mail and telephone calls, and can even escalate to an in-person meeting between the predator and victim. Data from the National Center for Missing and Exploited Children 2005 survey of online child victimization show that 23% of youth who received an unwanted sexual solicitation were asked by the predator to meet in-person.[8] The obvious danger of an in-person meeting is direct sexual contact between predator and victim.

Alarmingly, unwanted online sexual solicitations are rarely reported to a law enforcement agency. Data from the National Center for Missing and Exploited Children 2005 survey of online child victimization show that only 5% of the solicitations were reported to a law enforcement agency or Internet service provider.[9] Also troubling is the likelihood of the victim not disclosing the incident to anyone. Fifty-six percent of victims did not tell anyone, including friends and parents, of the solicitation they received online.

Child pornography

Child pornography involves any depiction, including computer-generated representations, "of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child, the dominant characteristic of which is depiction for a sexual purpose."[10] Computer related technologies, including the Internet, have simplified the creation, distribution, and collection of child pornography. Home computers, digital cameras, and point-and-click graphics software have simplified the production of child pornography as compared to earlier times when production involved expensive cameras, complicated editing equipment, and a chemical laboratory to develop photographs. Distributors of child pornography can use the Internet to advertise their illicit wares to a much wider audience when compared to the limited reach of word-of-mouth advertisement or postings in the back of on-topic magazines. Collectors can download child pornography from the safety of their own homes faster and with an increased perception of anonymity than in the past when they relied on face-to-face exchanges and the postal mail to obtain images and movies.

The Internet offers many venues through which people can interact to exchange child pornography. Usenet groups, email, chat rooms, instant messengers, and websites have, for example, all been used to distribute child pornography. Child pornographers are also quick to adopt new online services and computer technologies. The same peer-to-peer networks that are being used by teens and young adults to exchange copyrighted music and movies are also being used by child pornographers to exchange their illicit images and videos.[11] Social networking sites, such as Orkut, allow child pornographers to build a community network with like-minded others to promote their wares and give them ready access to children who frequent such sites.[12] Cell phones with Internet accessibility have also been used to download and store child pornography, thus expanding the scope of technologies used by child pornographers beyond traditional computing devices and giving child pornographers the benefits that mobility affords.[13]

Unwanted Exposure of Children to Pornographic Material

Children are also victimized in cyberspace through exposure to pornographic material. The widespread availability of pornography on the Internet makes purposeful exposure an easy feat irregardless of a user's age. Children are, however, being exposed to pornography without proactively searching for it. The National Center for Missing and Exploited Children found, for example, that 34% of youth Internet users were exposed to pornography while on the Internet without purposely seeking out the material.[14]

Unwanted exposure to pornography by youth can occur through a number of ways. Innocuous Internet searches for musicians or actors who are popular among youth often return results of pages containing pornography picturing celebrity look-alikes. Youth may also be exposed to pornography through spam, or unsolicited commercial email, used to advertise pornographic material. Additionally, unwanted pornography may be directed at youth through email or instant messenger programs by peers or by sexual predators trolling for potential victims.

Misleading domain names have also exposed children to pornography. Website owners have, in the past, profited from the tendency of youth to misspell the domain name addresses of popular child-oriented programs. John Zuccarini, for example, was sentenced under the *Truth in Domain Names Act*[15] to a 30-month prison term for using deceptive websites addresses to purposely direct minors to pornographic material.[16] Among the misleading sites used by Zuccarini was

www.bobthebiulder.com, a domain name address based upon a common misspelling of the children's cartoon *Bob the Builder*.[17] Instead of seeing content based upon the construction-themed cartoon, children visiting the website were exposed to hard-core images of young people engaging in sexual intercourse.

Child Sex Tourism and Prostitution

The Internet further contributes to the sexual exploitation of children in that it is used to promote child prostitution in the United States and abroad. The global reach of the Internet combined with the low cost and ease of maintaining and updating a website makes the world-wide-web an extremely useful tool to advertise products and services, including sex-for-hire services. Escort agencies and pimps have been quick to catch on to the benefits of marketing over the web. Prostitution websites that offer a virtual "line-up" of available prostitutes, provide contact information, and list services and associated fees are appearing with evermore frequency and are created by those promoting sex with adults and minors. Sites promoting prostitution with minors have included teenage runaways[18] and children as young as 12.[19]

Travel agents specializing in sex-tours have also taken to the web to advertise their services. Sex-tour operators tend to focus on countries where the age of majority for sex is younger than the age in the United States and where government enforcement efforts against adult-child sexual encounters are lax. In addition to airfare arrangements and hotel accommodations, these travel agents provide access to the local brothels, sex clubs, and escort agencies and are generally knowledgeable about the sex-trade industry in the destination country. The Internet further supports the child-sex tourism industry by providing patrons of these tours a means by which to easily connect with like-minded others throughout the world.[20] Usenet groups, online bulletin boards, and chat rooms, for example, offer sex-tourism patrons the venue to share travel experiences, exploits, and cautionary advice to those wishing to travel aboard for the purpose of having sex with minors. The use of the Internet by those interested in underage sex has been cited by the United Nations as a factor leading to an increase in number of destination countries for child-sex tourism.[21]

Online Child Sexual Exploitation: Victim and Offender Characteristics

Computers and the Internet have not only changed the nature of child sexual exploitation, but have affected the types of people who fall victim to and commit such crimes. The global reach of the Internet facilitates new social relationships by easily connecting people who are geographically distant. The facelessness of cyberspace minimizes relationship barriers posed by traditional social categories (e.g. age, class, and race). People are, consequently, able to establish relationships that were previously unlikely and that do not involve physical-world interaction. With the Internet, the pool of suitable targets for victimization by child sexual predators is, thus, no longer limited to family members, the children of friends, and youth within one's community. Predators who use the Internet can easily point-and-click their way across the globe, making all children who spend time online a potential target for victimization.

The facelessness of cyberspace further affects behavior by increasing the perception of anonymity. The increased perception of anonymity experienced by those communicating via computer is likely to reduce inhibitions towards previously restrained behavior. As such, predilections towards sexually exploiting children might be more pronounced in computer-mediated environments. At the same time, safeguards employed in the physical world to prevent

victimization might be disregarded online. Youth who would shun a stranger in the physical world might not be so hesitant to befriend the same stranger in cyberspace. Thus, we can expect sexual solicitations to occur more frequently among strangers in cyberspace than in more traditional settings. Research examining sexual solicitations in cyberspace shows that predators and their victims are very likely to be strangers and to have had no previous in-person contact. An overwhelming majority of youth (86%) who were sexually solicited via the Internet indicated that they had first met the predator online.[22]

Victims Examined

Questions remain as to whether the stereotypical profile describing victims of child sexual exploitation pre-Internet fits the profile of victims exploited online. Children who are timid and reclusive and who suffer from low self-esteem are less likely than children who are adventurous and outgoing to take advantage of the social benefits of Internet connectivity to meet new people. Efforts to socialize and meet new people in cyberspace are likely to place children at risk of sexual exploitation by online predators.

Important to preventing the online sexual exploitation of children is recognizing the environments from which it is occurring. Online victimization is occurring in environments which are traditionally thought of as safe places and with trusted adults under the same roof. Victimization is taking place while youth are connected to the Internet at home, in the home of a friend, at school, and in the public library. Despite the presence of guardians (i.e. parents, teachers, and librarians) in these environments, children are still falling victim to online sexual exploitation at alarming rates. Complicating matters further is the increased familiarity with new Internet technologies and services among youth when compared to the familiarity with such technologies and services among adults. Consequently, guardians are unlikely to discover the potential dangers posed by new Internet services until after their children have adopted them.

Further complicating efforts by guardians to keep children safe online is the widespread use of cell phones among youth. Data gathered by the Pew Internet & American Life Project in October 2004 on the adoption of technologies by youth show that 45% of teens in the United States have a cell phone.[23] Increasingly, these cell phones are being used to send and receive instant text messages, access the world-wide-web and email, and participate in chat rooms. The mobility and connectivity afforded to cell phone users place few limits as to where children can be reached by predators.

Data gathered through official crime statistics and victimization surveys give a look at the types of children who are falling victim to online sexual exploitation. Females, as compared to males, are much more likely to receive unwanted solicitations for sex while connected to the Internet.[24] Conversely, males were more likely than females to be exposed to pornography on the Internet.[25] Data from the National Center for Missing and Exploited Children show a positive correlation between age and the receipt of unwanted solicitations for sex. A comparison of victimization rates among Internet users between the ages of 10 and 17 shows victimization to be highest among 16 year-olds (24%), followed by 15 year-olds (23%) and 17 year-olds (19%).[26]

An examination of child pornography seized in the course of an arrest provides some insight into the types of children who are falling victim during its production and the preferences of predators.[27] Understanding these preferences helps us gauge future victimization involving the sexual abuse of minors for the purpose of satisfying the child pornography market. Images

containing children between the ages of 6 to 12 were the most popular among those whose arrest charges included the possession of child pornography. Specifically, 83% of offenders possessed child pornography with victims from this age category. Seventy-five percent of offenders possessed child pornography depicting victims between the ages of 13 to 17. Younger children were also to the liking of those arrested for possessing child pornography. Thirty-nine percent of offenders possessed child pornography depicting victims between the ages of 3 to 5 and 19% of offenders possessed child pornography with victims less than 3 years of age.

Predators Examined

Predators who sexually exploit children can be differentiated based upon whether their criminal activity involves direct sexual contact with children. *Traders* and *closet collectors* both use the Internet to access and download child pornography, but do not get involved in its production and do not directly abuse children.[28] *Traders* will seek out and communicate with like-minded others online to exchange child pornography images and movies in hopes of building their collection. Conversely, c*loset collectors* conceal their penchant for child pornography and do not actively engage link-minded others to exchange materials. Instead, *closet collectors* accumulate child pornography by purchasing it through online commercial channels.

Unlike *traders* and *closet collectors, isolated collectors, cottage collectors,* and *commercial collectors* do engage in direct sexual contact with children.[29] *Isolated collectors* abuse children and in the process create child pornographic images and movies for their own personal use. These materials are generally not distributed for fear of attracting attention from the law enforcement community. As with *isolated collectors, cottage collectors* do sexually abuse children and do record the abuse to create child pornography. *Cottage collectors* are, on the other hand, not shy about distributing the child pornography they produce. They will share the illicit materials with other predators for free through online channels as part of an exchange network that allows them to continue building their child pornography collection. C*ommercial collectors*, conversely, distribute child pornography with the goal of making a profit. They too will sexually abuse children and record the abuse to make child pornography. They will, however, charge other predators who want to access and download the material.

As indicated, the increased perception of anonymity experienced when communicating via the Internet is likely to reduced previous restraints to offending for those with predilections towards sexual involvement with children. The Internet also creates new opportunities to explore sexual curiosities and gives rise to the *situational offender*.[30] *Situational offenders,* in terms of child pornography, see the ease at which they can access child pornography over the Internet and the ability to view it while hidden behind a computer screen as the reason for experimenting with the material.

Data from victimization surveys, official crime statistics, and media reports of police investigations provide a look at the types of people who use computers and the Internet to exploit children. Consistent among the various sources of available data are the sex and race of the predator. Males were more likely than females to sexually exploit children in cyberspace. In examining media reports of online child sexual exploitation cases occurring from 1996 to 2002, Alexy, Burgess, and Baker found that in 95.1% of the cases the offenders were male.[31] With respect to race, predators were overwhelmingly white. Wolak, Mitchell, and Finkelhor found, for example, that 92% of those arrested for Internet sex crimes against minors were white.[32]

Predators in both online sexual solicitation and child pornography cases were not always adults. At times youth fell victim to exploitation by other youth. In a survey by the National Center for Missing and Exploited Children on online exploitation, victims of sexual solicitation indicated that in 43% of cases their solicitor was less than 18 years of age.[33] These results should, however, be taken with some suspect since the solicitor's age was gauged by the victim and not validated at the time of arrest. Official crime statistics show a much larger proportion of adult offenders. For example, Wolak, Mitchell, and Finkelhor found that 97% of offenders arrested for Internet sex crimes against children were at least 18 years of age.[34]

Challenges Faced by Law Enforcement Officials and Government Policymakers in Addressing the Online Sexual Exploitation of Children

Independent Efforts to Prevent Online Exploitation of Children

Several programs, projects, and efforts have been undertaken to protect children from online exploitation. Much of this work has met with success and has ultimately raised the awareness of law enforcement, policy makers, parents, and children of the techniques used by Internet predators. While these efforts compliment each other, they generally operate independently and, at times, overlap. A strategic action plan that incorporates the coordination of these independent efforts would advance the efforts underway as well as future efforts to protect children from online exploitation. The establishment of a comprehensive, nationwide plan to prevent the online exploitation of children is imperative. The true scope of this issue must be identified in order to develop an effective strategic action plan to address online exploitation of children. The scope can only be accurately assessed if it is based on reliable statistics. The lack of clear statistics on child exploitation is a due in large part to the absence of standard protocols for law enforcement to capture detailed relevant information about online exploitation. The absence of standard protocols is a significant impediment to establishing a comprehensive nationwide plan to prevent online exploitation of children. The available statistical information stems from surveys, which while providing valuable insight, do not provide the empirical information necessary to fully understand the true scope of this problem.

Assessment of Law Enforcement Training in Online Exploitation of Children

Law enforcement officers and prosecuting attorneys face the challenge of accessing quality and continued training to provide the necessary general knowledge of electronic crime and digital evidence, as well as the knowledge specific to the online exploitation of children. Understanding the circumstances of the crimes as well as the technology that facilitated the criminal activity is paramount to the success of law enforcement in preventing and investigating these crimes. It is equally important to raise the level of expertise and capabilities of prosecuting attorneys in order to ensure that investigation efforts are successful.

Several training courses in online exploitation of children investigations are available to law enforcement personnel from a variety of sources. However, training course selections, order, and practical skills development remain largely unstructured. There is no clear information as to the order in which the available training should be attended. Information is also lacking on the courses which may overlap or present similar material. Further, there is no clear data collection process to identify the number of law enforcement personnel who have successfully completed training in investigating and preventing online exploitation of children or the quality of that

training. An accurate assessment of law enforcement's capacity and capability to investigate and prevent youth from sexual exploitation by Internet predators is necessary to realistically determine the current level of preparedness and assess the anticipated rate of improvement.

Jurisdiction and Honor of out State Court Orders by Internet Service Providers

In the age of the Internet, we can longer think of criminal investigations as local occurrences. Official crime data from the New York City Police Department show a highly significant difference in inter-jurisdictional offending for crimes committed using a computer as compared to similar crimes committed in the physical world. Approximately 39% of the computer crimes, compared to only 6.3% of similar crimes committed in the physical world, involved an offender or victim outside New York State.[35] Law enforcement agencies often meet obstacles when conducting investigations that rely on electronic records held by service providers and on computers outside their jurisdiction. These obstacles can result in investigative delays when court orders are deemed to lack the necessary and appropriate authority to compel the compliance of the custodian of the records. Often such delays cause lapses in the investigative timeline and prevent law enforcement from acting on the information in a timely manner. The resolution to this obstacle is the implementation of full faith and credit in court orders issued on behalf of law enforcement agencies seeking electronic records and data in furtherance of child exploitation investigations and prosecutions from custodians of records in other jurisdictions.

Assessment of Online Exploitation of Youth Training Material for Youth

A variety of efforts are underway to protect youth from Internet predators. In addition to training law enforcement personnel in proactive investigations to stop Internet predators, online safety programs for youth have been developed. ISafe, NetSmartz, WiredKids, and CyberAngels have online safety curriculum for youth. These programs provide information to keep children safe online. The impact of these programs and their effect on youth have not been assessed.

Research and Policy Recommendations Related to the Online Sexual Solicitation of Children

A plan to adequately assess the magnitude of online child exploitation is essential to mounting prevention and response strategies that are both effective and efficient. Gauging the magnitude of problem requires agreement at the national level on the crimes that constitute online exploitation. A uniform system to record these crimes should then be devised and implemented within law enforcement agencies across all levels of government. A centralized reporting structure should then be set up to enable aggregate assessments at the state and federal levels. Additionally, victimization data should be collected regularly through surveys to account for any bias in official crime statistics arising from underreporting to law enforcement.

A program that addresses all efforts to protect children from online exploitation and coordinates the work of all agencies and organizations working in this field is strongly recommended. There is currently no entity that coordinates or addresses all aspects of the online exploitation of children on a national level. This effort would not supplant work currently being done by the various groups involved. Instead, it would coordinate and facilitate the current efforts in order to leverage the otherwise independent work of many and create a comprehensive and effective force working toward common goals and objectives.

The government should continue to sponsor research into understanding security techniques used by online predators to elude law enforcement and hide their identities while traversing

cyberspace. We should look to better understand how knowledge of criminal methodologies and security techniques is transferred within the predator community, recognizing that crime requires offenders to learn and possess the requisite skills and tools associated with a specific type of act. Research on decryption, steganography detection, and information extraction methods should continue. Additional areas to explore concerning security and anonymizing techniques used in the online exploitation of children include:

- Remote storage and its use by child pornographers.
- The use and benefits of distributed peer-to-peer networks to trade child pornography.
- The reliance on remailers and proxies to mediate predator-child exchanges.
- The adoption of wireless technologies to mask location and identity when interacting with minors.

Government officials should make funding available to support the development of training curriculum related to online child exploitation investigations and to regularly training law enforcement officers who investigate these types of cases. An investigator's knowledge needs to keep pace with the evolving methodologies and tools used by online predators. Investigators also need to be familiar with the new Internet technologies children adopt and the latest online services children use to socialize since these are the venues through which predators will entice and solicit. Likewise, continued attention needs to be paid to providing investigators and law enforcement first-responders with training to enable them to identify and seize electronic evidence at a crime scene.

Attention should also be paid to the needs of community corrections agencies (e.g. probation and parole). These agencies increasingly have to serve non-institutionalized offenders who are under government supervision for online child sexual exploitation. Officers in these agencies need training on the monitoring solutions to manage predators' computer and Internet usage. This type of training should go beyond the technical aspects of installing and using monitoring software. Probation and parole officers need to be well-versed on the methodologies and online services that predators are using to lure children in cyberspace. Legal training pertaining to electronic monitoring and wiretaps is also recommended for those officers who monitor the computer and Internet usage of offenders. Existing monitoring programs within probation and parole agencies should be evaluated in terms of their deterrent and enforcement value. These evaluations should be taken into account when refine existing programs and expanding monitoring into new jurisdictions.

Resources

Resources are available to assist law enforcement agencies and government officials with investigations, forensic examinations, training, and awareness/preventative initiatives concerning the online sexual exploitation of children.

Investigative Assistance

The following task forces and professional associations provide assistance to law enforcement agencies with investigations, forensic examinations, and operational policies related to the online exploitation of children:

- *International Association of Computer Investigative Specialists (IACIS)*: IACIS is a volunteer, not-for-profit organization dedicated to education and training for law enforcement in the field of forensic computer science. Its 800 members come from law enforcement agencies at all levels of government and from numerous countries, including the United States. IACIS members can be called upon to provide consultation for electronic crime investigations and forensics.[36]
- *High Technology Crime Investigation Association (HTCIA)*: HTCIA is a professional association that brings together law enforcement officers, security officials, and researchers who are interested in cybercrime, e-commerce fraud, online safety, and computer forensics. It has 39 chapters, 29 of which are located in the United States. HTCIA members can be called upon to provide consultation for electronic crime investigations and forensics.[37]
- *United States Secret Service Electronic Crimes Task Force (ECTF)*: The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA Patriot Act) mandated that the U.S. Secret Service establish a nationwide network of Electronic Crimes Task Forces to prevent, detect, and investigate crimes involving our nation's critical infrastructure, including the Internet. Currently, there are 24 ECTFs located in major metropolitan areas throughout the United States. Each ECTF brings with it the resources of the U.S. Secret Service and will assist federal, state, and local law enforcement agencies with the seizure of electronic evidence and subsequent investigations and forensic examinations.[38]
- *Federal Bureau of Investigation Regional Computer Forensics Laboratory (RCFL)*: The RCFL is a full-service digital forensic laboratory created to support criminal investigations, including investigations involving the online exploitation of children. Currently, there are 12 RCFLs located in the United States. Each RCFL is staff by FBI personnel and personnel from regional law enforcement partners. Law enforcement agencies without the internal capacity to conduct the necessary forensic examinations can call upon the RCFL in their region for assistance.[39]
- *Internet Crimes Against Children Task Force (ICAC)*: The ICAC task force program is designed to assist local and state law enforcement agencies with investigations involving the use of computer technology to sexually exploit children. The program is funded by the United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention. Currently there are 48 ICAC task forces spread throughout the country.[40]

Training Assistance

Investigations involving the online exploitation of children require law enforcement officers with a background in the seizure of electronic evidence and digital forensic methodologies. Additionally, knowledge of the substantive and procedural laws pertaining to computer crime and related investigative techniques is also essential to preparing a workforce to fight the online sexual exploitation of children.

The following organizations offer training on seizing, obtaining, and processing electronic evidence. Courses offered by these organizations are applicable to investigations involving many types of computer-related crimes, not just crimes involving the online sexual exploitation of children.

- *International Association of Computer Investigative Specialists (IACIS)*: IACIS training is limited to active law enforcement professionals. Its students and members represent law enforcement agencies from all levels of government and from many nations.[41]
- *SEARCH: The National Consortium for Justice Information and Statistics (SEARCH)*: SEARCH is a non-profit organization supported by U.S. justice agencies, and federal, state, and local government contracts. SEARCH training is only available to law enforcement professionals.[42]
- *National White Collar Crime Center (NW3C)*: NW3C is a congressionally-funded non-profit organization that provides a nationwide system to support government agencies with the prevention, investigation, and prosecution of economic and high-tech crimes. Professionals from law enforcement, corrections, probation, and parole agencies can attend NW3C courses.[43]

The following organizations offer technical and legal training pertaining specifically to the investigation and prosecution of online sexual crimes against children.

- *National Center for Missing and Exploited Children (NCMEC)*: Pursuant to its congressional mandate[44], NCMEC serves as a national clearinghouse for information about missing and exploited children. Its mandate includes better preparing law enforcement and social service professionals to carry out investigative and preventative duties concerning the online sexual exploitation of children.[45]
- *Internet Crimes Against Children Training and Technical Assistance Program (ICAC)*: Criminal justice professionals from law enforcement, probation, parole, and prosecutorial agencies can attend ICAC training. Participation in ICAC training must be coordinated through local ICAC task force.[46]
- *National District Attorney's Association (NDAA)*: In keeping with its mission to improve the administration of justice in the United States, the NDAA offers workforce training to prosecutors and investigators on a variety of topics, including the online sexual exploitation of children. Its offerings related to online sexual exploitation tend to focus on procedural practices of the investigation process.[47]

Awareness/Preventative Initiatives

A number of programs are available to increase awareness among children, parents, and educators on the dangers posed to children who use the Internet and to promote online safety. It should be noted that the programs listed below have yet to undergo scientific evaluations to demonstrate they are effective at increasing online safety for children. It is strongly recommended that Internet safety programs go through an evaluation to safeguard against delivering programs with unintended negative effects on the safety of our children. The following Internet safety programs have garnered widespread attention in the law enforcement community and among educators:

- *NetSmartz Workshop*: NetSmartz offers self-paced awareness programs on Internet safety and cyber bullying for children and parents delivered via its website. NetSmartz also provides teachers and law enforcement professionals with an Internet safety curriculum that can be delivered in-person to child and parent audiences.[48]

- *High Technology Crime Investigation Association Internet Safety for Children Campaign*: HTCIA has partnered with Hewett Packard, the United States Secret Service, LiveWWWires, and NCMEC on a program to train law enforcement professionals to deliver Internet safety courses to parents and children.[49]
- *CyberAngels*: CyberAngels is Internet safety program offered by the Guardian Angels. It has online safety courses that cater to children, parents, educators, and librarians.[50]
- *I-Safe*: I-Safe provides educators, law enforcement professionals, and parents with training materials to promote a safe and responsible Internet experience for children. I-Safe also provides children with web-based resources on Internet safety, including a chat room for children to interact with I-Safe staff about online safety issues.[51]
- *WiredSafety*: WiredSafety offers online training courses related to Internet safety, including courses on the online sexual exploitation of children, cyber bullying, and online harassment. WiredSafety also keeps an online library of resources to keep parents and educators up to date on the latest dangers posed to children who use the Internet.[52]

End Notes

[1] Hansen, C. (2005, Nov. 10). Catching Potential Internet Sex Predators. *MSNBC* [On-Line], Available: http://www.msnbc.msn.com/id/9927253/ and U.S. Arrests Dozens over Internet Child Porn Distribution. (2004, May 14). *CNN* [On-Line], Available: http://www.cnn.com/2004/LAW/05/14/child.porn.arrests/index.html.
[2] Koch, W. (2006, Mar. 15). Chat Site Showed Live Molestation. *USA Today* [On-Line], Available: http://www.usatoday.com/news/nation/2006-03-15-child-ring_x.htm.
[3] McAuliffe, W. (2001, Feb. 13). Wonderland Paedophiles are Sentenced. *ZD NetUK* [On-Line], Available: http://news.zdnet.co.uk/business/legal/0,39020651,2084402,00.htm.
[4] Wolak, J, Mitchell, K, and Finkelhor, D. (2006). *Online Victimization of Youth: Five Years Later*. Washington, DC: National Center for Missing & Exploited Children.
[5] D'Ovidio, R and Doyle, J. (2003). Cyberstalking: Understanding the Investigative Hurdles. *FBI Law Enforcement Bulletin*, 72(3):10-17 and Wolak, J, Mitchell, K, and Finkelhor, D. (2003). *Internet Crimes Against Minors: The Response of Law Enforcement*. Washington, DC: National Center for Missing & Exploited Children.
[6] http://www.icactraining.org/TF_Contacts.htm.
[7] Wolak, J, Mitchell, K, and Finkelhor, D. (2006)
[8] Wolak, J, Mitchell, K, and Finkelhor, D. (2006).
[9] Wolak, J, Mitchell, K, and Finkelhor, D. (2006).
[10] Office of the United Nations High Commissioner for Human Rights. (Jan. 18, 2002). Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. *United Nations Secretariat* [On-line], Available: http://www.ohchr.org/english/law/crc-sale.htm
[11] The United States Customs Cyber Smuggling Center found that child pornography was easily accessible through the peer-to-peer network KaZaA. For details on the analysis see: United States General Accounting Office. (2003). *File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography* (GAO Publication No. 03-351). Washington, DC: United States General Accounting Office.

[12] Brazilian Prosecutors Seek to Sue Google (2006, Sept. 1), *MSNBC* [On-Line], Available: http://msnbc.msn.com/id/14622759/
[13] Owner Of Child Porn Cell Phone Gets 8 Years (2006, July 26), *NewsNet5* [On-Line], Available: http://www.newsnet5.com/news/9579424/detail.html
[14] Wolak, J, Mitchell, K, and Finkelhor, D. (2006).
[15] 18 USC § 2252B
[16] Man Sentenced for Registering Misleading Web Site Names. (2004, Feb. 27). *USA Today* [On-Line], Available: http://www.usatoday.com/tech/news/2004-02-27-zuccarini-gets-jailtime_x.htm.
[17] The official site for the *Bob the Builder* cartoon is www.bobthebuilder.com.
[18] Brunker, M. (1999, June 2). Streetwalkers in Cyberspace. *MSNBC* [On-Line], Available: http://msnbc.msn.com/id/3078778/ and McKim, Jennifer. (2006, July 12). Pimp Pleads Guilty to Prostituting Minor. *Orange County Register* [On-Line], Available: http://www.ocregister.com/ocregister/news/atoz/article_1209170.php.
[19] Alonzo-Dunsmoor, M. (2006, Mar. 11). Phoenix Officials to Crack Down on Child Prostitution. *The Arizona Republic* [On-Line], Available: http://www.azcentral.com/arizonarepublic/local/articles/0311prostitution0311.html
[20] Hall, M. (2003, Sept. 13). The Darker Side of Travel. *The UK Telegraph* [On-Line], Available: http://www.telegraph.co.uk/travel/main.jhtml?xml=/travel/2003/09/13/etsextr.xml&sSheet=/travel/2003/09/16/ixtrvhome.html
[21] Asia's Child Sex Victims Ignored. (2000, Sept. 15). *BBC* [On-Line], Available: http://news.bbc.co.uk/1/hi/world/asia-pacific/926853.stm.
[22] Wolak, J, Mitchell, K, and Finkelhor, D. (2006).
[23] Lenhart, A, Madden, M, and Hitlin, Paul. (2005). *Teens and Technology*. Washington, DC: Pew Internet & American Life Project.
[24] Wolak, J, Mitchell, K, and Finkelhor, D. (2006); Mitchell, K, Wolak, J, and Finkelhor, D. (2005). Police Posing as Juveniles Online to Catch Sex Offenders: Is it Working?. *Sexual Abuse: A Journal of Research and Treatment*, 17(3): 241-267.
[25] Wolak, J, Mitchell, K, and Finkelhor, D. (2006).
[26] Wolak, J, Mitchell, K, and Finkelhor, D. (2006).
[27] Wolak, J, Mitchell, K, and Finkelhor, D. (2003).
[28] Klain, E, Davies, H, and Hicks, M. (2001). *Child Pornography: The Criminal Justice System Response*. Washington, DC: National Center for Missing and Exploited Children.
[29] Klain, E, Davies, H, and Hicks, M. (2001).
[30] Klain, E, Davies, H, and Hicks, M. (2001).
[31] Alexy, E, Burgess, A, and Baker, T. (2005). Internet Offenders: Traders, Travelers, and Combination Trader-Travelers. *Journal of Interpersonal Violence*, 20(7): 804-812. Cases include instances where a computer was used to trade or collect child pornography and instances where predators solicited a minor online and then arranged an in-person meeting for the purposes of sexual contact.
[32] Wolak, J, Mitchell, K, and Finkelhor, D. (2003).
[33] Wolak, J, Mitchell, K, and Finkelhor, D. (2006).
[34] Wolak, J, Mitchell, K, and Finkelhor, D. (2003).
[35] D'Ovidio, R. (2003). *Policing the Net: The Effect of Jurisdiction*. Presented at the Academy of Criminal Justice Sciences Annual Meeting, Boston, MA.

[36] http://www.iacis.info
[37] http://www.htcia.org
[38] http://www.ectf.usss.gov/ectf/home/index_html
[39] http://www.rcfl.gov/
[40] http://www.icactraining.org/default.htm
[41] http://www.iacis.info/iacisv2/pages/training.php
[42] http://www.search.org/programs/hightech/courses.asp
[43] http://www.nw3c.org/ocr/courses_desc.cfm
[44] 42 U.S.C. § 5771
[45]http://www.ncmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=989
[46] http://www.icactraining.org/Training.htm
[47] http://www.ndaa-apri.org/education/ndaa/child_abuse_training_schedule.html
[48] http://www.netsmartz.org/
[49] http://www.htcia.org/isfc/
[50] http://www.cyberangels.org/
[51] http://www.isafe.org/
[52] http://www.wiredsafety.org/