Center for Problem-Oriented Policing

Child Pornography on the Internet

Guide No.41 (2006)

by Richard Wortley and Stephen Smallbone

The Problem of Internet Child Pornography

The guide begins by describing the problem and reviewing factors that increase the risks of Internet child pornography. It then identifies a series of questions that might assist you in analyzing your local Internet child pornography problem. Finally, it reviews responses to the problem and what is known about these from evaluative research and police practice.

The treatment of children as sexual objects has existed through the ages, and so too has the production of erotic literature and drawings involving children. However, pornography in the modern sense began with the invention of the camera in the early nineteenth century. Almost immediately, sexualized images involving children were produced, traded, and collected.[1]Even so, child pornography remained a restricted activity through most of the twentieth century. Images were usually locally produced, of poor quality, expensive, and difficult to obtain. The relaxation of censorship standards in the 1960s led to an increase in the availability of child pornography, and, by 1977, some 250 child pornography magazines were circulating in the United States, many imported from Europe.[2]Despite concern about the extent of child pornography, law enforcement agencies had considerable success in stemming the trafficking of these traditional hard-copy forms. However, the advent of the Internet in the 1980s dramatically changed the scale and nature of the child pornography problem, and has required new approaches to investigation and control.

Internet child pornography is unlike most crimes local police departments handle. Local citizens may access child pornography images that were produced and/or stored in another city or on another continent. Alternatively, they may produce or distribute images that are downloaded by people thousands of miles away. An investigation that begins in one police district will almost certainly cross jurisdictional boundaries. Therefore, most of the major investigations of Internet child pornography have involved cooperation among jurisdictions, often at an international level.

However, within this broader scheme, local police departments have a crucial role to play. By concentrating on components of the problem that occur within their local jurisdictions, they may uncover evidence that initiates a wider investigation. Alternatively, they may receive information from other jurisdictions about offenders in their districts. Because of the increasing use of computers in society, most police departments are likely to encounter Internet child pornography crimes. Therefore, it is important that all police departments develop strategies for dealing with the problem. Larger departments or districts may have their own dedicated Internet child pornography teams, but most smaller ones do not, and the responsibility for day-to-day investigations will fall to general-duties officers.[3]It would be a mistake to underestimate the importance of local police in detecting and preventing Internet child pornography offenses. One study found that 56 percent of arrests for Internet child pornography crimes originated from non-specialized law enforcement agencies.[4]

Related Problems

Internet child pornography is only one of a number of problems related to either child abuse or the Internet. Other related problems not directly addressed by this guide include:

Child Abuse

- violence and fatalities
- neglect
- abandonment
- exposure to hazardous materials (e.g., clandestine drug labs)
- trafficking of children and babies and illegal adoption agencies
- juvenile runaways.

Internet Crime

- online solicitation of children for sexual activity
- identity theft (sometimes known as phishing)§
- hacking.

> § See the POP Guide on Identity Theft.

Defining Child Pornography

Legal Definitions

The idea of protecting children from sexual exploitation is relatively modern. As late as the 1880s in the United States, the age of consent for girls was just 10 years.[5] In 1977, only two states had legislation specifically outlawing the use of children in obscene material. The first federal law concerning child pornography was passed in 1978, and the first laws that specifically referred to computers and child pornography were passed in 1988. Since that time, there has been a steady tightening of child pornography laws[6] (see Table 1).

Table 1: Development of child pornography law in the United States

Date	Legislation/Ruling [7]	Comment
1978	Sexual Exploitation of Children Act	First federal law specifically dealing with child pornography. Prohibited the manufacture and commercial distribution of obscene material involving minors under 16.
1982	New York v. Ferber	Child pornography not protected by the First Amendment. Child pornography separated from obscenity laws, to be judged on a different standard.
1984	Child Protection Act	Age of minor covered by child pornography legislation was raised to 18, and distinction between child pornography and obscenity codified.
1986	United States v. Dost	Expanded the definition of child pornography to include sexually suggestive depictions of a lascivious nature.
1988	Child Protection and Obscenity Enforcement Act	Illegal to use a computer to depict or advertise child pornography.
1990	Osborne v. Ohio	Private possession of child pornography ruled to be illegal.
1996	Child Pornography Protection Act	Definition of child pornography expanded to include virtual images of children and images that appear to be of a minor.
1998	Child Protector and Sexual Predator Punishment Act	Internet Service Providers (ISPs) required to report known incidents of child pornography to authorities, but not required to actively monitor customers or sites.

2002	Ashcroft v. Free Speech Coalition	Virtual images ruled not to be pornography; 'appear to be a minor' ruled to be too broad.

To summarize the current federal legal situation in the United States:

- A child is defined as any person under the age of 18. Legislation has attempted to broaden the law to include computer-generated images (virtual images that do not involve real children) and people over 18 who appear to be minors. However, the court overturned both of these provisions. Congress has subsequently made a number of amendments to tighten federal law in these areas. Because of the evolving nature of legal provision with respect to Internet child pornography, the reader is advised to obtain up-to-date legal advice on the current situation.
- A different and more stringent standard is applied to images involving children than to images involving adults. Pornography involving a child does not have to involve obscene behavior, but may include sexually explicit conduct that is lascivious or suggestive. For example, in United States v. Knox (1993)[8] a man was convicted for possessing videos in which the camera focused on the clothed genital region of young girls.[9]
- Possession of (not just production and trading of) child pornography is an offense. In the case of the Internet, images do not have to be saved for an offense to have occurred—they simply need to have been accessed.

Most states have followed the federal lead with specific legislation, allowing state police to join federal agencies in the fight against child pornography.[10] However, the exact nature of the legislation varies considerably among states. There is also a wide variation in international laws covering child pornography, and this can have significant implications for law enforcement.

Non-legal Definitions

Because legal definitions of both child and pornography differ considerably among jurisdictions, for research purposes child pornography is often defined broadly as any record of sexual activity involving a prepubescent person. Pornographic records include still photographs, videos, and audio recordings. The images themselves vary considerably in their graphic content. In some cases individuals may collect images that do not involve overt pornography and are not technically illegal. There are 10 levels of image severity:[11]

1. Indicative: non-sexualized pictures collected from legitimate sources (e.g., magazines, catalogs).
2. Nudist: naked or semi-naked pictures of children in appropriate settings collected from legitimate sources.
3. Erotica: pictures taken secretly of children in which they reveal varying degrees of nakedness.
4. Posing: posed pictures of children in varying degrees of nakedness.
5. Erotic posing: pictures of children in sexualized poses and in varying degrees of nakedness.
6. Explicit erotic posing: pictures emphasizing the genitals.
7. Explicit sexual activity: record of sexual activity involving children but not involving adults.
8. Assault: record of children subjected to sexual abuse involving digital touching with adults.
9. Gross assault: record of children subjected to sexual abuse involving penetrative sex, masturbation, or oral sex with adults.
10. Sadistic/bestiality: record of children subjected to pain, or engaging in sexual activity with an animal.

The Role of the Internet in Promoting Child Pornography

The Internet has escalated the problem of child pornography by increasing the amount of material available, the efficiency of its distribution, and the ease of its accessibility. (See Appendix A for a summary of key terms and concepts relating to the Internet.) Specifically, the Internet:

- permits access to vast quantities of pornographic images from around the world
- makes pornography instantly available at any time or place
- allows pornography to be accessed (apparently) anonymously and privately

- facilitates direct communication and image sharing among users
- delivers pornography relatively inexpensively
- provides images that are of high digital quality, do not deteriorate, and can be conveniently stored
- provides for a variety of formats (pictures, videos, sound), as well as the potential for real-time and interactive experiences
- permits access to digital images that have been modified to create composite or virtual images (morphing).

Components of the Problem

The problem of Internet child pornography can be divided into three components—the production, distribution, and downloading of images. In some cases, the same people are involved in each stage. However, some producers and/or distributors of child pornography are motivated solely by financial gain and are not themselves sexually attracted to children.

Production

This involves the creation of pornographic images. Collectors place a premium on new child pornography material. However, many images circulating on the Internet may be decades old, taken from earlier magazines and films. Images may be produced professionally, and, in these cases, often document the abuse of children in third-world countries. However, more commonly, amateurs make records of their own sexual abuse exploits, particularly now that electronic recording devices such as digital cameras and web cams permit individuals to create high quality, homemade images.[12] With the advent of multimedia messaging (MMR) mobile phones, clandestine photography of children in public areas is becoming an increasing problem.

Distribution

This involves the uploading and dissemination of pornographic images. These images may be stored on servers located almost anywhere in the world. Distribution may involve sophisticated pedophile rings or organized crime groups that operate for profit, but in many cases, is carried out by individual amateurs who seek no financial reward. Child pornography may be uploaded to the Internet on websites or exchanged via e-mail, instant messages, newsgroups, bulletin boards, chat rooms, and peer-to-peer (P2P) networks. Efforts by law enforcement agencies and Internet Service Providers (ISPs) to stop the dissemination of child pornography on the Internet have led to changes in offenders' methods. Child pornography websites are often shut down as soon as they are discovered, and openly trading in pornography via e-mail or chat rooms is risky because of the possibility of becoming ensnared in a police sting operation (e.g., undercover police entering chat rooms posing as pedophiles or as minor children). Increasingly those distributing child pornography are employing more sophisticated security measures to elude detection and are being driven to hidden levels of the Internet (see Table 2).

Table 2: Distribution methods of child pornography on the Internet. *[13]*

Method	Use
Web pages and websites	Specific child pornography websites may be created, or child pornography images may be embedded in general pornography sites. However, there is debate about how much child pornography is available on the web. Some argue that it is relatively easy to find images.[14] Others argue that, because of the vigilance of ISPs and police in tracking down and closing child pornography websites, it is unlikely that a normal web search using key words such as childporn would reveal much genuine child pornography.[15] Instead, the searcher is likely to find legal pornographic sites with adults purporting to be minors, 'sting' operations, or vigilante sites. One strategy of distributors is to post temporary sites that are then advertised on pedophile bulletin boards. To prolong their existence these sites may be given innocuous names (e.g., volleyball) or other codes (e.g., ch*ldp*rn) to pass screening software. The websites may be immediately flooded with hits before they are closed down. Often the websites contain Zip archives, the password for which is then later posted on a bulletin board.
Web cam	Images of abuse may be broadcast in real time. In one documented case of a live broadcast, viewers could make

	online requests for particular sexual activities to be carried out on the victim.[16]
E-mail	E-mail attachments are sometimes used by professional distributors of child pornography, but more frequently they are used to share images among users, or they are sent to a potential victim as part of the grooming/seduction process. This method is considered risky by seasoned users because of the danger in unwittingly sending e-mails to undercover police posing as pedophiles or as potential victims.
E-groups	Specific child pornography e-groups exist to permit members to receive and share pornographic images and exchange information about new sites. Some of these groups appear on reputable servers and are swiftly shut down when they are detected. However, they may use code names or camouflage child pornography images among legal adult pornography to prolong their existence.
Newsgroups	Specific child pornography newsgroups provide members with a forum in which to discuss their sexual interests in children and to post child pornography. This is one of the major methods of distributing child pornography. Some child pornography newsgroups are well known to both users and authorities (for example, the abpep-t or alternative binaries pictures erotica pre-teen group). Most commercial servers block access to such sites. Some servers do provide access to them but a user runs the risk of having his/her identity captured either by the credit card payments required for access, or the record kept by the server of his/her IP address. However, a computer-savvy user can access these groups by using techniques that hide his/her identity by concealing his/her true IP address.
Bulletin Board Systems (BBS)	Bulletin boards may be used legally to host discussions that provide advice to seekers of child pornography, including the URLs of child pornography websites and ratings of those sites. These bulletin boards may be monitored by system administrators to exclude bogus or irrelevant postings, such as from vigilantes.
Chat rooms	Chat rooms may be used to exchange child pornography and locate potential victims. Chat rooms may be password-protected. Open chat rooms are avoided by seasoned child pornographers because they are often infiltrated by undercover police.
Peer-to-peer (P2P)	P2P networks facilitate file sharing among child pornography users. These networks permit closed groups to trade images.

Downloading

This involves accessing child pornography via the Internet. The images do not need to be saved to the computer's hard drive or to a removable disk to constitute downloading. In some cases a person may receive spam advertising child pornography, a pop-up link may appear in unrelated websites, or he may inadvertently go to a child pornography website (e.g., by mistyping a key word). In most cases, however, users must actively seek out pornographic websites or subscribe to a group dedicated to child pornography. In fact, it has been argued that genuine child pornography is relatively rare in open areas of the Internet, and, increasingly, those seeking to find images need good computer skills and inside knowledge of where to look.[17] Most child pornography is downloaded via newsgroups and chat rooms. Access to websites and online pedophile groups may be closed and require paying a fee or using a password.

Extent of the Problem

It is difficult to be precise about the extent of Internet child pornography, but all of the available evidence points to it being a major and growing problem. At any one time there are estimated to be more than one million pornographic images of children on the Internet, with 200 new images posted daily.[18] One offender arrested in the U.K. possessed 450,000 child pornography images.[19] It has been reported that a single child pornography site received a million hits in a month.[20] As noted above, one problem in estimating the number of sites is that many exist only for a brief period before they are shut down, and much of the

trade in child pornography takes place at hidden levels of the Internet. It has been estimated that there are between 50,000 and 100,000 pedophiles involved in organized pornography rings around the world, and that one-third of these operate from the United States.[21]

Profile of Users

There is no one type of Internet child pornography user, and there is no easy way to recognize an offender. Having a preconceived idea of a child sex offender can be unhelpful and prove a distraction for investigating police.[22] Users of Internet child pornography:

- **are not necessarily involved in hands-on sexual abuse of children.** It is not known exactly how many people may access child pornography on the Internet without ever physically abusing a child. Before the Internet, between one-fifth and one-third of people arrested for possession of child pornography were also involved in actual abuse.[23] However, the Internet makes it easy for people who may never have actively sought out traditional forms of child pornography to satisfy their curiosity online and this may encourage casual users. Looking at the relationship from the other direction, those convicted of sexually abusing children will not necessarily seek out or collect child pornography, with one study putting the number of offenders who do so at around 10 percent.[24]The term child molester covers a wide variety of offenders, from serial predators to situational offenders who may not have ingrained sexual interest in children.
- **may come from all walks of life and show few warning signs.** In fact, users of child pornography on the Internet are more than likely to be in a relationship, to be employed, to have an above average IQ, to be college educated, and to not have a criminal record.[25]Those arrested for online child pornography crimes have included judges, dentists, teachers, academics, rock stars, soldiers, and police officers.[26] Among the few distinguishing features of offenders are that they are likely to be white, male, and between the ages of 26 and 40, and may be heavy Internet users to the extent that it interferes with other aspects of their lives.[27]

A Psychological Typology

Sexual attraction to children is known as pedophilia.[28]However, an interest in Internet child pornography may be best thought of as falling along a continuum rather than in terms of a hard and fast distinction between pedophiles and non-pedophiles. People can behave very differently on the Internet than they do in other areas of their lives. Interacting anonymously with a computer in the safety of one's own home encourages people to express hidden thoughts and desires.[29] Offenders vary in the strength of their interest in child pornography, as well as in the level of severity of the pornographic image to which they are attracted. From a psychological perspective, based on a typology of general pornography users,[30] the following categories of Internet child pornography users are suggested:

1. Recreational users: They access child pornography sites on impulse, out of curiosity, or for short-term entertainment. They are not seen to have long-term problems associated with child pornography use.
2. At-risk users: They are vulnerable individuals who have developed an interest in child pornography, but may not have done so had it not been for the Internet.
3. Sexual compulsives: They have a specific interest in children as sexual objects and seek out child pornography.

An Offending Typology

Variations among offenders translate into different patterns of Internet behavior. Offenders vary in the level of their involvement in Internet child pornography, the degree of networking in which they engage with other offenders, their expertise in employing security strategies to avoid detection, and the extent to which their Internet behavior involves direct sexual abuse of children. The following typology of child pornography offending has been suggested:[31]

1. **Browsers:** Offenders who stumble across child pornography but knowingly save the images. They are not involved in networking with other offenders and do not employ security strategies to avoid detection. Their browsing is an indirect

abuse of children.

2. **Private fantasizers:** Offenders who create digital images (e.g., through morphing) for private use to satisfy personal sexual desires. These offenders do not network with other offenders, do not employ security strategies, and their private fantasies are an indirect abuse of victims.
3. **Trawlers:** Offenders who seek child pornography on the web through open browsers. They may engage in minimal networking, but they employ few security strategies and their trawling is an indirect abuse of victims.
4. **Non-secure collectors:** Offenders who seek child pornography in non-secure chat rooms (i.e., chat rooms that do not employ security barriers such as passwords) and other open levels of the Internet. They are involved in relatively high levels of networking, and, by definition, do not employ security strategies. Their collecting behavior is an indirect abuse of children. Because of the non-secured nature of their activities, there are limits to the number and nature of the images they can collect.
5. **Secure collectors:** Offenders who are members of a closed newsgroup or other secret pedophile ring. They engage in high levels of networking and employ sophisticated security measures to protect their activities from detection. Their collecting behavior is an indirect abuse of children. Because they occupy hidden levels of the Internet, they have access to a wide range of images. They may engage in obsessive levels of collecting, which not only involves amassing huge numbers of images, but also carefully cataloging and cross referencing them. As with other types of collections, they may expend considerable effort in obtaining rare and highly prized images. The collection may become an end in itself.
6. **Groomers:** Offenders who develop online relationships with children and send pornography to children as part of the grooming process. Grooming involves direct abuse of children. They may or may not be involved in wider networking with other offenders, but their contact with children exposes them to risk of detection. The child may tell someone about the relationship, or the offender may be unwittingly communicating with an undercover police officer.
7. **Physical abusers:** Offenders who sexually abuse children and for whom an interest in child pornography is just part of their pedophilic interests. They may record their own abuse behaviors for their personal use, in which case, from a legal standpoint, the possession of pornography is secondary to the evidence of their abusive behavior that it records. They may or may not network. By definition, a physical abuser directly abuses victims and his security depends upon the child's silence.
8. **Producers:** Offenders who record the sexual abuse of children for the purpose of disseminating it to others. The extent of their networking varies depending on whether they are also distributors. Again the producer's direct abuse of the victim compromises his security.
9. **Distributors:** Offenders involved in disseminating abuse images. In some cases they have a purely financial interest in child pornography. More often, offenders at any of the above levels who share images may be classified as distributors. Thus, the extent of a distributor's networking, his level of security, and whether he engages in direct abuse of children depends upon the level at which he is operating.

Effects of Child Pornography

Effects on the Children Portrayed

The vast majority of children who appear in child pornography have not been abducted or physically forced to participate. [32] In most cases they know the producer—it may even be their father—and are manipulated into taking part by more subtle means. Nevertheless, to be the subject of child pornography can have devastating physical, social, and psychological effects on children.[33]

The children portrayed in child pornography are first victimized when their abuse is perpetrated and recorded. They are further victimized each time that record is accessed. In one study,[34] 100 victims of child pornography were interviewed about the effects of their exploitation—at the time it occurred and in later years. Referring to when the abuse was taking place, victims described the physical pain (e.g., around the genitals), accompanying somatic symptoms (such as headaches, loss of appetite, and sleeplessness), and feelings of psychological distress (emotional isolation, anxiety, and fear). However, most also felt 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. Only five cases were ultimately reported to authorities. In later years, the victims

reported that initial feelings of shame and anxiety did not fade but intensified to feelings of deep despair, worthlessness, and hopelessness. Their experience had provided them with a distorted model of sexuality, and many had particular difficulties in establishing and maintaining healthy emotional and sexual relationships.

Effects on Users

The effects of pornography on users have been extensively researched but results are contentious. There are at least five possible relationships between pornography use and the sexual abuse of children:

- **Pornography use is an expression of existing sexual interests.** An individual who sexually abuses children seeks out child pornography as part of his/her pattern of sexual gratification.[35] The offender's sexual interests cause his/her pornography use rather than the other way around.
- **Pornography is used to prime the individual to offend.** An individual deliberately views child pornography immediately prior to offending. Pornography is used in the short term to sexually stimulate the offender in preparation for offending.[36]
- **Pornography has a corrosive effect.** An individual becomes increasingly interested in child pornography, is attracted to images of increasing severity, and becomes desensitized to the harm victims experience. Use of pornography in the long term may also increase the risk that the person will sexually abuse a child.[37]
- **Pornography has a cathartic effect.** Viewing child pornography is the sole outlet for an individual's sexual attraction to children. Pornography use may substitute for, or even help the individual resist, engaging in hands-on offending.[38]
- **Pornography is a by-product of pedophilia.** Pornography is created in the process of carrying out sexual abuse or is used to groom potential victims and prepare them for abuse.[39] Pornography is incidental to the abuse suffered by the victim.

In all likelihood, the effects of child pornography vary among users, and all of the above relationships may apply depending upon the individual in question.

The Internet and Other Forms of Child Sexual Abuse

In addition to child pornography, the Internet facilitates child sexual abuse in the following ways:

- It allows networking among child abuse perpetrators. The Internet facilitates a subculture of pedophiles, who may share information and tactics and support each other's belief systems.[40]
- It may be used to seek out and groom victims. Perpetrators may enter children's or teens' chat rooms under an assumed identity to access and establish relationships with potential victims.[41]
- It may be used in cyber-stalking. Children may be sexually harassed via the Internet.[42]
- It may be used to promote child sexual tourism. Information is made available to help individuals locate child-sex tourism operators or to make direct contact with child prostitutes.[43]
- It may be used in trafficking children. Mail-order children are available over the Internet.[44]

Sources of Digital Evidence

Computers and their associated services retain a considerable amount of evidence of their use. Determined, computer-savvy offenders may take precautions to cover their tracks, but many offenders will have neither the foresight nor the necessary expertise to do so, and will leave a trail of incriminating evidence.[45]

- **The offender's computer:** Downloaded images saved to a computer's hard drive are the most obvious evidence of pornography use. However, there are also more subtle records that technicians can locate when examining a suspect's computer. For example, log files show who was logged into the computer and when; modem logs record when a computer was connected to the Internet; Web browser history entries show an offender's online activity; and e-mail and

chat logs reveal online communication with cohorts or potential victims. Note, however, that seizure of a suspect's computer requires specialized expertise, and, if handled incorrectly, may result in the loss of critical evidence.[46]

- **Hand-held devices:** An increasing number of devices contain components of a computer (referred to as embedded computer systems) and can be used in child pornography. These devices include digital cameras, personal digital assistants (PDAs), and mobile phones. For example, digital cameras can be used to record abuse; the files can then be easily uploaded to the Internet. Similarly, in addition to voice conversations between perpetrators, mobile phones increasingly permit the recording, storing, and transmitting of digital images. These devices may have incriminating digital records stored on their memory cards.
- **Servers:** Different servers may provide information with which to track pornography use. ISP authentication servers record customer account details against IP addresses (authentication logs), which can then be used to identify users. FTP and web servers used to upload and download electronic files have logs that record users' IP addresses, what files were accessed, and when. Similarly, e-mail servers retain logs of customer use. Local area network servers may be used to store collections of pornography for personal use. Individuals may use local servers connected to their work computers so that searching a suspect's work server may reveal hidden collections of pornography.
- **Online activity:** Purpose-built or commercially available digger engine software allows law enforcement personnel to monitor online activity and identify the IP addresses of chat room contributors.[47] Although online operations can yield conclusive digital evidence of an offender's involvement in Internet child pornography activities, officers should be careful not to become overzealous and engage in entrapment.[48]

Challenges in Controlling Internet Child Pornography

Internet child pornography presents some unique challenges for law enforcement agencies. These challenges include:

- **The structure of the Internet:** The structure of the Internet makes control of child pornography very difficult. The Internet is a decentralized system with no single controlling agency or storage facility. Because it is a network of networks, even if one pathway is blocked, many alternative pathways can be taken to reach the same destination. Similarly, if one website or newsgroup is closed down, there are many others that can instantaneously take its place. The decentralized nature of the Internet, and resultant difficulties in restricting the distribution of child pornography, is exemplified by P2P networks involving direct connections among computers without the need for a central server.[49] It has been argued that the Internet is the ultimate democratic entity and is essentially ungovernable.
- **The uncertainties of jurisdiction:** The Internet is an international communication tool that crosses jurisdictional boundaries. Not only is cooperation among law enforcement agencies necessary to track offenders across jurisdictions, it is required to coordinate resources and avoid duplication of effort.[50] Parallel operations run from different jurisdictions may unknowingly target the same organization or offender. Equally problematic is the issue of who is responsible for investigating child pornography on the Internet when there is no clue as to where the images originate. There is a potential for pornography crimes to go uninvestigated because they do not fall within a particular law enforcement jurisdiction.
- **The lack of regulation:** The Internet, by its nature, is difficult to regulate, but many jurisdictions are reluctant to introduce laws that might help control Internet use. There are debates about the appropriate weight to give to the community's protection on the one hand, and to freedom of speech and commercial interests on the other.[51] There is also legal ambiguity about whether ISPs should be liable for the material they carry (as are television stations) or merely regarded as the conduits for that material (similar to the mail service).[52] The end result is that ISPs' legal obligations with respect to Internet child pornography are often unclear, and, for the most part, the emphasis has been on self-regulation.[53]
- **The differences in legislation:** To the extent that there have been attempts to regulate the Internet, control efforts are hampered by cross-jurisdictional differences in laws and levels of permissiveness regarding child pornography. For example, in the United States a child is defined as someone under 18; in Australia the age is 16.[54]Moreover, countries vary in their commitment to enforce laws and act against offenders, either for cultural reasons or because of corruption.[55]
- **The expertise of offenders:** As the typology of Internet offending behavior suggests, offenders vary in the degree to

which they employ elaborate security measures to avoid detection.[56] There is a core of veteran offenders, some of whom have been active in pedophile newsgroups for more than 20 years, who possess high levels of technological expertise. Pedophile bulletin boards often contain technical advice from old hands to newcomers. It has been argued that many Internet sting operations succeed only in catching inexperienced, low-level offenders.

- **The sophistication and adaptation of Internet technology:** The expertise of offenders is enhanced by the rapid advances in Internet technology. In addition to P2P networks, recent developments include remailers (servers that strip the sender's identity from e-mail) and file encryption (a method of hiding or scrambling data).[57]A technological race has developed between Internet pornographers and law enforcement agencies.[58]
- **The volume of Internet activity:** The sheer amount of traffic in child pornography makes the task of tracking down every person who visits a child pornography site impossible.[59] Many offenders realize that realistically their chances of being caught are quite remote. Similarly, while perhaps worthwhile activities, catching peripheral offenders or disrupting individual networks may have little overall impact on the scale of the problem.

Understanding Your Local Problem

The information provided above is only a generalized description of Internet child pornography. You must combine the basic facts with a more specific understanding of your local problem. Analyzing the local problem carefully will help you design a more effective response strategy.

Asking the Right Questions

The following are some critical questions you should ask in analyzing your particular problem of Internet child pornography, even if the answers are not always readily available. Your answers to these and other questions will help you choose the most appropriate set of responses later on.

Offenses

- How many complaints relating to Internet child pornography have been investigated in your jurisdiction? What were the sources of the complaints?
- What component or components of the problem are occurring locally—production, distribution and/or downloading?
- Is the local problem part of a national or international Internet child pornography ring?
- What level of severity are the pornographic images?
- Are the pornographic images of recent child sexual abuse, or are they old images?
- If the pornographic images are recent, can you identify the locations in which they were made, and are they local?

Victims

- Do victims of child sexual abuse report participating or being depicted in child pornography?
- Do victims of child sexual abuse report being shown child pornography by the offender?
- If the pornographic images are recent, can you identify the victims and are they local?
- Have any local children been the subjects of child pornography? If so, what physical and emotional harms did they suffer?
- If local children have been the subjects of child pornography, how were they recruited or coerced into this activity?

Offenders

- Do suspects arrested on child sexual abuse charges possess collections of downloaded pornography?
- Do suspects arrested on child sexual abuse charges keep photographic records of their abusive behaviors?
- Do suspects arrested for possessing child pornography also commit hands-on offenses against children?
- How strong are offenders' interests in Internet child pornography (e.g., are they recreational, at-risk, or sexual compulsive users)?

- What level of severity of pornographic images do the offenders prefer?
- How large are the offenders' collections of child pornography?
- How much time do the offenders devote to Internet child pornography?
- What level of computer expertise do the offenders have?
- Do the offenders network with other offenders?
- What offender-type are the offenders—browsers, private fantasies, trawlers, non-secure collectors, secure collectors, groomers, physical abusers, producers, or distributors?
- If the pornographic images are recent, can the perpetrators be identified, and are they local?

Computer Personnel

- What links does the police department have with local computer personnel (repairers, ISP managers, IT technicians, etc.)?
- Do local ISPs monitor their customers' child pornography use?
- Do local businesses and organizations have formal policies governing their employees' use of the computer at work?
- Have local computer repairers or IT technicians reported evidence of child pornography on their customers' computers?

Community Members

- How concerned is the public about Internet child pornography?
- Has the police department received complaints from the public about child pornography websites?
- Has the police department received complaints from the public about online sexual harassment of children?
- Has the police department received complaints from the public about unauthorized photographs being taken of children in public areas?

Resources and Collaborations

- Which component or components of the problem should be given priority by the police department—production, distribution, and/or downloading?
- Who within the police department has computer expertise that may be useful in assisting with investigations?
- Who in the community may provide technical advice to the police department on Internet child pornography?
- What training is relevant for officers investigating Internet child pornography?
- Should the police department establish a dedicated Internet child pornography unit?
- Does the police department have links with other police departments and agencies that permit coordinated investigations of Internet child pornography?
- How do the activities of the police department synchronize with national and international priorities and initiatives?

Measuring Your Effectiveness

Measurement allows you to determine to what degree your efforts have succeeded, and suggests how you might modify your responses if they are not producing the intended results. You should take measures of your problem before you implement responses, to determine how serious the problem is, and after you implement them, to determine whether they have been effective. (For more detailed guidance on measuring effectiveness, see the companion guide to this series, *Assessing Responses to Problems: An Introductory Guide for Police Problem-Solvers*.)

The following are potentially useful measures of the effectiveness of responses to Internet child pornography:

- Reduced number of complaints from the public about Internet child pornography. Initially, you might want to see an increase in complaints from the public if you have reason to believe the problem is underreported.
- Reduced number of child pornography sites and images on the Internet.
- Reduced number of new child pornography images on the Internet.

- Reduced level of severity of the child pornography images on the Internet.
- Reduced number of images possessed by offenders who are arrested for downloading child pornography.
- Reduced level of severity of the images possessed by offenders who are arrested for downloading child pornography.
- Reduced level of involvement (possession, distribution, or production) of the offenders arrested for Internet child pornography crime.

Other measures are important for tracking official actions taken to address the problem. Among them are:

- The number of offenders arrested for Internet child pornography crimes.
- The number of victims portrayed in Internet child pornography who are identified and assisted.

Responses to the Problem of Internet Child Pornography

Your analysis of your local problem should give you a better understanding of the factors contributing to it. Once you have analyzed your local problem and established a baseline for measuring effectiveness, you should consider possible responses to address the problem.

The following response strategies provide a foundation of ideas for addressing your particular problem. These strategies are drawn from a variety of research studies and police reports. Several of these strategies may apply to your community's problem. It is critical that you tailor responses to local circumstances, and that you can justify each response based on reliable analysis. In most cases, an effective strategy will involve implementing several different responses. Law enforcement responses alone are seldom effective in reducing or solving the problem. Do not limit yourself to considering what police can do: carefully consider whether others in your community share responsibility for the problem and can help police respond to it.

General Considerations for an Effective Response Strategy

As noted, Internet child pornography presents some unique challenges for law enforcement agencies. However, despite the difficulties involved in controlling the problem, local police have an important role to play. To maximize their contribution, local police departments need to:

- **Acquire technical knowledge and expertise in Internet pornography.** If your department does not have a specialized Internet crime unit, then find out where you can obtain assistance or training. Appendix B lists online resources that can provide information on national and international initiatives, tips and leads, technical assistance, and staff training.
- **Establish links with other agencies and jurisdictions.** It is important that local police departments share information and coordinate their activities with other jurisdictions. Appendix B also lists agencies that have specific programs or sections designed to provide a coordinated response to Internet child pornography.
- **Establish links with ISPs.** ISPs can be crucial partners for police. As has been noted, there is often a lack of specific legislation setting out ISPs' obligations. This makes it especially important for police to establish good working relations with ISPs to elicit their cooperation in the fight against Internet child pornography.
- **Prioritize their efforts.** Because of the volume of Internet child pornography crime, police forces need to prioritize their efforts and concentrate on the most serious offenders, particularly those actually involved in abusing children and producing pornographic images.[60] For example, one strategy may be to cross reference lists of Internet child pornography users with sex offender registries to increase the chance of targeting hands-on offenders (see Appendix B). It has been noted that success in combating child pornography is too often judged in terms of the number of images recovered, rather than by the more significant criterion of whether the crimes the images portray have been prevented.[61]

Specific Responses to Reduce Internet Child Pornography

It is generally acknowledged that it is impossible to totally eliminate child pornography from the Internet. However, it is possible to reduce the volume of child pornography on the Internet, to make it more difficult or risky to access, and to identify and arrest the more serious perpetrators. Since 1996, ISPs have removed some 20,000 pornographic images of children from the web.[62] Around 1,000 people are arrested annually in the United States for Internet child pornography offenses.[63] The following strategies have been used or suggested to reduce the problem of child pornography on the Internet.

Computer Industry Self Regulation

ISPs have a central role to play in combating Internet child pornography. The more responsibility ISPs take in tackling the availability of child pornography images on the Internet, the more resources police can devote to addressing the production side of the problem. However, there are two competing commercial forces acting on ISPs with respect to self regulation. On the one hand, if an ISP restricts access to child pornography on its server, it may lose out financially to other ISPs who do not. Therefore, it will always be possible for offenders to find ISPs who will store or provide access to child pornography sites. On the other hand, ISPs also have their commercial reputation to protect, and it is often in their best interests to cooperate with law enforcement agencies. Most major ISPs have shown a commitment to tackling the problem of child pornography. By establishing working relationships with ISPs, and publicizing those ISPs who take self regulation seriously, police may be able to encourage greater levels of self regulation. Current self-regulatory strategies include:

1. A number of ISP associations have drafted formal codes of practice that explicitly bind members to not knowingly accept illegal content on their sites, and to removing such sites when they become aware of their existence. Service agreement contracts with clients will often set out expected standards that apply to site content. Large ISPs may have active cyber patrols that search for illegal sites.[64]
2. Establishing complaint sites/hotlines. Some ISP associations have set up Internet sites or hotlines that allow users to report illegal practices.[65] These associations either deal directly with the complaint (e.g., by contacting the webmaster, the relevant ISP, or the police) or refer the complainant to the appropriate authorities.
3. ISPs can apply filters to the browsers and search engines their customers use to locate websites. There are numerous filtering methods. For example, filters can effectively treat certain key words as if they do not exist, so that using these words in a search will be fruitless.[66] Software that can identify pornographic images is also being developed.[67]

Legislative Regulation

Not everyone is satisfied with the current reliance on self regulation, and there have been calls for increased legislation to compel the computer industry to play a greater role in controlling Internet child pornography. Police may be an important force in lobbying for tighter restrictions. Among the proposals for tighter regulation are:

4. Making ISPs legally responsible for site content. ISPs' legal responsibilities to report child pornography vary among jurisdictions. In the United States, ISPs are legally required to report known illegal activity on their sites, but they are not required to actively search for such sites.[68] It has been argued that ISPs' legal responsibilities should be strengthened to require a more proactive role in blocking illegal sites.[69]
5. Police may apply for a court order to seize ISP accounts.[70] However, to assist in the prosecution of offenders, ISPs need to maintain good records of IP logging, caller ID, web hostings, and so forth.[71]
6. Requiring user verification. ISPs often exercise little control over verifying the identities of people who open Internet accounts. Accounts may be opened using false names and addresses, making it difficult to trace individuals who engage in illegal Internet activity. In addition, without verifying users' ages, there is no way of knowing if children are operating Internet accounts without adult supervision. This problem of Internet anonymity is likely to increase as the potential to access the Internet via mobile phones becomes more common. It has been argued that both ISPs and mobile phone networks need to strengthen procedures for user verification.[72]
7. Remailers are servers that forward emails after stripping them of sender identification. It has been argued that much tighter regulation of remailers is necessary. Some have advocated making remailer administrators legally responsible for knowingly forwarding illegal material, while others have called for a complete ban on remailers.[73]

8. Encryption of pornographic images is shaping to be the biggest technological problem facing law enforcement agencies. Key escrowed encryption would require anyone selling encryption software to supply a trusted third party with a key to the code.[74] This has been strongly resisted by the computer industry. In the meantime, work continues on developing code-breaking software.

Strategies for Related Industries

There are a number of other promising strategies involving other industries with a stake in the Internet. Again, although police may have no direct role in implementing these strategies, they may be able to use their influence to encourage industries to act. Strategies include:

9. Although there has been considerable focus on the role of ISPs in enabling the distribution of Internet child pornography, there has been less attention given to the role played by credit card companies in allowing customers to pay for that pornography. It has been argued that credit card companies have a duty to not knowingly contribute to illegal acts.[75] Some credit card companies have acknowledged the problem and vowed to act.[76]
10. Economic pressure may be applied to service providers to encourage them to monitor illegal content. In one example of this, major brands have withdrawn advertising from P2P networks that carry child pornography.[77]

Workplace Responses

Many medium to large organizations maintain their own servers, which allow employees to access the Internet from and store data on their work computer. Work computers have been implicated in a number of child pornography cases.[78] Workplace strategies may be directed toward altering the behavior of potential offenders by reinforcing the costs associated with offending.

11. **Adopting and enforcing workplace codes of conduct.** Many organizations have explicit policies regarding and consequences for the improper use of work computers. These policies need to be made clear to employees to remove any doubt about what standard of behavior is expected.
12. The traffic through most work-based servers is less than that for commercial ISPs, making it more feasible for the system administrator to electronically monitor staff Internet use.
13. By employing web filters, companies can place restrictions on the sites that employees can visit.[79]

Citizens' Groups

A number of nonprofit organizations have been established to raise public awareness about the issue of Internet child pornography and to act as political lobby groups. These groups include Wired Safety, Safeguarding Our Children – United Mothers (SOC-UM), and End Child Prostitution, ChildPornography and Trafficking of Children for Sexual Purposes (ECPAT).[80] Citizens' groups will usually work in cooperation with law enforcement agencies, and local police can provide active support for their activities, which include:

14. The main activity of these groups is to raise public awareness and provide tips for parents and teachers through their websites, publications, and online classes.
15. Searching the Internet. Many of these groups have their own teams of volunteers who search the Internet, or hotlines where people can report Internet child pornography. Information gathered about child pornography is then passed on to law enforcement agencies. Volunteers should be careful not to inadvertently download child pornography and thus commit a crime.

Parental Strategies

One of the concerns about Internet child pornography is that children may inadvertently access material, or may have material sent to them either as part of a grooming process or by cyber-stalkers. A number of products are available to assist parents in regulating Internet content for their children.[81]Police can play an educative role in informing parents of these effective

strategies by:

16. Encouraging parents to use filtering software. Commercially available software allows parents to restrict or monitor their children's Internet usage and may be available as part of free parental controls by certain ISPs. These programs may block undesirable sites or provide a record of Internet sites visited.
17. The Recreational Software Advisory Council on the Internet (RSACi) rates websites in much the same way movies are rated. This is a voluntary system that allows website operators to obtain a rating, which they can then code into their site. Ratings may be used as a filter on web browsers to help parents control their children's Internet use.
18. Those in charge of a website (the webmaster) may provide key words (meta-tags) that broadly identify their site to assist in the search process. However, a webmaster may include inappropriate key words in the meta-tag to increase visits to their site. For example, a child pornography site may be located under the key word 'Disney'. A number of child-oriented search engines (e.g., Yahooligans!) manually inspect sites for inappropriate material.

Law Enforcement Responses

In the strategies discussed so far the police role has largely involved working in cooperation with other groups or acting as educators. A number of strategies are the primary responsibility of police. As a rule, local police will not carry out major operations. Most major operations require specialized expertise and inter-agency and inter-jurisdictional cooperation. (See Appendix C for a summary of major coordinated law enforcement operations in recent years.) However, local police will almost certainly encounter cases of Internet child pornography in the course of their daily policing activities. Law enforcement responses include:

19. Locating child pornography sites. Police agencies may scan the Internet to locate and remove illegal child pornography sites. Many areas of the Internet are not accessible via the usual commercial search engines, and investigators need to be skilled at conducting sophisticated searches of the 'hidden net.' Police may issue warnings to ISPs that are carrying illegal content.
20. Law enforcement agents may enter pedophile newsgroups, chat rooms, or P2P networks posing as pedophiles and request emailed child pornography images from others in the group.[82]Alternatively, they may enter child or teen groups posing as children and engage predatory pedophiles lurking in the group who may send pornography or suggest a meeting. A variation of the sting operation is to place ads on the Internet offering child pornography for sale and wait for replies.[83]Recently, Microsoft announced the development of the Child Exploitation Tracking System to help link information such as credit card purchases, Internet chat room messages, and conviction histories.[84]
21. These sites purport to contain child pornography but in fact are designed to capture the IP or credit card details of visitors trying to download images. These can be considered a type of sting operation and have resulted in numerous arrests. However, their primary purpose is to create uncertainty in the minds of those seeking child pornography on the Internet, and, therefore, reduce the sense of freedom and anonymity they feel (see Operation Pin in Appendix C).
22. Publicizing crackdowns. Many police departments have learned to use the media to good effect to publicize crackdowns on Internet child pornography.[85] Coverage of crackdowns in the mass media increases the perception among potential offenders that the Internet is an unsafe environment in which to access child pornography.
23. Although most media attention is often given to technological aspects of controlling Internet child pornography, in fact many arrests in this area arise from traditional investigative police work. Investigations may involve information from:

    - **The public:** The public may contact police directly, or information may be received on one of the various child pornography hotlines.
    - **Computer repairers/technicians:** Some states mandate computer personnel to report illegal images.[86] There are cases where computer repairers have found child pornography images on an offender's hard drive and notified police.[87] Police may establish relationships with local computer repairers/ technicians to encourage reporting.
    - **Victims:** A point of vulnerability for producers of child pornography is the child who appears in the pornographic image. If the child informs others of his/her victimization, then the offender's activities may be exposed.[88]
    - **Known traders:** The arrest of one offender can lead to the arrest of other offenders with whom he has had dealings,

producing a cascading effect. In some cases the arrested offender's computer and Internet logs may provide evidence of associates. (See Operation Cathedral in Appendix C.)

- **Unrelated investigations:** There is increasing evidence that many sex offenders are criminally versatile and may commit a variety of other offenses.[89] Police may find evidence of Internet child pornography while investigating unrelated crimes such as drug offenses.

Responses with Limited Effectiveness

24. There are a few citizens' groups (e.g., Ethical Hackers Against Pedophilia) that engage in direct vigilantism by hacking into and disabling suspected offenders' computers, posting anti-pedophile messages on pedophile bulletin boards, and swamping pedophile newsgroups with the aim of closing them down.[90] These activities are often illegal and are not endorsed by most citizens' groups or by law enforcement agencies

Responses to the Problem of Internet Child Pornography

The Internet is a global network comprising millions of smaller networks and individual computers connected by cable, telephone lines, or satellite links. The Internet permits individuals to connect with other computers around the world from the privacy of their own homes. Although the terms Internet and the World Wide Web (WWW) are often used interchangeably, the web specifically refers to the worldwide collection of electronic documents and other files stored throughout the Internet (on web pages and in websites). The web accounts for 90 percent of Internet usage.[91]The web allows individuals to search for and download text, graphics, audio, and video on topics of interest from around the world. They can also upload their own electronic files for others to access. In addition to the World Wide Web, the Internet enables a number of other services and forms of communication, including e-mail, mailing lists, e-groups, newsgroups, bulletin boards, chat rooms, instant messaging, and peer-to-peer (P2P) networks. These services permit a user to engage in conversations with other individuals and share electronic files. Specific terms associated with the Internet, the World Wide Web, and related communication services are in the following table:

The Internet	
Term	Definition [92]
Host	Any computer or network connected to the Internet.
Modem	Device for connecting a host to the Internet. Includes dial-up modems that may use standard telephone lines and dedicated cable modems.
Internet Protocol (IP) address	A number that uniquely identifies each host using the Internet.
Server	A computer configured to provide a service to other computers in a network, including access to hardware and software and centralized data storage. Different servers may be used to perform specific functions (e.g., web server or email server).
Internet Service Provider (ISP)	A business that provides individuals or companies access to the Internet (e.g., AOL, MSM, Earthlink). ISPs use authentication servers to verify customers' passwords.
File Transfer Protocol (FTP)	A protocol that permits the downloading and uploading of electronic files. Downloading is the process by which a computer receives an electronic file from the Internet via an FTP server; uploading is the process of transferring electronic files from a computer to an FTP server on the Internet.

The World Wide Web	
Term	Definition [93]
Web page	An electronic document that may comprise text, graphics, audio, and video, as well as links to other pages.
Website	A collection of related web pages and associated media stored on a web server.

Home page	First page displayed on a website that usually acts as an introduction to the site.
Web cam	Video camera that permits live images to be displayed via a web page.
Universal Resource Locater (URL)	A web page's unique location or address.
Web browser	Software that allows web pages to be accessed and viewed (e.g., Internet Explorer, Netscape, Mozilla-Firefox).
Hyperlink	A link provided within a web page to connect other related web pages. Pop-up links not requested by the user may also appear on some web pages.
Search engine	A program (e.g., Google, Alta Vista) that locates websites and web pages using key words.

Communication Services

Term	Definition [94]
E-mail	A method of communication between individuals connected to the Internet involving the transmission of text messages and attached files.
Mailing lists	A group of e-mail addresses given a common name so all members on the list receive the same message. There is a central list owner who controls who is on the list and what material can be sent. Individuals may subscribe to have their name and address added to the mailing list.
E-groups	Groups established to share information on a topic of common interest. Potential members need to subscribe to the group. In addition to email, an e-group may offer other features such as a chat room, a bulletin board, and a central home page.
Newsgroups	A site, stored on a news server, that allows contributors to have discussions about a particular subject by posting text, pictures, etc., and responding to previous posts. In most cases no one owns a newsgroup and there is no central authority. However, in some cases a password may be required, and some newsgroups filter posts through a moderator. The network of newsgroups is called Usenet.
Bulletin Board Systems (BBS)	Bulletin board systems, which predate the Internet, are similar to newsgroups, but tend to be in real time to allow contributors to engage in conversations. Bulletin boards are often hosted by an owner rather than a server, and may be accessed directly via a modem without going through the Internet.
Chat rooms	A chat room is a location on a server that permits multiple users to engage in real-time conversations and exchange electronic files. Many chat rooms are open to anyone to log into, but some are closed. They may employ a moderator, but users can nominate a pseudonym.
Instant messaging (IM)	Similar to chat rooms, but instant messaging permits private conversations with nominated contacts. Once a connection is established, direct contact between users is possible without the need for a central server.
Peer-to-peer (P2P)	A network in which each computer is an equal partner and all work cooperatively together. All computers in the network have a common file-sharing program (e.g., KaZaA, Morpheus, Limewire), allowing users to connect directly to each other's hard drive to search for and exchange files.

Appendix B: Agencies and Programs Addressing Internet Child Pornography

A variety of law enforcement agencies have a stake in preventing and investigating Internet child pornography. Some of these agencies have specific programs or sections to focus resources and coordinate ongoing responses. In the United States, key agencies and services include: [95]

- Child Exploitation and Obscenity Section (CEOS): A section of the U.S. Department of Justice's Criminal Division, CEOS specializes in the investigation and prosecution of child exploitation and obscenity cases, including child pornography. It provides training for federal, state and local prosecutors and law enforcement agents concerning these crimes. www.usdoj.gov/criminal/ceos/childporn.html
- CyberSmuggling Center: Formed by the U.S. Customs Service, the center focuses particularly on undercover operations into international production and distribution of child pornography. http://www.cbp.gov/xp/cgov/home.xml
- Cyber Tipline: An online clearinghouse for tips and leads on Internet child exploitation. The program is jointly sponsored by the NCMEC, the U.S. Postal Inspection Service, the U.S. Customs Service, and the FBI. www.cybertipline.com
- Innocent Images: The central operation and case management system coordinating FBI investigations into child exploitation via the Internet. www.fbi.gov/hq/cid/cac/innocent.htm
- Internet Crimes Against Children (ICAC): A task force program initiated by the Office of Juvenile Justice and Delinquency Prevention (OJJDP), U.S. Department of Justice. It provides regional clusters of forensic and investigative expertise to assist state and local law enforcement agencies in dealing with Internet child exploitation. http://www.ojjdp.ncjrs.org/programs/index.html
- National Center for Missing & Exploited Children (NCMEC): A private, nonprofit organization whose mission includes following up on tips from the Cyber Tipline and providing technical assistance and training to other agencies. www.missingkids.com
- National Sex Offender Public Registry: A web site supported by the U.S. Department of Justice that provides details on the location of offenders convicted of sexually violent offenses. www.nsopr.gov
- U.S. Postal Inspection Service: This service has particular responsibilities to investigate the distribution of child pornography via mail. Internet activity is often supported through traditional mail. www.usps.com/postalinspectors

A number of major law enforcement operations demonstrate the need for interagency and international cooperation. A summary of major operations is shown in the table below.

Appendix C: Examples of Coordinated Law Enforcement Operations

Operation Avalanche/Ore [96]		
The Problem	The Response	The Outcome
Landslide Productions was a child pornography company operating out of Fort Worth, Texas. Landslide had a complex network of some 5,700 websites worldwide (especially in Russia and Indonesia) that stored child pornography images. The operation in Fort Worth acted as a gateway into the network. Online customers provided credit card details to obtain network access. Landslide scrambled these credit card numbers to protect customers' identities. There were more than 390,000 subscribers from 60 countries, generating a monthly turnover of up to $1.4 million.	The investigation began in 1999 when the U.S. Postal Inspection Service discovered that Landslide's customers were sending monthly subscription fees to a post office box or paying them through the Internet. A joint investigation between the U.S. Postal Inspection Service and the Internet Crimes Against Children Task Force (ICAC), comprising more than 45 officers, was conducted over two years (Operation Avalanche). Officers cracked the code that scrambled the credit card numbers and then tracked down the card owners. Landslide's bank accounts were seized and 160 search warrants were executed that recovered large quantities of child pornography. The investigation was expanded to include the U.K. police (Operation Ore).	To date, 120 arrests have been made in the U.S., including the two principal operators who were given life and 14year sentences respectively in 2001. In the U.K. some 7,000 customers were identified, 1,300 people arrested, and 40 children taken into protective custody. Despite closing down Landslide Productions, there has been criticism that relatively few offenders have been successfully prosecuted.
Operation Cathedral [97]		
The Problem	The Response	The Outcome
The Wonderland Club was an exclusive online pedophile ring in which members reportedly had to produce 10,000 child	In 1996, two U.S. offenders charged with online child pornography offenses (the Orchid Club) cooperated with police and provided information about a British offender.	The Wonderland Club was destroyed, and there were 107 arrests around the

pornography images for membership. At least 180 individuals from at least 33 countries had met this criterion, and seven members between them had contributed 750,000 images.	Evidence from that offender's computer hard drive led to the discovery of the Wonderland Club. The operation, conducted between 1998 and 2001, involved U.S. and British police coordinating through Interpol. Although agents were unable to gain undercover entry into the club, they were able to monitor transactions and gather evidence from the outside. Eventually, 35 members were identified. Police forces in 12 countries carried out more than 100 simultaneous raids on suspects.	world, 14 of which were in the United States.

Operation Candyman ***[98]***

The Problem	The Response	The Outcome
Candyman, was an open e-group maintained by Yahoo that was involved in exchanging child pornography. It had 7,000 members, 4,600 of which were in the United States and the remaining 2,400 lived around the world.	Undercover FBI agents identified and infiltrated the e-group in a year-long undercover operation ending in 2002. The task force comprised 56 FBI field officers. A court order was obtained to compel Yahoo to provide the unique e-mail addresses of all members, and subpoenas were issued to all ISPs to provide the addresses of U.S. users.	The FBI was able to obtain 1,400 addresses, from which 707 suspects were identified, 266 searches carried out, and 89 arrests made to date. Those arrested include a school bus driver, a teacher's aide, law enforcement personnel, and clergy members.

Operation Pin ***[99]***

The Problem	The Response	The Outcome
The operation is directed at the general proliferation of child pornography websites and the number of people accessing these sites. In particular it is aimed at casual or first-time offenders.	The operation was started in 2003 by West Midlands (U.K.) police and expanded to include the FBI, the Australian Federal Police, the Royal Canadian Mounties, and Interpol. Far from being a covert operation, it was officially launched with media releases by the relevant police forces. It is a classic honey trap operation. A website purporting to contain child pornography was set up. Visitors to the site were required to go through a series of web pages, which appeared to be identical to real web porn sites, searching for the image they wanted. At each point it was reinforced that they were in a child pornography site, and they were given the option to exit. When they did try to access an image they were told they had committed a crime. They were tracked down via their credit card details, which they were required to provide to login.	This crime prevention operation has resulted in numerous arrests; however, precise numbers are not available. Its main purpose is to make searchers of child pornography on the Internet uncertain that they can do so anonymously. Details of the sting operation were widely publicized on child pornography sites, contributing to the deterrent effect.

Summary of Responses to Internet Child Pornography

The table below summarizes the responses to false burglar alarms, the mechanism by which they are intended to work, the conditions under which they ought to work best, and some factors you should consider before implementing a particular response. It is critical that you tailor responses to local circumstances, and that you can justify each response based on reliable analysis. In most cases, an effective strategy will involve implementing several different responses. Law enforcement responses alone are seldom effective in reducing or solving the problem.

The table below summarizes the responses to Internet child pornography, the mechanisms by which they are intended to work, the conditions under which they ought to work best, and some factors you should consider before implementing a particular response. It is critical that you tailor your responses to local circumstances, and that you can justify each response based on reliable analysis. In most cases, an effective strategy will involve implementing several different responses. Law enforcement responses alone are seldom effective in reducing or solving the problem.

#	Response	How It Works	Works Best If…	Considerations
Computer Industry Self Regulation				
1.	**Removing illegal sites**	Reduces availability of pornography; ISPs agree voluntarily to refuse to accept child pornography sites and to remove any sites once identified	…all ISPs agree to participate	There is a financial advantage for some ISPs to continue to accept child pornography sites. Pressure may be applied to ISPs by police to increase compliance; some international ISPs are beyond the reach of formal codes of conduct
2.	**Establishing complaint sites/hotlines**	Facilitates reporting; public is given the opportunity to report illegal sites	…existence of the complaint sites/ hotlines are widely known	Although many reported sites will have already been identified by the ISP, sites that have escaped the cyber patrols may be uncovered
3.	**Filtering browsers/ search engines**	Prevents customers from accessing child pornography sites	…all providers agree to use filters	Not all illegal sites will be identified; applies only to child pornography located on open areas of the web
#	Response	How It Works	Works Best If…	Considerations
Legislative Regulation				
4.	**Making ISPs legally responsible for site content**	Enhances screening and surveillance of child pornography; ISPs to be legally required to identify and remove illegal sites	…there is national and international consistency in legislative approach	Resisted by computer industry, which favors self-regulation; debate about the balance between protecting society and free speech
5.	**Requiring the preservation of ISP records**	Facilitates criminal investigations; records of customers' Internet use are retained in case required as evidence	Same as No. 4 above	Same as No. 4 above
6.	**Requiring user verification**	Deters offenders from seeking child pornography on the World Wide Web; ISPs should require verification of an applicant's identity before providing an account	Same as No. 4 above	Same as No. 4 above; this problem will become more critical as greater integration of Internet and mobile phone services occurs
7.	**Regulating anonymous remailers**	Reduces anonymity of offenders; remailer administrators are made legally responsible for material forwarded	Same as No. 4 above	Same as No. 4 above
8.	**Using key escrowed encryption**	Reduces anonymity of offenders; encryption keys held by a trusted third party	Same as No. 4 above	Same as No. 4 above
#	Response	How It Works	Works Best If…	Considerations
Strategies for Related Industries				
9.	**Blocking credit card transactions**	Deters offenders and/or reduces profitability of online child pornography; credit card companies refuse to authorize payments for child pornography	…all companies agree to participate	Not all child pornography requires payment
10.	**Boycotting sites by advertisers**	Reduces profitability of online child pornography; companies refuse to place advertisements on networks that carry child pornography	…the boycott is widespread and highly publicized	The aim of boycotts is to pressure service providers to monitor illegal activity

Workplace Responses				
11.	**Adopting and enforcing workplace codes of conduct**	Deters offenders by removing excuses for using workplace computers to access child pornography; organizations that maintain their own servers have explicit policies governing computer use by staff	…codes are formal and clearly communicated to all staff	Applies only to child pornography accessed or stored at work
12.	**Auditing computer use**	Deters offenders by increasing surveillance of their computer use; staff Internet use is routinely monitored	…staff are aware in advance that audits will be conducted	Same as No. 11 above
13.	**Filtering web usage**	Reduces access to online child pornography; companies restrict the sites that employees may visit	Same as No. 11 above	Same as No. 11 above
#	Response	How It Works	Works Best If…	Considerations
Citizens' Groups				
14.	**Educating the public**	Enhances awareness and improves web surveillance; information is provided to parents and teachers about Internet child pornography	…it is done in cooperation with law enforcement agencies	Directed mainly toward preventing online exploitation of children and access by children to child pornography
15.	**Searching the Internet**	Enhances web surveillance; hotlines and Internet searches by volunteers identify child pornography sites	Same as No. 14 above	Volunteers need to be careful not to download pornography and thus commit a crime
#	Response	How It Works	Works Best If…	Considerations
Parental Strategies				
16.	**Encouraging parents to use filtering software**	Reduces exposure of children to online child pornography; software installed on home computers that restricts sites that may be visited and/or keeps a record of sites visited	…combined with supervision of children's computer use and education about appropriate sites	Specifically targets children's access to child pornography; police have a role in educating the public about safe Internet use
17.	**Encouraging parents to review web ratings**	Reduces exposure of children to online child pornography; websites independently rated for age suitability	Same as No. 16 above	Same as No. 16 above
18.	**Promoting the use of child-oriented search engines**	Reduces exposure of children to online child pornography; search engines specifically designed for children, where sites are manually inspected for inappropriate material	Same as No. 16 above	Same as No. 16 above
#	Response	How It Works	Works Best If…	Considerations
Law Enforcement Responses				
19.	**Locating child pornography sites**	Increases an offender's risk of apprehension; law enforcement agencies conduct their own searches of the Internet for child pornography	…coordinated with other agencies and jurisdictions	Requires specialized expertise to access hidden areas of the Internet
20.	**Conducting undercover sting operations**	Deters offenders through increased risk of apprehension; undercover law enforcement agents enter pedophile newsgroups, etc., to collect evidence against offenders	Same as No. 19 above	Same as No. 19 above; may target novice or low-level offenders

21.	**Setting up honey trap sites**	Increases an offender's risk of apprehension; phony child pornography sites are established that capture the details of offenders who attempt to access the supposed pornography	…the existence of the sites is widely publicized to increase the deterrent effect	Same as No. 20 above
22.	**Publicizing crackdowns**	Increases the perception among offenders that the Internet is an unsafe environment to access child pornography	…publicity is widespread and sustained	Same as No. 20 above
23.	**Conducting traditional criminal investigations**	Increases an offender's risk of apprehension; police uncover information about child pornography in the course of their daily work	…police have strong links with key community groups	Key role for local police
#	Response	How It Works	Works Best If…	Considerations
Responses With Limited Effectiveness				
24.	**Engaging in vigilantism**	Increases an offender's risk of apprehension; vigilantes disable suspected offenders' computers and disrupt pedophile newsgroups		Actions may be illegal

Endnotes

[1] Tate (1990); Tyler (1985).

[2] Crewdson (1988); Tate (1990).

[3] Jewkes and Andrews (2005); Williams (2003).

[4] Wolak et al. (2003).

[5] Jenkins (2001).

[6] Alder (2001); Esposito (1998); Graham, (2000)[Full Text] ; Grasz and Pfaltzgraff (1998)[Full Text] ; Klain, Davies, and Hicks (2001)[Full Text] ; Linz and Imrich (2001).

[7] Sexual Exploitation of Children Act (Pub.L. 95-225, 92 Stat. 7); *New York v. Ferber*, 458 U.S. 747 (1982); Child Protection Act (18 U.S.C. § 2251, 2252, et seq.); *United States v. Dost*, 636 F.Supp. 828, 832 (S.D. Cal. 1986), aff'd sub nom.; *United States v. Wiegand*, 812 F.2d 1239, 1244-45 (9th Cir. 1987), cert. denied, 484 U.S. 856 (1987); Child Protection and Obscenity [9] Enforcement Act (amending § 2251, 2252); *Osborne v. Ohio*, 495 U.S. 103 (1990); Child Pornography Protection Act (18 U.S.C. § 2252A, 2256(8)); Child Protector and Sexual Predator Punishment Act (42 U.S.C. § 13032); *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

[8] *United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), cert denied, 513 U.S. 1109 (1995).

[9] Jenkins (2001).

[10] Klain, Davies, and Hicks (2001)[Full Text] .

[11] Taylor, Holland, and Quayle (2001)[Full Text] .

[12] Lanning and Burgess (1989).

[13] Blundell et al. (2002); Calder (2004); Ferraro et al. (2004); Jenkins (2001); U.S. General Accounting Office (2003)[Full Text] .

[14] Khan (2000)[Full Text] .

[15] Forde and Patterson (1998)[Full Text] ; Jenkins (2001); Lesce (1999)[Full Text] .

[16] Burke et al. (2002).

[17] Forde and Patterson (1998)[Full Text] ; Jenkins (2001); Lesce (1999)[Full Text] .

[18] Wellard (2001)[Full Text] .

[19] Carr (2004)[Full Text] .

[20] Jenkins, (2001).

[21] Jenkins (2001).

[22] Simon (2000).

[23] Dobson (2003); Wellard (2001)[Full Text] .

[24] Smallbone and Wortley (2000)[Full Text] .

[25] Blundell et al. (2002); Schwartz and Southern (2000).

[26] Calder (2004).

[27] Blundell et al. (2002); Schneider (2000).

[28] Linz and Imrich (2001).

[29] Quayle and Taylor (2001).

[30] Cooper et al. (1999).

[31] Krone (2004)[Full Text] .

[32] Lanning and Burgess (1989).

[33] Klain, Davies, and Hicks (2001)[Full Text] .

[34] Silbert (1989).

[35] Marshall (2000).

[36] Marshall (1988); Proulx, Perreult, and Ouimet (1999).

[37] Linz and Imrich (2001); Marshall (2000).

[38] Kennedy-Souza (1998); Taylor and Quayle (2003).

[39] Goldstein (1999).

[40] O'Connell (2001).

[41] Aftab (2000).

[42] Finkelhor, Mitchell, and Wolak (2000)[Full Text] ; Donnerstein (2002).

[43] Aloysius (2001).

[44] Calder (2004).

[45] Ferraro et al. (2004).

[46] Ferraro et al. (2004).

[47] Grant, David, and Grabosky (1997).

[48] Ferraro et al. (2004); Graham (2000)[Full Text] .

[49] U.S. General Accounting Office (2003)[Full Text] .

[50] Jewkes and Andrews (2005).

[51] Graham (2000)[Full Text] ; Stanley (2001)[Full Text] ; Thomas (1997).

[52] Jenkins (2001).

[53] Grant, David, and Grabosky (1997).

[54] Krone (2004)[Full Text] .

[55] Khan (2000)[Full Text] .

[56] Jenkins (2001).

[57] Burke et al. (2002); Forde and Patterson (1998)[Full Text] ; Mostyn (2000); Thornburgh and Lin (2002).

[58] Jewkes and Andrews (2005).

[59] Jewkes and Andrews (2005).

[60] Jewkes and Andrews (2005).

[61] Taylor and Quayle (2003).

[62] Wellard (2001)[Full Text] .

[63] Wolak et al. (2003).

[64] Canadian Resource Centre for Victims of Crime (2000)[Full Text] .

[65] Stewart (1997).

[66] Thornburgh and Lin (2002); Lee, Hui, and Fong (2003).

[67] Wang et al. (1998).

[68] Klain, Davies, and Hicks (2001)[Full Text] ; Canadian Resource Centre for Victims of Crime (2000)[Full Text] .

[69] Stanley (2001)[Full Text] .

[70] Ferraro et al. (2004); Kreston (2004).

[71] Canadian Resource Centre for Victims of Crime (2000)[Full Text] .

[72] Carr (2004)[Full Text] .

[73] Mostyn (2000).

[74] Graham (2000)[Full Text] .

[75] Taylor and Quayle (2006) [Abstract Only].

[76] Anonymous (2003); Sutton and Jones (2004)[Full Text] .

[77] Adegoke (2003).

[78] Ferraro et al. (2004).

[79] Lee, Hui, and Fong (2003).

[80] Arnaldo (2000).

[81] Aftab (2001); Lee, Hui, and Fong (2003); Thornburgh and Lin (2002); Wang et al. (1998).

[82] U.S. Department of Justice (2004)[Full Text] .

[83] Avarda, Colorado Police Department (1996)[Full Text] ; Lesce (1999)[Full Text] .

[84] Duff-Brown (2005)

[85] BBC News (13 February 2001); BBC News (11 November 2002); BBC News (18 December 2003).

[86] DeMarco (2005).

[87] Jenkins (2001).

[88] Lesce (1999)[Full Text] .

[89] Simon (2000).

[90] Grant, David, and Grabosky (1997); Jenkins (2001).

[91] Arnaldo (2001).

[92] Calder (2004); Ferraro et al. (2004); Shelley, Cashman, and Vermaat (2004).

[93] Calder (2004); Ferraro et al. (2004); Shelley, Cashman, and Vermaat (2004).

[94] Blundell et al. (2002); Calder (2004); Ferraro et al. (2004); Jenkins (2001); Thornburgh and Lin (2002).

[95] U.S. General Accounting Office (2002)[Full Text] ; Klain, Davies, and Hicks (2001)[Full Text] .

[96] BBC News (11 November 2002); Jewkes and Andrews (2005); U.S. Postal Inspection Service (n.d.)[Full Text] .

[97] BBC News (13 February 2001); Graham (2000)[Full Text] .

[98] Federal Bureau of Investigation (March 18 2002)[Full Text] .

[99] BBC News (18 December 2003).

References

Adegoke, Y. (2003). “Top Brands Start to Pull Ads From P2P Networks. New Media Age, April 24, p. 1.

Adler, A. (2001). “The Perverse Law of Child Pornography.” Columbia Law Review 101(2):209–273.

Aftab, P. (2000). The Parent’s Guide to Protecting Your Children in Cyberspace. New York: McGraw-Hill.

Aloysius, C. (2001). “The Media Response: A Journalist’s View of the Problem in Asia.” In C.A. Arnaldo, ed., Child Abuse on the Internet: Ending the Silence. New York: Berghahn Books.

Anonymous (2003). “Buried by a Pile of Porn: Child Pornography.” The Economist (U.S.), Jan. 18, 2003, Vol. 366, Issue 8307.

Arnaldo, C. (2002). “The Naked, Hairy Caveman: Child Abuse on the Internet.” In C. von Feilitzen and U. Carlsson, eds., Children in the New Media Landscape. Goteberg, Sweden: UNESCO International Clearinghouse on Children and Violence on the Screen at Nordicom.

Arnaldo, C. (2001). Child Abuse on the Internet: Ending the Silence. Paris: UNESCO Publishing; New York: Berghahn Books.

Arvada (Colorado) Police Department (1996). “Arvada Police Department Crimes Against Children Unit.” Submission for the Herman Goldstein Award for Excellence in Problem-Oriented Policing.[Full Text]

BBC News, “Tackling Online Child Pornography.” news.bbc.co.uk/1/hi/uk/1166135.stm (Accessed February 13, 2001).

BBC News, “Operation Avalanche: Tracking Child Porn.” news.bbc.co.uk/2/hi/uk_news/2445065.stm (Accessed November 11, 2002).

BBC News, “Police Trap Online Paedophiles.” news.bbc.co.uk/1/hi/uk/3329567.stm (Accessed December 18, 2003).

Blundell, B., M. Sherry, A. Burke, and S. Sowerbutts (2002). “Child Pornography and the Internet: Accessibility and Policing.” Australian Police Journal 56(1):59–65.

Burke, A., S. Sowerbutts, B. Blundell, and M. Sherry (2002). “Child Pornography and the Internet: Policing and Treatment Issues.” Psychiatry, Psychology and Law 9(1):79–4.

Calder, M. (2004). Child Sexual Abuse and the Internet: Tackling the New Frontier. Lyme Regis (United Kingdom): Russell House Publishing.

Canadian Resource Centre for Victims of Crime (2000). “Child Sexual Exploitation and the Internet.” Ottawa (Ontario). the Author.[Full Text]

Carr, J. (2004). Child Abuse, Child Pornography and the Internet. London: NCH.[Full Text]

Cooper, A., D.E. Putnam, L.A. Planchon, and S.C. Boies. (1999). “Online Sexual Compulsivity: Getting Tangled in the Net.” Sexual Addiction and Compulsivity 6:79–104.

Crewdson, J. (1998). By Silence Betrayed: Sexual Abuse of Children in America. Boston: Little Brown.

DeMarco, R.T. (2005). “Technology and the Fight Against Child Pornography. Watch Right.” blog.watchright.com/ ?itemid=337.

Dobson, A. (2003). “Caught in the Net.” Care and Health, Feb. 13 pp. 6–9.

Donnerstein, E. (2002). “The Internet.” In V.C. Strasburger and B.J. Wilson, eds., Children, Adolescents and the Media. Thousand Oaks (California): Sage Publications.

Duff-Brown, B. (2005). “Software Helps Track Child Pornographers.” Associated Press.

Esposito, L. (1998). “Regulating the Internet: The New Battle Against Child Pornography.” Case Western Reserve Journal of International Law 30:541–565.

Federal Bureau of Investigation (2002). “Operation Candyman.” [Full Text]

Ferraro, M., E. Casey, and M. McGrath (2004). Investigating Child Exploitation and Pornography: The Internet, The Law and Forensic Science. Amsterdam, Boston: Elsevier/Academic.

Finkelhor, D., K.J. Mitchell, and J. Wolak (2000). Online Victimization: A Report on the Nation’s Youth. Crimes Against Youth Research Center. [Full Text]

Forde, P., and A. Patterson (1998). Paedophile Internet Activity. Trends & Issues in Crime and Criminal Justice, No. 97. Canberra: Australian Institute of Criminology.[Full Text]

Goldstein, S. (1999). The Sexual Exploitation of Children: A Practical Guide to Assessment, Investigation, and Intervention. (2nd ed.). Boca Raton (Florida): CRC Press.

Graham, W., Jr. (2000). “Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement’s Access to ‘Wonderland’.” The Law Review of Michigan State University-Detroit College of Law 2:457–484.[Full Text]

Grant, A., F. David, and P. Grabosky (1997). “Child Pornography in the Digital Age.” Transnational Organized Crime 3(4):171–188.

Grasz, L., and P. Pfaltzgraff (1998). “Child Pornography and Child Nudity: Why and How States May Constitutionally Regulate the Production, Possession, and Distribution of Nude Visual Depictions of Children.” Temple Law Review 71:609–636.[Full Text]

Jenkins, P. (2001). Beyond Tolerance: Child Pornography on the Internet. New York: New York University Press.

Jewkes, Y., and C. Andrews (2005). “Policing the Filth: The Problems of Investigating Online Child Pornography in England and Wales.” Policing and Society 15: 42–62.

Kennedy-Souza, B.L. (1998). “Internet Addiction Order.” Interpersonal Computing and Technology 6:1–2.

Khan, K. (2000). “Child Pornography on the Internet.” Police Journal 73(1):7–17.[Full Text]

Klain, E., H. Davies and M. Hicks (2001). Child Pornography: The Criminal-Justice-System Response. Washington, D.C.: National Center for Missing & Exploited Children. [Full Text]

Kreston, S.S. (2004). “Computer Search and Seizure Issues in Internet Crimes Against Children Cases.” Rutgers Computer and Technology Law Journal 30:327–373.

Krone, T. (2004). A Typology of Online Child Pornography Offending. Trends & Issues in Crime and Criminal Justice, No. 279. Canberra: Australian Institute of Criminology. [Full Text]

Lanning, K., and A. Burgess (1989). “Child Pornography and Sex Rings.” In D. Zillmann and J. Bryant, eds., Pornography: Research Advances & Policy Considerations. Hillsdale (New Jersey): Lawrence Erlbaum.

Lee, P., S. Hui, and A. Fong (2003). “A Structural and Content-Based Analysis for Web Filtering.” Internet Research: Electronic Networking Applications and Policy 13(1):27–37.

Lesce, T. (1999). “Pedophiles on the Internet: Law Enforcement Investigates Abuse.” Law and Order 47(5):74–78.[Full Text]

Linz, D., and D. Imrich (2001). “Child Pornography.” In S. White, ed., Handbook of Youth and Justice. New York: Kluwer Academic/Plenum.

Marshall, W.L. (1988). “The Use of Explicit Sexual Stimuli by Rapists, Child Molesters and Nonoffender Males.” Journal of Sex Research 25:267–288.

Marshall, W.L. (2000). “Revisiting the Use of Pornography by Sexual Offenders: Implications for Theory and Practice.” The Journal of Sexual Aggression 6:67–77.

Mostyn, M. (2000). “The Need for Regulating Anonymous Remailers.” International Review of Law, Computers & Technology 14(1):79–88.

Newman, G.R. (2004). “Identity Theft.” Problem Oriented Guides for Police. Problem-Specific Guide Series, No. 25. U.S. Department of Justice Office of Community Oriented Policing Services. www.cops.usdoj.gov/mime/open. pdf?Item=1271.

O’Connell, R. (2001). “Pedophiles Networking on the Internet.” In C. Arnaldo, ed., Child Abuse on the Internet: Ending the Silence. New York: Berghahn Books.

Proulx, J., C. Perreult, and M. Ouimet (1999). “Pathways in the Offending Process of Extrafamilial Sexual Child Molesters.” Sexual Abuse: A Journal of Research and Treatment 11:117–29.

Quayle, E., and M. Taylor (2001). “Child Seduction and Self-Representation on the Internet.” CyberPsychology & Behavior 4(5):597–608.

Schneider, J.P. (2000). “Effects of Cybersex Addiction on the Family: Results of a Survey.” In A. Cooper, ed., Cybersex: The Dark Side of the Force. New York: Brunner/Mazel.

Schwartz, M.F., and S. Southern (2000). “Compulsive Cybersex.” In A. Cooper, ed., Cybersex: The Dark Side of the Force. New York: Brunner/Mazel.

Shelley, G.B., T.J. Cashman, and M.E. Vermaat (2004). Discovering Computers: A Gateway to Information. Boston: Thomson.

Silbert, M. (1989). “The Effects on Juveniles of Being Used for Pornography and Prostitution.” In D. Zillmann and J. Bryant, eds., Pornography: Research Advances & Policy Considerations. Hillsdale (New Jersey): Lawrence Erlbaum.

Simon, L. (2000). “An Examination of the Assumptions of Specialization, Mental Disorder, and Dangerousness in Sex Offenders.” Behavioral Sciences and the Law 18:275–308.

Smallbone, S., and R. Wortley (2000). Child Sexual Abuse in Queensland: Offender Characteristics and Modus Operandi. Brisbane: Queensland Crime Commission. [Full Text]

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

Stewart, J. (1997). “If This Is the Global Community, We Must Be On the Bad Side of Town: International Policing of Child Pornography on the Internet.” Houston Journal of International Law 20(1):205–246.

Sutton, D., and V. Jones (2004). Position Paper on Child Pornography and Internet-Related Sexual Exploitation of Children. Save the Children.[Full Text]

Tate, T. (1990). Child Pornography: An Investigation. London: Methuen.

Taylor, M., G. Holland, and E. Quayle (2001). “Typology of Paedophile Picture Collections.” Police Journal 74(2):97–107.[Full Text]

Taylor, M., and E. Quayle. (2006). “The Internet and Abuse Images of Children: Search, Precriminal Situations and Opportunity.” In R. Wortley and S. Smallbone (eds.) Situational Prevention of Child Sexual Abuse. Crime Prevention Studies, Vol. 19. Monsey (New York): Criminal Justice Press.[Abstract Only]

Taylor, M., and E. Quayle (2003). Child Pornography: An Internet Crime. London: Brunner-Routledge.

Thomas, D.S. (1997). “Cyberspace Pornography: Problems with Enforcement.” Internet Research: Electronic Networking Applications and Policy 7(3):201–207.

Thornburgh, D., and H. Lin (2002). Youth, Pornography, and the Internet. Washington, D.C.: National Academy Press.

Tyler, R. (1985). “Child Pornography: Perpetuating the Sexual Victimization of Children.” Child Abuse & Neglect 9(3):313–318.

U.S. Department of Justice (2004). Department of Justice, Homeland Security Announce Child Pornography File-Sharing Crackdown: Law Enforcement Initiative Targets Child Pornography Over Peer-to-Peer Networks. [Full Text]

U.S. General Accounting Office (2002). Combating Child Pornography: Federal Agencies Coordinate Law Enforcement Efforts, But An Opportunity Exists for Further Enhancement. Washington, D.C.: the Author. [Full Text]

U.S. General Accounting Office (2003). File-sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography. Washington, D.C.: the Author. [Full Text]

U.S. Postal Inspection Service, (n.d.). Operation Avalanche. [Full Text]

Wang, J., J. Li, G. Wiederhold, and O. Firschein (1998). “System for Screening Objectionable Images.” Computer Communications 21:1355–1360.

Wellard, S.S. (2001). “Cause and Effect.” Community Care March 15–21, pp. 26–27.[Full Text]

Williams, K. (2003). “Controlling Internet Child Pornography and Protecting the Child.” Information & Communications Technology Law 12(1):3–24.

Wolak, J., K. Mitchell, and D. Finkelhor (2003). “Escaping or Connecting? Characteristics of Youth Who Form Close Online Relationships.” Journal of Adolescence 26:105–119.

Related POP Projects

Important!

The quality and focus of these submissions vary considerably. With the exception of those submissions selected as winners or finalists, these documents are unedited and are reproduced in the condition in which they were submitted. They may nevertheless contain useful information or may report innovative projects.

Crimes Against Children Unit , Arvada Police Department (Arvada, CO, US), 1996