U.S. Department of Justice
Office of Justice Programs
Office of Juvenile Justice and Delinquency Prevention

Use of Computers in the Sexual Exploitation of Children

Portable Guides to Investigating Child Abuse

Foreword

Like the real world, the "virtual world" of cyberspace poses serious risks to children. Unfortunately, while we advise our children not to talk to strangers at the playground, we may fail to adequately educate them about the dangers of online exchanges with strangers.

These dangers are real. As a result of the anonymity and validation it affords sex offenders, the Internet has become a cyberplayground for those who prey on children. With the evolving nature of computer technology and the legal issues surrounding its use, the investigation of child sexual exploitation involving computers poses significant challenges to law enforcement.

Use of Computers in the Sexual Exploitation of Children is designed to help investigators meet those challenges. This Portable Guide offers basic information about adapting time-tested investigative techniques to the realm of cyberspace, discusses legal issues triggered by electronic communication investigations, and describes the behavioral characteristics of sex offenders who focus on children.

Developing this knowledge about the latest technologies employed by child sexual predators can help law enforcement officials hold them responsible for their crimes and protect other children from being victimized. Anything less is unacceptable.

Shay Bilchik
Administrator
Office of Juvenile Justice and
Delinquency Prevention

June 1999

NCJ 170021

Overview

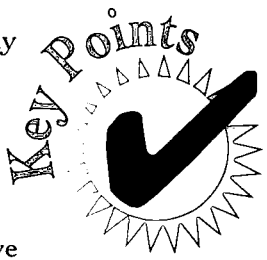
As more and more people discover the ability to communicate faster and more efficiently through computers and the Internet, the possibility that computers will be used to advance criminal activity also increases. Traditionally, online services have been oriented toward adults, but an increasing number of children are logging on to commercial services, private bulletin boards, and the Internet through schools and in their homes. This increased access to computer technology puts children at greater risk of sexual exploitation. While the vast majority of computer users rely on their computers for legitimate purposes, criminals involved in the sexual exploitation of children use the computer as a convenient tool to enter the homes of their victims, correspond with one another, and exchange depictions of illicit activities with child victims.

As used in this guide, the term "child sexual exploitation" refers to forms of sexual victimization of children involving pornography, sex rings, or prostitution. Apart from the legally defined crime of prostitution, child sexual exploitation does not necessarily involve commercial or monetary gain. In fact, in the United States, child pornography and child sex rings usually do not involve financial profit. Cases of child sexual exploitation may involve members of the child's own family (intrafamilial offenders), although this is not typical.

Given the rapid changes in computer technology and the complexity of the legal issues surrounding it, even the most basic investigation of child sexual exploitation involving computers can be a massive undertaking that requires numerous investigators with different areas of expertise. It is wise to identify experts and resources available to assist in computer-related cases. To ensure that your actions are within the law, stay in contact with the prosecutor working on your case at all times. **Mishandling of computer equipment or improper investigative techniques that result in a violation of a defendant's rights can result in the loss of valuable evidence.** Once that information is lost, it may be irretrievable.

Exploitation cases involving computers present many investigative challenges, but they also present the opportunity to obtain a great deal of corroborative evidence and investigative intelligence. The investigation of child sexual exploitation cases involving computers requires knowledge of the behavioral, technical, and legal aspects of computer use. The first section of this guide focuses primarily on the dynamics of offender behavior in the use of computers. The second section offers investigative guidelines based on this information. The final section covers the legal considerations all investigators must know when searching and seizing computer systems.

Understanding Offender Behavior in Relation to Computers



Preferential sex offenders engage in highly predictable sexual behavior patterns. The ability to recognize and use these patterns is critical to investigations of child sexual exploitation. The term "preferential sex offender" is a descriptive label used only to identify, for investigative purposes, a certain type of offender. To avoid possible confusion with a mental health diagnosis and potential challenges in court, use of the term "pedophile" should be kept to a minimum.

Although a variety of individuals sexually victimize children, preferential sex offenders are the primary sexual exploiters of

children. Using a computer to validate behavior, to facilitate interaction with child victims, or to traffic in child pornography usually requires the above-average intelligence and economic means typical of preferential sex offenders. Such offenders also tend to be predatory, serial offenders.*

Recognizing Preferential Sex Offenders

Knowing the kind of offender you are dealing with can go a long way toward determining the most effective investigative strategy. This knowledge can influence interview approaches and facilitate discovery of corroborative evidence. It can be useful in determining the existence and location of other victims or child pornography or erotica. A preferential sex offender can usually be identified by the following interrelated behaviors:

- **Long-term and persistent patterns of behavior.** The individual begins the pattern in early adolescence; is willing to commit time, money, and energy; commits multiple offenses; and makes ritual or need-driven mistakes.
- **Specific sexual interests.** The individual manifests paraphiliac preferences, possibly more than one type. (Paraphilias are recurrent, intense sexually arousing fantasies, sexual urges, or behaviors that generally involve (1) nonhuman objects, (2) the suffering or humiliation of oneself or one's partner, or (3) children or other nonconsenting persons, and that occur for a period of at least 6 months.)[1] There is a focus on defined sexual interests and victim characteristics. These individuals rationalize their sexual interests and center their lives around their preferences.
- **Well-developed techniques.** The individual evaluates experiences; lies and manipulates, often skillfully; has methods of access to victims; and is quick to use modern technology (e.g., computer, VCR) for sexual needs and purposes.
- **Fantasy-driven behavior.** The individual collects pornography, paraphernalia, souvenirs, and videotapes; records fantasies; and acts to turn fantasy into reality.

Because these sexual behavior patterns are highly predictable, investigators must recognize and use them when they are present. If the investigation identifies enough of these

---

*Note: For a more extensive discussion of preferential sex offenders, see the 11th guide in this series, *Understanding and Investigating Child Sexual Exploitation*. The category of predatory serial sex offenders includes other types of offenders, such as those who use intimidation and force to engage in sexually motivated child abduction. A discussion of these other types of offenders is beyond the scope of this guide.

characteristics, many of the remaining ones can be assumed. However, no particular number constitutes "enough"—just a few characteristics may be "enough" if they are especially significant. Most of these indicators mean little by themselves, but as they are identified and accumulated through investigation, they can constitute reason to believe a suspect is a preferential sex offender.

How Offenders Use Computers

When you understand sex offenders, especially the preferential sex offender, the great appeal of a computer becomes obvious. The computer—whether a stand-alone system or one using online service capability, whether at work or, more likely, a personal computer at home—provides the preferential sex offender with an ideal means of filling his needs for validation, organization, finding potential new victims, and trafficking in child pornography. In this case, modern technology has caught up with long-known personality traits. Anonymous communication with people of similar criminal interests and a seemingly safe method of identifying and communicating with potential victims is a powerful attraction for the preferential sex offender.

Validation

Communicating with other people who have similar interests validates the offender's interests and behavior. This is actually the most important and compelling reason that preferential sex offenders are drawn to the online computer. Now, in addition to physical contact and putting a stamp on a letter or package, they can use their computers to exchange information and validation.

Through the Internet, national and regional online services, or specialized electronic bulletin boards, offenders can use their computers to locate individuals with similar interests. The great appeal of this type of communication is perceived anonymity and immediate feedback. The computer enables them to obtain active validation from other users with less risk of identification or discovery. Like advertisements in "swinger" magazines, computer online services are used to identify individuals of mutual interest concerning age, gender, and sexual preference. The offender may use an electronic bulletin board to which he has authorized access, or he may illegally enter a system. The

offender can also set up his own online bulletin board or participate in surreptitious or underground ones.

Organization

Offenders use computers to organize their collections and correspondence. Many preferential sexual offenders seem to be compulsive recordkeepers. A computer makes it much easier to store and retrieve names and addresses of victims and of individuals with similar interests. Innumerable characteristics of victims and sexual acts can be easily recorded and analyzed. An extensive pornography collection can be cataloged by subject matter. Even fantasy writings and other narrative descriptions can be stored and retrieved for future use.

One problem the computer creates for law enforcement is determining whether texts describing sexual assaults are fictional stories, sexual fantasies, diaries of past activity, plans for future activity, or current threats. This problem can be compounded by the fact that some individuals believe cyberspace is a new frontier where the old rules of society do not apply. There is no easy solution to this problem. Painstaking analysis and investigation are essential tools in working toward a solution.

Maintenance of Financial Records. Offenders who have turned their child pornography into a profit-making business use computers the same way any business uses them. Such things as customer lists, dollar amounts of transactions, and descriptions of inventory can all be recorded on the computer. Because trafficking in child pornography by computer lowers the risks, it may also increase profit-motivated distribution.

Finding victims

Offenders can use the computer to troll for and communicate with potential victims with minimal risk of being identified. The use of a vast, loose-knit network like the Internet can make identifying the actual perpetrator difficult. On the computer, the offender can assume any identity or characteristics he wants or needs. Adolescent boys who spend many hours "hacking" on their computers are at particularly high risk of such contacts. The child can be indirectly "victimized" through conversation ("chat") and the transfer of sexually explicit information and material, or he can be evaluated for future face-to-face contact and direct victimization. The latest technology even allows

real-time group participation in child exploitation through digital teleconferencing by computer.

Investigators must recognize that children who have been lured from their homes after online computer conversations were not simply duped while doing homework. Most are curious, rebellious, or troubled adolescents seeking sexual information or contact. Nevertheless, they have been seduced and manipulated by a clever offender who has taken advantage of their vulnerabilities, and they do not fully understand or recognize the risks involved.

Child pornography

As a result of computer online services, child pornography is now more readily available in the United States than it has been since the late 1970's. An offender can use a computer to transfer, manipulate, and even create child pornography. With a typical home computer and modem, still images can easily be digitally stored, transferred from print or videotape, and transmitted, with the quality of each copy as good as the original. Visual images can be stored on hard drives, floppy disks, CD–ROM's, or DVD's. Both information and images can be encrypted for storage or transmission to deter detection.

With newer technology, faster modems, digital cameras, and better computers, similar things can now be done with some moving images. Two other modern inventions invaluable to pornographers, the video camera and recorder, are now being paired with the computer. Multimedia images, with some motion and sound, and virtual reality programs provide an added dimension to pornography. However, it is still difficult—for now—to transmit child pornography over the Internet in the format most preferred by offenders—high-quality, lengthy moving images (e.g., videotape, films).

Some of these uses are now small problems that may eventually become big problems. Computer software and hardware are being developed so rapidly that their potential for abuse is almost unlimited. In the near future, most communication systems in a home (e.g., telephone, television, fax, videotape, music, newspapers, financial records) may be funneled through a computer. With computer graphics programs, images can be easily changed, or "morphed." The ability to manipulate digital visual images may make it difficult

to believe your own eyes. A recent television commercial makes it appear that John Wayne is talking to a drill sergeant. Halfway through the movie "Forrest Gump," Lt. Dan's legs are no longer visible. This is the same technology used to "age" photographs of long-missing children.

Computer-manipulated and, soon, computer-generated, visual images of "children" engaging in sexually explicit conduct may call into question the basis for highly restrictive child pornography laws (i.e., possession, advertising). Under the recently passed Child Pornography Prevention Act of 1996,[2] the Federal definition of child pornography has been expanded to include any visual depiction that "has been created, adapted, or modified to **appear** [emphasis added] that an identifiable minor is engaging in sexually explicit conduct." Although this new law makes the prosecution of cases involving manipulated computer images easier, it also means that it is no longer possible in every case to argue that child pornography is the permanent record of the abuse or exploitation of an actual child if no real child is involved. If the new law is found unconstitutional, only existing obscenity laws may apply to such simulated child pornography.

Types of Computer Offenders

Those who use computers to traffic in child pornography usually fall into two broad categories:

- **Dabbler.** Usually a typical adolescent searching for pornography, a curious adult with a newly found access to pornography, or a profit-motivated criminal. Dabblers can be investigated and prosecuted, but their behavior tends not to be as long-term, persistent, or predictable as that of a preferential offender.
- **Preferential offender.** Usually a sexually indiscriminate individual with a wide variety of deviant sexual interests or a pedophile with a definite preference for children. The main difference between these individuals is that the collection of the sexually indiscriminate preferential offender will be more varied, usually with a focus on the offender's particular sexual preferences or paraphilias, whereas a pedophile's collection will focus primarily on children. Also, the sexually indiscriminate offender is less likely to molest children, especially prepubescent children. With either of the preferential types, the characteristics and dynamics previously discussed concerning preferential sex offenders should be considered.

Other miscellaneous "offenders" include media reporters who erroneously believe they can traffic in child pornography as part of a news exposé, pranksters who disseminate false or incriminating information to embarrass the targets of their

"dirty tricks," and concerned citizens who, either on their own or at the suggestion of law enforcement, conduct their own investigations into this problem. Investigators must be cautious of overzealous citizens who offer their services in these cases.

When trying to determine whether an offender using a computer to traffic in child pornography is a dabbler or a preferential offender, evaluate all available background information. The following information about online computer activity can be valuable in making this assessment. This information can often be obtained from the online service provider and through undercover communication, pretext contacts (investigators posing as children online), informants, and other investigative techniques:

- Screen name.
- Screen profile.
- Accuracy of profile.
- Length of time active.
- Amount of time spent online.
- Number of files.
- Number of transmissions.
- Number of files originated, forwarded, or received.
- Number of recipients.
- Theme of messages and chat.
- Theme of pornography.

Investigators must not overreact to reported allegations, but neither should they fail to react appropriately. Remember that not all offenders are stereotypical "pedophiles" who fit some common profile. Keeping an open mind and objectively attempting to determine the type of offender involved will help you to avoid embarrassing errors in judgment and to develop appropriate interview, investigation, and prosecution strategies. For example, knowing that preferential offenders are more likely to commit multiple offenses, make need-driven mistakes, and compulsively collect pornography and other offense-related paraphernalia can be used to build a stronger case. Investigators must be alert to the fact that any offender with intelligence, economic means, or employment access may be using a computer in any or all of the above ways, but preferential sex offenders are highly likely to do so.

Investigative Guidelines

The investigation of the use of computers in child sexual exploitation is complex and may exceed the resources available to your jurisdiction. When initiating an investigation, you should take the following issues into consideration:

- **Jurisdiction.** *Will your investigation remain local or extend to Federal or State jurisdiction?* Often you will not know this until the computer system has been seized and analyzed. In most cases, computer exploitation investigations will rise to the Federal or interstate level. You must recognize this possibility at the earliest moment in order to prepare for the future involvement of all agencies as soon as possible. This will ensure the continuity of the investigation.

- **Expertise.** *Does your organization have the technical expertise to deal with this investigation?* Expertise means understanding not only the child predator but computer and software technology also. If you do not have this knowledge, look to other agencies at the Federal, State, or local level for help. The private computer industry may also be able to assist you. (See glossary for definitions of basic computer terms.)

- **Equipment.** *Does your organization have the equipment needed or the resources to obtain the necessary equipment to conduct this investigation?* If not, decisions must be made to purchase, lease, or borrow the necessary equipment from other agencies. Forensic computer examinations, depending on the sophistication of the equipment seized for evidence, may require significant resources beyond the capacity of your agency. The decision may be affected by what evidence the prosecuting attorney decides is needed and how it should be presented to the court. Early contact with the prosecuting attorney can save time and significant expense.

- **Time/Personnel.** *Does your organization have the time and personnel to devote to this type of investigation? Is it willing to do so?* Again, seeking assistance from other agencies or forming a task force must be considered. You must advise your command staff of this need and determine if they are willing to make the commitment.

- **Followup.** *Can your organization perform the necessary followup on additional suspects and victims that may arise from the investigation?* Most of these investigations will uncover more suspects and more victims—often a significant number of both. Multiple jurisdictions are often involved. Plans for dealing with such complications and for properly collecting and packaging the evidence need to be formulated before proceeding with the investigation.

Once you have answered these questions, consider the following guidelines as a basis on which to proceed with your investigation. The guidelines describe what to do and what not to do when investigating child exploitation using computer systems.

Establishing the Context

- Establish that a child sexual exploitation situation exists. To determine the type of offender you are dealing with, you must

Glossary of Computer Terms

CD–ROM: Compact disk read-only memory. A CD–ROM is a compact disk containing data that can be read by a computer. Unlike data on hard drives and diskettes, data on CD–ROM's can only be read, not altered by the user.

Computer bulletin board: See "electronic bulletin board system" (BBS).

CPU: Central processing unit; the part of a computer that controls all the other parts.

Crackers: "Hackers with malice" who want to do more than explore other computers. Crackers often attempt to plunder or pillage information.

Digital teleconferencing: Real-time, interactive conferences or meetings using sight and sound that are conducted among participants in different locations through digital means (i.e., desktop computers).

DVD: Digital video disk.

Electronic bulletin board system (BBS): Central system, accessed via modem and phone lines, where information is posted for dissemination. A BBS can have many telephone lines or one line, so the number of access points to the BBS at any given moment is dictated by the system operator, who may be an individual, a business, or an organization. A BBS may have several levels of access, often referred to as "subboards" or "conferences." Access to the various conferences is by password, which is controlled by the operator. Photographs, documents, messages, and data of various kinds may be stored at the different levels of the BBS.

A BBS functions as a meeting place in electronic cyberspace. The material presented is usually theme-oriented, offering information on specific issues or interests. Most BBS's that feature "adult"-oriented material attempt to limit minors from accessing such information, with varying success. BBS's are the destination of choice for interactive discussions with like-minded sex offenders and children.

E-Mail: Electronic mail; written correspondence between two or more online users through online servers or over the Internet.

Hacking: Activities engaged in by those who are usually quite inventive and talented in the use of computers. This may include breaking into computers.

Hard disk drive: Storage device based on a fixed, permanently mounted disk drive. It may be either internal (part of the computer itself) or external (a separate but connected component). Both applications and data may be stored on the disk.

Glossary of Computer Terms *(continued)*

Hot button: Keyboard buttons preprogrammed to open a particular file in a sequential manner that, if not executed in a predetermined sequence, destroys all electronic evidence in the file.

Input/Output (I/O) device: Equipment that sends data to or receives data from a computer. Keyboards, monitors, and printers are all common I/O devices.

Internet: Global "network of networks," not governed by any entity, with no limits or checks on the kind of information maintained by and accessible to its users. The Internet is the gateway to unmonitored communication among sex offenders of all types.

Kill command: Command automatically sent to destroy all electronic evidence within a file if an attempt is made to open the file improperly.

Modem: Device that allows one computer to communicate with another computer, normally over standard telephone lines. It converts the digital signal of the computer to the analog signal for outgoing telephone transmission and reverses the conversion for incoming messages.

Mouse: Pointing device that controls input by moving a cursor or other figure on the screen. Normally, the user points to an object on the screen and then presses a button on the mouse to indicate a selection.

Network: System of interconnected computer systems and terminals.

Online services: Commercial, self-regulated businesses that provide access to the Internet. Online services may screen or provide editorial/user controls, when possible, of the material contained in their systems.

Password: Any combination of letters and/or numbers, linked to the screen name, that provides access to online services.

Real time: Simultaneous; at the same time.

Scanner: Optical device that can recognize characters on paper and, using specialized software, convert them into digital form.

Screen name: Identification required by every online service. Each user must have at least one screen name; some services allow up to five. The names are exclusive to the user—no duplication is allowed.

Software: Programs or instructions that tell a computer what to do.

have the most complete, detailed, and accurate information possible. Your background investigation of the suspect should obtain more than the date and place of birth, credit history, and criminal background checks. School, juvenile, military, medical, driving, employment, bank, sex offender, and child abuse registry records can be valuable sources of information.

- Establish that the suspect owns or has access to a computer and uses it for child sexual exploitation. This can be done by asking specific questions related to the use of the computers of which the suspect(s), victim(s), witnesses, or others may have firsthand or circumstantial knowledge.

- Establish probable cause to show that the suspect used his computer for the crime. Again, appropriate interview questions should be used. Search warrants and searches of public information sources can also yield important information.

Obtaining a Search Warrant

- If enough probable cause exists, a warrant or subpoena can be obtained to serve on telephone companies for telephone records and online services for screen names, account information, and e-mail. Most online services require that the account be paid with a credit card and will not accept post office boxes as mailing addresses.

- If sufficient probable cause exists, obtain a search warrant for the suspect's computer system.

- In preparing the search warrant, be sure to include all the computer hardware and software, keeping in mind the independent component doctrine, discussed below. The entire system is necessary to replicate the suspect's use of it and to enable you to analyze it.

- In your search warrant, list accounting records to identify payment to online services currently in use and those used in the past. Keep in mind that these records may be located on the computer system. Remember that payment for services could be charged to credit card accounts. Such records should be seized to find these accounts.

- Once the system is transported to your agency, be aware that another warrant may be needed to search hard drives and software programs. It is a good idea to work closely with your prosecutors, as case law is forever changing in this area. Depending on the suspect, a "special master" (an attorney appointed by a judge to review privileged or confidential information in an investigation to determine its relevancy as admissible evidence) may be needed to do the searching for you. Also, if the system is used as part of the suspect's business, case law may limit your time and ability to search the system.

Handling Computer Equipment

- When executing a warrant for the suspect's computer system, make sure a computer expert is present. If your agency does not have this capability, try the private sector. Corporations are sometimes willing to assist in the actual handling of the equipment. Local offices of Federal agencies may also be able to aid with resources. **The rule to follow is, "If you don't know what to do, don't touch it."** Secure the system until you can find someone with the proper expertise to handle the equipment safely.

- While searching the suspect's residence and/or business, be sure to look for passwords for the system. Most suspects use passwords for better security. They can consist of any combination of letters and numbers. Some are as simple as the suspect's telephone number; others are more sophisticated. Some companies specialize in decoding passwords. Check with your nearest Federal Bureau of Investigation or U.S. Customs Service office for assistance in this area.

- Once the computer system is seized, try to keep it intact as much as possible. It is best to move the system as a whole, entirely connected together, if possible.

- If you need to disassemble the suspect's computer system, take pictures of the front and back to identify how the system is set up before you physically move it. Before beginning the computer analysis, you or the computer specialist can use the photographs to put the system back together exactly as it was used by the suspect.

Analyzing a Computer System

- The cleanest method of analyzing the suspect's computer system is to copy the data onto an exact duplicate of the suspect's hardware. Use the second system as the working system for your analysis. Then, if an error is made, the suspect's original system is not damaged, saving you from possible civil liability at a later time. Your agency's budget and expertise will dictate your course of action in this matter.

- With the proper software, erased files (e.g., text, graphics) can be recreated if they have not been written over with new data. Even though these files may not be visible on the system directory, they may still exist. Child sexual predators who use computers are aware of this and sometimes will erase files to keep them from being detected. An expert in this area is critical to your investigation.

- Depending on your prosecuting attorney, hard copies (i.e., paper printouts) of all the data on the system may be required. The data can be reviewed by child sexual exploitation experts to determine what is appropriate evidence.

Many of the problems that can arise during investigation of child sexual exploitation through computers can be eliminated or minimized if you follow these guidelines and act within the legal boundaries described below.

Legal Considerations in the Use of Search Warrants

This section discusses the legal principles governing the search and seizure of computer systems and provides guidance on how to avoid the pitfalls and trapdoors involved in searching and seizing computers as evidence of crimes against children. Search warrants are an invaluable investigative tool, and search warrants on computers are an integral part of a comprehensive investigative strategy. However, if you violate any of the doctrines, statutes, or principles set forth below, you and/or your employer may owe a great deal of money to the former defendant, now plaintiff, and your criminal case will disappear.

Expert Search Warrants

Behavioral characteristics may provide a basis for obtaining a warrant to search a suspect's residence, business, or computer system. An expert search warrant uses an expert's opinion to supplement case-specific, documented behaviors in which child predators repeatedly engage and applies this information to the targeted individual. Determining the type of offender in question is crucial to the use of these warrants. If the expert opinion is based on the subject's being a certain type of offender, the affidavit for the search warrant **must** set forth the probable cause for believing that the subject is that type. This technique can be used with any of the preferential sex offender types previously discussed.

As a result of legal uncertainties stemming from a lack of consistent court decisions on such warrants, expert search warrants in child sexual exploitation cases should be used only when absolutely necessary. Expert warrants should be considered, when they are needed, to provide additional probable cause, justify expanding the scope of the search, or address problems concerning the staleness of information.

Avoid the use of boilerplate or generic language in describing the behavioral traits of the target offender. Courts will suppress evidence gathered through expert search warrants if they are not factually specific and relevant to the target of the search and his behavior typology. You should develop evidence that supports a particular offender type to enable experts to assess the specific traits of the target. This evidence may be referenced in the affidavit of probable cause, which corroborates the expert opinion.

Exceptions to Search Warrant Requirements

Exigent circumstances exception

The general exceptions to the warrant requirement apply to computer systems. Exigent circumstances may justify a warrantless search under the appropriate factual circumstances. If a suspect's computer screen is displaying evidence that you reasonably believe is about to be destroyed, the doctrine of exigent circumstances permits you to download the information before obtaining a warrant. However, if you have sufficient time to procure a warrant and fail to do so, the evidence will probably be suppressed.

For the exception to apply, the specific facts of the case must cause a reasonable person to believe exigent circumstances exist. The concerns need not be correct as long as they are reasonable. Consider the following factors in determining whether exigent circumstances exist:

- The degree of urgency involved.
- The amount of time necessary to obtain a warrant.
- Whether evidence is about to be removed or destroyed.
- The possibility of danger at the site for police officers, citizens, and targets.
- Information indicating the possessors of the contraband know the police are on their trail.
- The destructibility of the contraband.[3]

While exigent circumstances may justify *seizing* a computer and/or component attachments, *searching* the computer may not be authorized without obtaining a warrant subsequent to the seizure. The authority to seize containers does not necessarily authorize a warrantless search of the containers' contents.[4] You

must be able to explain to the court why obtaining a search warrant before seizing the evidence would have jeopardized your ability to obtain the evidence at all.

The unique nature of electronic evidence and its susceptibility to humidity, temperature, magnetic fields, "hot buttons," and "kill commands" may destroy evidence instantaneously. Exigent circumstances may exist in searching computers simply because of the fragile character of such evidence.

Plain view exception

Evidence of a crime can also be seized without a warrant if the police officer is in a lawful position to observe the evidence and if its criminal character is immediately apparent. Therefore, if you observe child pornography on a suspect's computer screen, you may seize, without a warrant, not only the computer that contains the unlawful images but also access codes or notes taped to the computer that are in plain view.

Consent exception

Police officers may conduct a warrantless search, even without probable cause to search, if a person with appropriate authority consents to the search. This consent may be expressed ("Yes, you may search my computer") or implied ("Here is the password to the computer data"). The court determines the voluntary nature of the consent by looking at several factors:

- The age of the person giving consent.
- The person's educational level, intelligence, and mental and physical conditions.
- Whether the person had been advised of his right to withhold consent.[5]

In crimes involving computers, two issues related to consent emerge:

- Did law enforcement exceed the scope of consent given?
- Did the person giving consent have the proper authority to allow a search of a particular place or item?

Scope of Consent. Any person who consents to a search may expressly limit the search to a specified area. Law enforcement must respect the explicit limitations placed on the scope of the search. The scope of consent may also be limited by implication.

If a person attempts to prevent you from seeing a password to encrypted data, that act implicitly limits the scope of consent to data available without the use of the password. A person who consents to a search may withdraw that consent at any time during the search.

Multiple Users. If more than one person has access to a computer, you can usually rely on the consent of any person who has authority over the computer. In such circumstances, all persons using the computer are considered to have assumed the risk that a co-user could discover evidence of a crime or permit law enforcement to search the computer for evidence of criminal activity.[6]

The usual defense in multiple-user consent searches is that the other users had no authority to give law enforcement consent to search "my computer." Courts analyze such claims of exclusive authority by determining what, if any, special safeguards the defendant took to protect his or her data from the scrutiny of others. Creating a separate directory on the same computer may not provide the exclusivity necessary to prevent the consent search, but guarding the separate directory with a secret password may prohibit a warrantless search without the defendant's consent to search that particular directory.

The test to determine whether a person has the authority to consent is an objective one: Would the facts available to law enforcement at the time of consent cause a person of reasonable caution to believe that the consenting party had authority over the premises and, therefore, authority to grant consent to the search?

Border exception

Law enforcement may search people and property without a warrant or probable cause when the people or property cross the U.S. border or its "functional equivalent." Diskettes, tapes, computer hard drives, or other media can be searched *at the border* to determine whether they contain items prohibited from being brought into the country.

The border search exception originates in the Government's power to prohibit illegal items from entering the country. However, the rationale no longer exists once such illegal items (e.g., electronic child pornography) have entered the country.

Once the illegal contraband is in, law enforcement is bound by the constraints of the Constitution, applicable statutes, and case law in conducting a search for evidence of a crime.

Similarly, this exception to the warrant requirement probably would not apply to electronic data transmitted via the Internet, e-mail, or other nonphysical means from a foreign country to the United States. For example, if an individual living in the United States downloads child pornography from a foreign bulletin board service, a warrantless search of his computer probably would not be upheld under the border search exception.

Undercover Agents

Undercover agents may, without a warrant, infiltrate computer child pornography rings or bulletin board services that facilitate illegal activities involving the sexual exploitation of children. Varying levels of access are granted to such services: (1) open to the public, (2) open to paying members of organizations, or (3) open to trusted individuals with secret passwords.

Undercover agents must adhere scrupulously to the scope of an invitation to join the organization. They should operate only within the level the system operator has authorized and not "hack" into areas of the bulletin board service for which access has not been granted.[7]

No-Knock Warrant

Forcible entry without knocking and announcing may be permitted if people in the dwelling already know your authority and purpose or if you reasonably believe that giving notice to people in the dwelling could cause you or any other individual to be hurt, a suspect to flee, or evidence to be destroyed.

In cases involving computer crimes, destruction of evidence is of particular concern. Suspects knowledgeable in computer programming can destroy evidence of a crime in any number of ways. The nonphysical nature of such evidence often allows immediate destruction by suspects. Nevertheless, these facts in themselves are not sufficient to dispense with the knock-and-announce rule. The majority of jurisdictions require law

enforcement to articulate specifically why *these* premises and/or *these* people make it dangerous or unwise to knock and announce before a search ensues.

Special Considerations

Independent component doctrine

The assertion often heard in law enforcement circles is that "you must have probable cause to seize the computer." This statement begs the question—what is the computer? Probable cause to seize the "computer" does not necessarily mean authorization to seize the entire computer system, that is, the central processing unit (CPU) and all its peripherals.

Each component in the computer system should be considered independently from the others in analyzing probable cause to seize. It is wrong to assume that any item connected to the target device may automatically be seized. To protect the execution of the search warrant from serious challenge in court, seize only those items necessary for basic input and output functions (e.g., CPU, keyboard, monitor). (See glossary of terms for definitions of computer parts.)

When you need to search and seize devices in addition to the basic components, list only those devices for which you can articulate an independent basis. The independent component doctrine does not mean that connected items are exempt; it only requires that investigators and prosecutors articulate a reason for searching and/or seizing each targeted device. Determine what role each component might have played in the commission of the crime. That determination constitutes probable cause to seize the "computer."

Privileged and confidential communications

Search warrants to examine computer data that contain privileged communications must be written narrowly to include only data relevant to the investigation. Such data should be described as specifically as possible. Generic, boilerplate affidavits are insufficient and often result in successful suppression of the evidence by the defendant.

Doctors, lawyers, and clergy possess recognized confidential communication safeguards and are governed by special statutes regarding searches of such information. Before

executing search warrants for privileged or confidential communications, data, or documents from disinterested third parties (such as doctors, lawyers, or clergy), you should be thoroughly briefed by a knowledgeable prosecutor on the Privacy Protection Act of 1980 (PPA),[8] the accompanying regulations,[9] and all applicable State statutes. While the PPA provides safeguards for confidential relationships, it does not apply to criminal suspects. It also does not require showing anything greater than probable cause to secure a warrant for a search that may intrude on confidential relationships.[10]

Privacy Protection Act of 1980

Through the PPA, Congress has given protection to the press and others extending beyond that which is currently provided by the Fourth Amendment. It is unlawful for any government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize the following:

- Work product materials (e.g., private memos, interview notes, or mental impressions).
- Documentary materials (other than work product materials) possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication in or affecting interstate or foreign commerce.

Under the PPA, however, government officers or employees, in connection with the investigation or prosecution of a criminal offense, may search for or seize work product or documentary materials if:

- Probable cause exists to believe the person possessing such materials has committed or is committing a criminal offense, other than possession, to which the materials relate. It should be noted that possession of child pornography is not protected under the PPA.
- There is reason to believe that immediate seizure of such materials is necessary to *prevent the death of, or serious bodily injury to, a human being.*

In addition, government officials or employees may search for or seize documentary materials if service of a subpoena would result in destruction, alteration, or concealment of evidence, or a court order was not complied with and either appellate remedies are exhausted or delay would threaten the ends of justice.

For a valid claim to be made under the PPA, two conditions must exist:

- A search and seizure must have taken place.
- Intent to disseminate the information publicly must be shown.[11]

Victims of searches that violate the PPA may not move to suppress the evidence obtained. However, the statute does allow for civil remedies. The PPA also precludes the State from asserting a good faith defense (a defense based on honest belief, with the absence of malice or design to defraud or seek an unfair advantage) to civil claims. In this regard, the PPA is a strict liability statute.

Steve Jackson Games v. *United States*[12] is an important case to understand before conducting searches and seizures that may involve the PPA. (For guidelines on how to read case citations and legal opinions, see sidebar, "Using Legal Opinions.") Based on information that an employee was using company computers for illegal activities, Secret Service agents in that case executed a search warrant on the target company, Jackson Games, producer of books, magazines, and games for the public. Jackson Games immediately requested return of the seized materials, but the Secret Service retained most of the records for several months. No criminal charges were ever filed. Jackson Games filed a civil suit against the Secret Service and the United States under the PPA and the Electronic Communications Privacy Act (ECPA).[13] The court found that the Secret Service agents who seized the materials in question violated the PPA when they realized the materials were protected under the Act and failed to return them promptly. A substantial award resulted from the verdict.

Before searching computers or bulletin board services, carefully consider the restrictions of the PPA, along with its exceptions and exemptions. If your case involves the protections of the PPA or ECPA, consult legal experts about how to avoid liability for violations of these laws.[14]

Stored electronic communications

You should request direction and legal advice when seeking to obtain stored electronic communications. Under Federal and State constitutional protections against unreasonable search and seizure, Congress has provided supplemental

protections through the enactment of the ECPA. This statute encompasses, among other things, access to and search and seizure of stored electronic communications. Under the ECPA, anyone who provides an electronic communication service or remote computing services *to the public* is prohibited from voluntarily disclosing the contents of the electronic communications they store or maintain on the service.[15] For the statute to apply, the communication must be electronically stored on a system that affects interstate or foreign commerce. The ECPA protects only communications in electronic storage in the possession of the service provider. It does not protect communications downloaded by the addressee to another computer not maintained by a provider.

There are, however, exceptions to the ECPA's nondisclosure provisions:

- Persons or entities may disclose the contents of the communications with lawful consent from the originator of the communications, an addressee, or the intended recipient of such communications.
- They may disclose the contents if the communications were inadvertently discovered and appear to be related to the commission of a crime.
- If the communication has been stored longer than 180 days, prosecutors may, under rule 41 of the *Federal Rules of Criminal Procedure,* use a search warrant (which does not require notice to the subscriber) to seize communications on e-mail. Alternatively, prosecutors may use an administrative subpoena, grand jury subpoena, or court order (which all require notice to the subscriber). If the communications are in storage 180 days or less, disclosure to a governmental entity requires a warrant.[16]
- Law enforcement can compel disclosure from both types of providers by warrant or subpoena under the ECPA. The type of legal process required depends on the age of the communication as set forth above and the predisposition of law enforcement to inform the target customer about its request for electronic evidence stored in the target's computer.
- The ECPA provides law enforcement with the ability to request the service provider to preserve all records and other evidence in its possession relating to the target computer pending the issuance of a court order or other legal process. This period of retention is 90 days, with an option for an additional 90 days if law enforcement requests. Law enforcement may include in its subpoena or court order a requirement that the service provider create a backup of all contents of communications contained in the target's e-mail file. This may be done without notice to the customer/target under certain circumstances.

Drafting the Warrant

The focus of the warrant should be on the items to be seized. The warrant should be as specific as possible. You must be creative and informative in articulating to the magistrate what it is you want to seize and where you want to conduct your search.

It may be impossible to isolate the location of information. If you suspect data are at multiple sites, your magistrate must be informed that the search may require searching multiple sites. If multiple sites in different jurisdictions are involved, address this issue with the magistrate before the warrant is executed. There is some legal precedent in drug court opinions for a search conducted under a single warrant to authorize wiretaps in multiple jurisdictions.[17] It is preferable under present law to seek a search warrant from a court of competent jurisdiction in each separate site to be searched. The affidavit should explain why a specific address is not available, including the various attempts to find the address. You need to demonstrate the connection between the computer described in the warrant and an offsite storage computer.

Using Legal Opinions

In published opinions, Federal and State appellate and supreme courts interpret legal issues, decide legal disputes, and set precedent for future cases. Their findings are considered binding on lower courts when subsequent cases raise identical issues. An opinion, however, can only set a precedent with regard to the issues in dispute that were actually decided by the court. The published opinion will contain a statement of the facts, a statement of the legal issues disputed by the parties, a ruling or holding (an answer to the issues raised), and the court's reasoning or rationale for its decision. The ruling is most significant, although the court's rationale provides valuable information with which to compare or distinguish the issues in other cases.

Legal case citations such as "713 F. Supp. 1308 (D. Minn. 1989)" are read as follows: 713 (volume number), F. Supp. (reporting entity—in this example, the Federal Supplement), 1308 (page number in the particular reporter where the opinion begins), D. Minn. (name of court that decided the case—in this case, the U.S. District Court for the District of Minnesota), 1989 (year the opinion was published). When a case is unreported, pending, or available only on a database such as Westlaw or LEXIS, the citation form varies. For an opinion available only on an electronic database, for example, the citation will include the name of the database and any unique database numbers or identifiers.

The scope of the search of the target's computer should be determined by the nature of the criminal conduct. If probable cause exists to believe that the criminal conduct includes use of data, e-mail, and the computer, the warrant may be drafted in broader terms, because it is unnecessary to distinguish seizable and nonseizable items. Conversely, if probable cause exists only to seize the computer as a storage container of child pornography, your warrant must be narrow and specific to the container and the child pornography stored in it, distinguishing that evidence from other noncriminal electronic data.

Chain of Custody

Protecting the integrity of evidence seized in cases involving computers requires the same considerations as in other cases. The chain of custody (the custody of evidence from the moment it is seized until the moment it is offered in evidence) must be documented, and access to evidence must be strictly controlled to avoid challenges to the admission of evidence at trial. Essentially, the chain of custody must show that the item offered into evidence is the same item that was seized.

The preservation of evidence in electronic form as found at the scene of the crime is essential. This is true whether you process the raw data and add hearsay information (resulting in processed evidence, that is, evidence that provides a context for interpreting the raw evidence and its connection to the crime) or offer only the raw data as evidence. In either situation, the party offering the evidence must demonstrate the reliability of the procedure used in acquiring, storing, processing, and retrieving the evidence. Usually, processed evidence is offered to prove the truth of certain facts. Those facts must be developed through a demonstrated, reliable model of taking raw data and adding certain statements to draw reliable conclusions. A phone bill is an example of processed evidence.

The processing of electronic evidence—how it is collected, stored, and retrieved—is a new area of litigation for technical experts and brings new challenges to law enforcement. Therefore, a technical expert should always be available for law enforcement teams investigating computer cases. The affidavit of probable cause should request the court's permission to use private, expert personnel for the execution of the search warrant. The affidavit should be specific as to

why a private expert is required and what the expert's role will be during the execution of the warrant. The private expert should always be accompanied by an experienced police officer during the execution of a search warrant and the seizure or processing of evidence seized pursuant to the warrant. The chain of custody and integrity of the evidence should be of paramount concern during this process.

There are many more legal issues regarding searching and seizing computer evidence that cannot be addressed in the space provided by this guide. Law enforcement officers should not use their role in searching and seizing computer evidence as an introduction to this technology. Most seizures require an expert to retrieve, analyze, and preserve data. If your department does not have staff who are adequately trained in how to search and seize computer evidence, the department should hire an expert. In determining what type of expert is required, you need as much information on the target equipment and system as possible.

Summary

Armed with knowledge of the highly predictable sexual behavior patterns of preferential sex offenders and their use of computer technology, investigators can confidently devise effective investigative strategies to combat the sexual exploitation of children. Such knowledge can influence interview approaches, collection of computer evidence, and location of corroborative evidence and other victims.

The sophisticated use of computers in criminal activity complicates law enforcement efforts, but it should not deter the aggressive pursuit of those who use computer technology to victimize children. By following proper investigative procedures and keeping in mind relevant legal considerations, investigators can avoid losing valuable evidence. By keeping abreast of technological advancements, the criminal justice system can successfully hold child sexual predators responsible for their behavior.

Endnotes

1. *Diagnostic and Statistical Manual of Mental Disorders, 4th edition.* Washington, DC: American Psychiatric Association, 1994.

2. 15 U.S.C. §§ 2251 *et seq.*
3. *United States* v. *Reed,* 935 F.2d 641 (4th Cir.), *cert. denied,* 1125 S. Ct. 923 (1991).
4. *Texas* v. *Brown,* 460 U.S. 730 (1983).
5. *Schnecklath* v. *Bustamonte,* 412 U.S. 28 (1973).
6. *United States* v. *Matlock,* 415 U.S. 164 (1974).
7. *Plessent* v. *Lovell,* 876 F.2d 787 (10th Cir. 1986).
8. 42 U.S.C. §§ 2000aa *et seq.*
9. 28 C.F.R. § 59.4b.
10. *United States* v. *Mittleman,* 999 F.2d 440 (9th Cir. 1993).
11. *Esmay* v. *United States,* 1993 U.S. Dist. LEXIS 20362 (D. Ariz. 1993).
12. 816 F. Supp. 432 (W.D. Tex. 1993).
13. 18 U.S.C. §§ 2510 *et seq.* and 2701 *et seq.*
14. The issue of attorney's fees and litigation costs under the PPA is discussed in *Minneapolis Star & Tribune Co.* v. *United States,* 713 F. Supp. 1308 (D. Minn. 1989).
15. 18 U.S.C. § 2702.
16. *Davis* v. *Gracey,* 111 F.3d 1472 (10th Cir. 1997) (discusses whether incidental seizure of electronic communications, standing alone, is a violation of the ECPA and the good faith elements of defense thereto); *United States* v. *Moriarty,* 1997 U.S. Dist. LEXIS 6678 (D. Mass. 1997) (interprets term "intercept" within the ECPA); *United States* v. *Reyes,* 922 F. Supp. 818 (S.D.N.Y. 1996) (addresses whether numbers from pagers fall within the ECPA).
17. *United States* v. *Rodriguez,* 968 F.2d 130 (2d Cir.), *cert. denied,* 113 S. Ct. 140 (1992).

Contributing Authors

Daniel S. Armagh, J.D.
Director, National Center for
Prosecution of Child Abuse
American Prosecutors Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, VA 22314
703–739–0321
703–549–6259 (fax)
E-Mail: daniel.armagh@ndaa-apri.org

Nick L. Battaglia
Sergeant, San Jose Police Department
201 West Mission Street
San Jose, CA 95110
408–277–4345
408–277–5218 (fax)
E–Mail: nickb1706@aol.com

Kenneth V. Lanning, M.S.
Supervisory Special Agent
Federal Bureau of Investigation
National Center for the Analysis of Violent Crime
FBI Academy
Quantico, VA 22135
540–720–4732
540–720–4792 (fax)

Supplemental Reading

Armagh D. A Safety Net for the Internet: Protecting Our Children. *Juvenile Justice* 5(1):9–15, 1998.

Child Safety on the Information Highway (pamphlet). Washington, DC: National Center for Missing and Exploited Children, 1994.

Whitcomb D. *When the Victim is a Child.* 2d ed. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 1992.

Organizations

Child Exploitation and Obscenity Section
Criminal Division
U.S. Department of Justice
1331 F Street NW., Sixth Floor
Washington, DC 20004
202–514–5780
202–514–1793 (fax)
202–305–4320 (fax)

The Child Exploitation and Obscenity Section (CEOS) of the Criminal Division, U.S. Department of Justice, has supervisory responsibility for Federal statutes covering obscenity, child exploitation, child sexual abuse,

activities under the Mann Act, sex tourism, missing and abducted children, and child support recovery. Created in 1987, CEOS is a specialized section composed of attorneys with broad expertise in prosecuting obscenity, child exploitation, and child abuse. CEOS's jurisdiction is limited to enforcement of Federal statutes. Section attorneys work with U.S. Attorneys on child exploitation cases across the country, providing litigation and support services. They also provide training, both domestically and internationally, for prosecutors, judges, attorneys, law enforcement, and victim service systems. CEOS attorneys advise task forces on missing and abducted children, child abuse, sex offender recidivism and registration, and youth placement. CEOS works with victim-witness offices of the U.S. Attorney's offices.

Federal Bureau of Investigation (FBI)
Innocent Images Initiative
Baltimore Division
11700 Beltsville Drive
Calverton, MD 20705
301–586–4519 (8:00 a.m. to 4:00 p.m.)
301–586–4500 (4:00 p.m. to 12:00 p.m.)
Internet: www.fbi.gov/fo/balt/mainfr.htm

Operation Innocent Images identifies and develops prosecutable cases on individuals who use Bulletin Board Systems to victimize children. FBI agents and task force officers, who pose as young children or sexual predators, go online to investigate those individuals who recruit minors into illicit sexual relationships, electronically distribute pornographic images of children, or post illegal images onto the Internet.

National Center for Missing and Exploited Children (NCMEC)
2101 Wilson Boulevard, Suite 550
Arlington, VA 22201–3052
800–THE–LOST (800–843–5678)
703–235–4067
Internet: www.missingkids.org

A clearinghouse of information on missing and exploited children, NCMEC operates a 24-hour hotline and child pornography tipline and provides a wide range of free services, including technical case assistance, link and pattern analysis on cases, forensic assistance, training programs, and educational material and publications. NCMEC also offers CyberTipline (www.missingkids.com/cybertip), an online service for reporting sexual exploitation. Parents or children can file a report by completing and submitting an online form that is reviewed by an Exploited Child Unit information analyst and submitted to law enforcement to include the FBI, the U.S. Customs Service, and the U.S. Postal Inspection Service.

National Center for Prosecution of Child Abuse
American Prosecutors Research Institute (APRI)
99 Canal Center Plaza, Suite 510
Alexandria, VA 22314
703–739–0321
Internet: www.ndaa-apri.org

The National Center for Prosecution of Child Abuse is a nonprofit and technical assistance affiliate of APRI. In addition to research and technical assistance, the Center provides extensive training on the investigation and prosecution of child abuse and child deaths. The national trainings include timely information presented by a variety of professionals experienced in the medical, legal, and investigative aspects of child abuse.

U.S. Customs Service
Cyber Smuggling Center
11320 Random Hills Road, Suite 400
Fairfax, VA 22030
703–293–8005
Internet: www.customs.ustreas.gov/

The Cyber Smuggling Center's main focus is to patrol the Internet for signs of the illegal importation and proliferation of child pornography or of sexual exploitation of children. The center conducts all Internet investigations from a central location.

U.S. Postal Inspection Service
475 L'Enfant Plaza West SW.
Washington, DC 20260
202–268–4286
Internet: www.usps.gov:80/postalinspectors/

The U.S. Postal Inspection Service, often working with agencies such as the Child Exploitation and Obscenity Section of the U.S. Department of Justice and the National Center for Missing and Exploited Children, conducts undercover operations to investigate individuals who use the Internet or a Bulletin Board Service to exchange pornography or who correspond with others who do the same. In some undercover operations, postal inspectors contact suspects via computer networks and the Internet. Individuals who use the U.S. mail for the actual exchange of material or for initial contact are subject to investigation.

Internet Crimes Against Children Program

In September 1998, with 10 awards to State and local law enforcement agencies across the Nation, OJJDP began a national program to counter the emerging threat of offenders using the Internet or other online technology to sexually exploit children. Designed to encourage communities to adopt a multidisciplinary, multijurisdictional response to this threat, the Internet Crimes Against Children (ICAC) Task Force Program ensures that participating State and local law enforcement agencies can acquire the necessary knowledge, equipment, and personnel resources to prevent, interdict, or investigate ICAC offenses. Under this program, ICAC task forces serve as regional sources of prevention, education, and investigative expertise to provide assistance to parents, teachers, law enforcement, and professionals working on child victimization issues.

Policing in cyberspace presents new and unique challenges for American law enforcement. In cyberspace, traditional boundaries are ignored and the usual constraints of time, place, and distance lose their controlling influence. Because very few cases start and end within the same jurisdiction, nearly all ICAC investigations involve multiple jurisdictions and require extensive multiagency collaboration. However, multiagency collaboration is challenging. Federal, State, and local law enforcement organizations have legitimate, understandable concerns about initiating cases based on information that may have been gathered through inappropriate conduct or investigative techniques by officers of another agency.

OJJDP has established operational and investigative standards for the ICAC Task Force Program through a collaborative process with the 10 original ICAC Task Force agencies and the Federal Bureau of Investigation (FBI); U.S. Customs Service (USCS); U.S. Postal Inspection Service (USPIS); U.S. Department of Justice, Criminal Division, Child Exploitation and Obscenity Section (CEOS); and the National Center for Missing and Exploited Children (NCMEC). These standards were designed to foster information sharing, coordinate investigations, avoid duplication or disruption of ongoing investigations, ensure the probative quality of undercover

operations, and facilitate interagency case referrals through the standardization of investigative practices. Collaborative undercover operations, when properly executed and documented according to the ICAC Task Force Program standards, can collect virtually unassailable evidence and, most important, allow law enforcement to bring a case before a suspect can victimize a child.

OJJDP's ICAC Task Force Program is administered through a shared management system that combines a national perspective with the local values of participating communities to address coordination and communication concerns related to ICAC investigations. OJJDP has established a review board, composed of law enforcement managers and prosecutors from participating agencies, to assist in the administration of this program. The board, while primarily responsible for reviewing undercover operations for compliance with the ICAC Task Force Program standards, plays a critical role in assessing the needs of the field and in formulating policy for the national program. Representatives from FBI, USCS, USPIS, and CEOS serve as technical advisors to the board.

In addition, OJJDP, in consultation with Federal law enforcement and prosecutorial agencies and NCMEC, has developed a certification course for agencies participating in the program. The course prepares ICAC Task Force investigators and managers to develop policies and employ proven investigative procedures in response to computer-facilitated sexual exploitation of children.

In fiscal year 1999, $5 million is available for the ICAC Task Force Program. OJJDP will award a total of $2.6 million in grants to a minimum of eight new jurisdictions. In addition, a total of $2.4 million in continuation funds will be available to the 10 jurisdictions that received initial grants in fiscal year 1998.

For more information on the ICAC Task Force Program, visit OJJDP's Web site at www.ojjdp.ncjrs.org or contact the Juvenile Justice Clearinghouse at 800–638–8736, 301–519–5212 (fax), or askncjrs@ncjrs.org (e-mail).

Other Titles in This Series

Currently there are 12 other Portable Guides to Investigating Child Abuse. To obtain a copy of any of the guides listed below (in order of publication), contact the Office of Juvenile Justice and Delinquency Prevention's Juvenile Justice Clearinghouse by telephone at 800–638–8736 or e-mail at puborder@ncjrs.org.

Recognizing When a Child's Injury or Illness Is Caused by Abuse, NCJ 160938

Sexually Transmitted Diseases and Child Sexual Abuse, NCJ 160940

Photodocumentation in the Investigation of Child Abuse, NCJ 160939

Diagnostic Imaging of Child Abuse, NCJ 161235

Battered Child Syndrome: Investigating Physical Abuse and Homicide, NCJ 161406

Interviewing Child Witnesses and Victims of Sexual Abuse, NCJ 161623

Child Neglect and Munchausen Syndrome by Proxy, NCJ 161841

Criminal Investigation of Child Sexual Abuse, NCJ 162426

Burn Injuries in Child Abuse, NCJ 162424

Law Enforcement Response to Child Abuse, NCJ 162425

Understanding and Investigating Child Sexual Exploitation, NCJ 162427

Forming a Multidisciplinary Team To Investigate Child Abuse, NCJ 170020

Additional Resources

American Bar Association
(ABA)
Center on Children and the
Law
Washington, D.C.
202–662–1720
202–662–1755 (fax)

American Humane Association
Englewood, Colorado
800–227–4645
303–792–9900
303–792–5333 (fax)

American Medical Association
(AMA)
Department of Mental Health
Chicago, Illinois
312–464–5066
312–464–5000
(AMA main number)

American Professional Society
on the Abuse of Children
(APSAC)
Chicago, Illinois
312–554–0166
312–554–0919 (fax)

C. Henry Kempe National
Center for the Prevention
and Treatment of Child
Abuse and Neglect
Denver, Colorado
303–864–5250
303–329–3523 (fax)

Federal Bureau of Investigation
(FBI)
National Center for the
Analysis of Violent Crime
Quantico, Virginia
800–634–4097
540–720–4700

Fox Valley Technical College
Criminal Justice Department
Appleton, Wisconsin
800–648–4966
414–735–4757 (fax)

Juvenile Justice Clearinghouse
(JJC)
Rockville, Maryland
800–638–8736
301–519–5212 (fax)

National Association of Medical
Examiners
St. Louis, Missouri
314–577–8298
314–268–5124 (fax)

National Center for Missing
and Exploited Children
(NCMEC)
Arlington, Virginia
703–235–3900
703–235–4067 (fax)

National Center for
Prosecution of Child Abuse
Alexandria, Virginia
703–739–0321
703–549–6259 (fax)

National Children's Alliance
Washington, D.C.
800–239–9950
202–639–0597
202–639–0511 (fax)

National Clearinghouse on
Child Abuse and Neglect
Information
Washington, D.C.
800–FYI–3366
703–385–7565
703–385–3206 (fax)

National Committee to Prevent
Child Abuse (NCPCA)
Chicago, Illinois
800–CHILDREN
312–663–3520
312–939–8962 (fax)

National SIDS Resource
Center
Vienna, Virginia
703–821–8955, ext. 249
703–821–2098 (fax)

U.S. Department of Justice
Office of Justice Programs
Office of Juvenile Justice and Delinquency Prevention

Washington, DC 20531

Official Business
Penalty for Private Use $300

PRESORTED STANDARD
POSTAGE & FEES PAID
DOJ/OJJDP
PERMIT NO. G–91