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 immediate world in which we live, the "virtual world" of the World Wide Web poses serious risks to children. Although parents advise their children not to talk to strangers at the playground, they often fail to warn them about the dangers of online conversations.

These dangers are considerable. With the anonymity and validation it affords sex offenders, the Internet has become a cyberplayground for those who prey on children. Given the swiftly evolving nature of computer technology, the investigation of child sexual exploitation involving computers poses significant challenges to law enforcement.

This second edition of *Use of Computers in the Sexual Exploitation of Children* updates the original to provide law enforcement—in particular, first responders—the information they need to meet those challenges. The guide describes the behavioral characteristics of sexual predators who target children, offers best practices for investigations involving computer evidence, and sets forth the legal principles governing the search and seizure of computer systems.

It is my hope that the information this Portable Guide provides will help police officers and investigators hold those who exploit computer technology to victimize children accountable for their crimes and protect children from being victimized by such predators. Anything less is unacceptable.

J. Robert Flores
Administrator
Office of Juvenile Justice and Delinquency Prevention

NCJ 214167

Use of Computers in the Sexual Exploitation of Children

Second Edition

Daniel S. Armagh
Nick L. Battaglia

Portable Guides to Investigating Child Abuse

Office of Justice Programs
Partnerships for Safer Communities
www.ojp.usdoj.gov

Office of Juvenile Justice and Delinquency Prevention
www.ojp.usdoj.gov/ojjdp

December 2006

Contents

Overview 1

Key Points 3

Understand the Behavior of Child Predators 3

Know How Child Predators Use Computers 4

Organizing Their Collections 5
Corresponding With Other Predators 6
Finding Potential Victims 6

Know How To Investigate Cases Involving Computers 7

Beginning the Investigation 7
Establishing the Context 8
Obtaining a Search Warrant 10
Handling Computer Equipment 12
Analyzing a Computer System 14

Know the Legal Considerations in the Use of Search Warrants 16

Drafting the Affidavit of Probable Cause 16
Use of discovered images to support your affidavit 17
Use of expert opinion 19
Use of anticipatory search warrants 20
Warrants for privileged and confidential communications 20
Conducting a Search Without a Warrant 21
Exigent circumstances 21
Evidence in plain view 21
Consent to search 22
No-knock warrant 24
Undercover agents 24

Summary 25

Resources 25

Contributing Authors 25

Supplemental Reading 26

Organizations 27

List of Sidebars

Relationship of Computer Evidence to the Behavioral Stage of the Predator 5

Child Pornography 6

Basic Questions To Ask Victims, Witnesses, and Suspects 9

What, Exactly, Constitutes "the Computer"? 11

Chain of Custody 13

What To Include in Your Affidavit of Probable Cause 18

Consent To Search a Computer Used by More Than One Person 23

Overview

As more and more people discover the ability to communicate faster and more efficiently through computers and the Internet, the possibility that predators will use these tools to advance their criminal activities also increases. The first online services were oriented toward adults, but children now make up one of the fastest growing populations of Internet users. Nearly 30 million children and youth go online each year to research homework assignments, play games, and meet friends. This increased access to computer technology puts children at greater risk of sexual exploitation. 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 images of illicit activities with child victims. Nineteen percent of children ages 10–17 surveyed in the U.S. Department of Justice's (DOJ's) Youth Internet Safety Survey received unwanted sexual solicitations online.[1]

What is child sexual exploitation? As used in this guide, the term "child sexual exploitation" refers to the sexual victimization of children and covers many different types of child sexual abuse. Child sexual exploitation encompasses more than physical sexual molestation. Any display or suggestion of sexual activity involving children, including written or graphic material, can be considered child sexual exploitation. Such material ranges from depictions of explicit sexual acts performed by children with adults or children with children to images depicting a fully dressed child in a sexual pose. The material need not meet the legal definition of child pornography. Nonsexual images of a child intermixed in a graphic display with other media that suggests sexually oriented activity can be considered child sexual exploitation.

---

[1] D. Finkelhor, K. Mitchell, and J. Wolak, *Highlights of the Youth Internet Safety Survey,* Fact Sheet (Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention, 2001).

Cases of computer-facilitated child sexual exploitation may involve members of the child's own family (intrafamilial offenders), although this is not typical. Most child sexual exploitation investigations will involve one or more perpetrators victimizing several children over long periods of time. The victims will engage in explicit sexual activity, and the predators will document that activity in text and/or graphics on some type of media. The evidence will show that the perpetrator sought out the child specifically for sexual activity—that his[2] actions were premeditated as opposed to being a "crime of opportunity."

Because of the broad spectrum of what can be considered exploitation, you must know what is prosecutable in your jurisdiction. You must then obtain all available evidence—subtle as well as blatant—to show the perpetrator's state of mind and the entire process of planning and ultimately committing the offense.

What do I need to know about investigating child sexual exploitation involving computers? Rapid changes in computer technology and the complexity of the legal issues surrounding it can make even the most basic investigation of child sexual exploitation involving computers a complicated undertaking. These investigations typically require numerous investigators with different areas of expertise. To be ready to respond, law enforcement should identify experts and resources available to assist in computer-related cases. Local agencies can do much to prepare themselves for dealing with the forensic complexities of this type of investigation by establishing a formal working relationship with their state or regional Internet Crimes Against Children (ICAC) Task Force. (Contact information for the ICAC Task Force Program is included in the Resources section at the end of this guide.)

Investigators should stay in contact with the prosecutor working on the case at all times to make sure that all actions taken are within the law. **Mishandling of computer equipment or improper investigative techniques that violate a defendant's rights can result in the loss of valuable evidence.** Once that information is lost, it may be impossible to recover.

Exploitation cases involving computers present many investigative challenges, but they also present the opportunity to obtain a great

[2] Women can also be child predators. In this guide, for simplicity's sake, the authors use the male pronoun to refer to all sexual offenders who prey on children.

deal of corroborative evidence and investigative intelligence. Investigating child sexual exploitation cases that involve computers requires an understanding of:

- The behavior of child predators and how they use computers.
- The issues involved in investigations of computer evidence.
- The legal considerations governing the search and seizure of computer systems.

Remember: The role of computers in child sexual exploitation goes beyond that of other technological advancements such as the Polaroid camera, video camera, and digital camera. Although the principles established for investigating child predators in the past are still relevant, investigators need specialized expertise when confronted with predators who use computers in committing their crimes.

Understand the Behavior of Child Predators

Child predators—sexual offenders who act on their sexual interest directed toward children—come from all economic and social backgrounds. Other terms used for these offenders include "pedophile" and "preferential sex offender." However, these terms have specific clinical definitions. This guide uses the term "child predator" because it is a nonclinical term that anyone can testify to in court.

Experience gained through hundreds of investigations and interviews shows that the behavior of child predators usually develops in four stages:

- **Awareness.** An individual first comes to realize that he has a sexual interest in children. This interest may manifest itself in several ways. Usually, the individual gathers as much information as possible on the subject in an attempt to understand his feelings. In this early stage, the Internet provides access both to a variety of information sources—newspaper articles, newscasts, groups such as the North American Man/Boy Love Association (NAMBLA)—and to online chats with other individuals who may have similar interests.

- **Fantasy.** The individual uses the research that he has collected as a source for sexual fantasizing and stimulation. Eventually, the fantasy becomes more fixated, with an emphasis on child pornography. An individual using a computer will exchange e-mail with others who share the same interests and save these messages and all other related material using some type of computer storage medium.
- **Stalking.** Fantasy is no longer enough, and the individual is now compelled to seek closeness to actual children. The child predator will loiter at athletic events, parks, playgrounds, school bus stops, and other locations where children are found and may seek positions of trust in order to have access to children. Hardcore child pornography plays an important role at this stage. An individual using a computer will progress from online chats with others with the same interests to chats with potential victims. He may send them photos of himself in sexual poses and request similar sexual photos in return.
- **Molestation.** The individual molests a child. The predator using a computer sets up a meeting with the child he has been corresponding with. Depending on the predator, the meeting may lead either to a seduction or to abduction of the child.

Understanding these behavioral patterns can help you structure the investigation and predict what and how much material evidence a computer is likely to yield (see the sidebar on page 5). However, be aware that an individual child predator may demonstrate all, some, or even none of these behaviors. Lack of evidence of the sequence of behaviors described above does not in itself clear a suspect. For more information on the general characteristics and behavioral dynamics of child predators, see *Understanding and Investigating Child Sexual Exploitation,* another guide in this series.

Know How Child Predators Use Computers

Like other child predators, those who use computers may be compelled to collect child pornography and child erotica (see sidebar, page 6), correspond with other predators, and, ultimately, solicit a child for sexual activity. The computer is a powerful tool that offers child predators an easy, efficient, and anonymous means

Relationship of Computer Evidence to the Behavioral Stage of the Predator

Behavioral Stage	Evidence
Awareness	News releases, research articles, and chat room conversations with organizations that promote child sex.
Fantasy	All of the above, plus child pornography and explicit chat room conversations with other suspects or unsuspecting children.
Stalking	All of the above, plus more graphic, hardcore child pornography, including pornographic photos or digitally altered ("morphed") photos of local children.
Molestation	All of the above, plus images of actual victims engaged in sexual acts with the suspect and/or other suspects.

of achieving all of these goals within the confines of their home, workplace, local library, or any other location that offers them access to a computer.

Organizing Their Collections

A child predator who is also a collector may save everything that relates to children. Before computers were widely available, predators often recorded their exploits in diaries. Now they can use word-processing software to write about their experiences. Where child predators once saved photos in albums, now they can store and organize all information they collect on their computer's hard drive or a removable storage device. This material may include chat room text, chat room user profiles, pictures chat room users have placed in their profiles, any Internet correspondence with a child, and child pornography. Child predators can hide text, digital images, graphics files, and video files by using passwords and/or encryption techniques.

Child Pornography

Computer technology and the Internet have made child pornography more readily available in the United States than ever before. In addition to collecting and storing images, text, and video, predators can use their computers to create and transmit child pornography. Increasingly sophisticated graphics and multimedia software have enabled child predators to manipulate and animate images and even to create full-length DVDs of their own or someone else's sexual molestation of a minor. Sexual predators may use some of this pornography to solicit children. Twenty-five percent of the youth surveyed in DOJ's Youth Internet Safety Survey reported unwanted exposure to sexually explicit material.

Corresponding With Other Predators

Child predators may seek validation by communicating with other adults who have similar interests. The Internet enables these individuals to exchange information and share child pornography with less risk of identification or discovery. For predators in the awareness stage, the Internet offers a means to research their interests anonymously from the privacy of their own home.

Finding Potential Victims

Previously, predators loitered in parks. Now they no longer need to seduce a child in person. Using the Internet, a predator can enter children's chat rooms to develop relationships and, ultimately, solicit a child. Curious children may also stray into adult chat rooms that advertise themselves as discussing adult/child sexual relationships, where the children become vulnerable to sexual exploitation.

Child predators enter children's chat rooms by posing as someone friendly or interesting to a child. The type of chat room can vary from educational to one devoted to a specific interest such as sports, music, movies, or television programs. Chat room participants fill out a profile that other users can see, listing their name, hobbies, and interests. The predator will check profiles of users to look for victims. After carrying on a dialog with the parties in the chat room, the predator usually will invite a potential victim into a "private chat room" not accessible to anyone else. The predator can download all conversation from the private chat room to a

computer storage medium. Once the predator downloads this conversation, he can use it for fantasizing, share it with other child predators, or use it to blackmail the victim into a personal meeting.

Know How To Investigate Cases Involving Computers

Investigating cases of child sexual exploitation in which computers were used is complex. The demands of these investigations may exceed the resources available to a jurisdiction. However, you can eliminate or minimize many of the problems that may arise if you follow the guidelines presented below and act within the legal boundaries described in the section beginning on page 16. Your state/regional ICAC Task Force can provide assistance with all of the issues outlined below.

Beginning the Investigation

When initiating an investigation, take the following issues into consideration:

- **Jurisdiction.** ***Will your investigation remain local or extend to federal or state jurisdiction?*** You may not know the answer to this question until you have seized and analyzed the computer system. Child exploitation investigations involving computers may rise to the state or federal levels because of victims and/or suspects identified in other locations. You must recognize this possibility at the earliest moment so you can begin immediately to prepare for the future involvement of all agencies. Doing so 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 also computer and software technology. If you do not have this knowledge, look to other agencies at the federal, state, or local levels for help. Key resource organizations are listed at the end of this guide (pages 27–30).
- **Equipment.** ***Does your organization have the equipment needed to conduct this investigation or the resources to obtain the necessary equipment?*** Forensic computer examinations, depending on the sophistication of the equipment seized for evidence, may require significant resources beyond the

capacity of your agency. You may need to purchase, lease, or borrow the necessary equipment (e.g., search software and state-of-the-art computer systems with DVD writers and other high-end capabilities) from other agencies. The prosecuting attorney's decision about what evidence is needed and how it should be presented to the court may affect this decision. 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?*** You may need to consider seeking assistance from other agencies or forming a task force. 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?*** Many of these investigations will uncover more suspects and more victims—often a significant number of both. Multiple jurisdictions are often involved. Before proceeding with the investigation, formulate plans for dealing with such complications and for properly collecting and packaging the evidence with a view to its future use.

Once you have answered these questions, consider the following guidelines as a basis from which to proceed with your investigation. The guidelines describe what to do and what not to do when investigating cases of child sexual exploitation involving computers.

Establishing the Context

- **Establish that a child sexual exploitation situation exists.** You must obtain 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. Other records—school, juvenile, military, medical, driving, employment, bank, sex offender history, and sex offender registry—can be valuable sources of information.

- **Establish that the suspect owns or has access to a computer and uses it for child sexual exploitation.** Ask the suspect, victim(s), witnesses, and others specific questions that will reveal any knowledge related to the suspect's use of any computer. The knowledge may be firsthand or circumstantial.

Basic Questions To Ask Victims, Witnesses, and Suspects

Questions for Victims:

- Does the suspect have a computer?
- Did you play games on his computer? Was anyone else present?
- Did he talk to you in a chat room?
- Did he send you any pictures? If so, what kind?
- Did he mail you anything (e.g., cameras, tickets, phone cards)?
- Did he tell you to delete files or take any other steps to hide your actions?

Questions for Witnesses:

- Has he ever minimized the screen when you came in?
- Does he have a desktop computer or a laptop?
- Does he take his laptop computer to work, or does he use a different computer at work?
- How much time does he spend on the Internet?
- Have you ever seen any pornography on his computer?

Questions for Suspects:

- Do you have a computer at home? If so, what kind?
- How long have you owned this computer?
- Do you have an Internet account? If so, with which service provider?
- What is your screen name? How many screen names do you have?
- Do you have any pornographic images on your computer?
- Who else uses your computer? Do they have their own password and screen name?
- Do you give your password to anyone else?
- Do you use a computer at work? Do you share files with it and your home computer, or do you use a laptop for both work and home?
- Do you have a network at work or at home?

- **Determine the type of computer the suspect used and the location of this computer.** Is it a desktop or laptop? Is it at the suspect's residence or workplace or both? If the computer is at the suspect's residence, does the suspect have e-mail access to computers in other locations, such as the workplace, the homes of neighbors or friends, or the public library? Keep in mind that other devices can also store valuable information. These devices include handheld computers; personal digital assistants (PDAs); mobile camera phones, some of which can take and send movies; digital camera flashcards; and storage media such as floppy disks, compact disks, digital video disks, and memory keys.

  Also be aware of wireless capabilities. With a wireless router and remote wireless storage device, a suspect can store files in an area of the residence away from the main computer area or even outside the residence. A suspect also may tap into a neighbor's wireless system. Wireless hubs are beginning to appear across many cities.

  Devices are available that will enable you to detect the presence of wireless systems. When a suspect is tapping into another's wireless system, more investigative steps and technical expertise are necessary to show the connection between the technical evidence seized and your suspect.

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

Obtaining a Search Warrant

If sufficient probable cause exists:

- Obtain a warrant or subpoena to serve on telephone companies (for telephone records) and online services (for screen names, account information, log files related to the suspect's use of the service, and e-mail records). Be aware that most online services require accounts to be paid with a credit card and do not accept Post Office boxes as mailing addresses. Financial records that banks or other financial institutions maintain also may contain information that shows the child predator's credit cards were used for illegal purposes online.

- Obtain a search warrant for the suspect's computer system and any related systems such as workplace computers, laptops, and digital handheld devices.

In preparing the search warrant:

- Include all computer hardware and software. **Note:** You must explain how the entire computer system played a role in the criminal conduct you are investigating. Specify a reason for seizing each component of the system. (See "What, Exactly, Constitutes 'the Computer'?" below.)
- List accounting records that will enable you to identify payments to online services in use currently and in the past. Keep in mind that these records may be located on the suspect's computer system. Remember that payment for services could

What, Exactly, Constitutes "the Computer"?

Do not assume that any item connected to the target device may automatically be seized. The fourth amendment to the Constitution specifies that a search warrant should "particularly" describe the place to be searched and the persons or things to be seized. This requirement presents challenges in drafting an affidavit of probable cause to search and seize "the computer": You must have the entire computer system to replicate the suspect's use of it and to analyze that use; however, when drafting your affidavit for the warrant, you may not know the exact configuration of the target computer or the kind of data storage media the suspect used.

State a basis for seizing each component of the computer system. To protect your execution of the search warrant from serious challenge in court, your application for the warrant should include facts that justify the seizure of all components of the suspect's computer system, namely, the base unit, each peripheral device, and all software, manuals, data storage media, and related items. Consider what role each component might have played in the commission of the crime and, based on your training, experience, and knowledge about criminal conduct involving computers, state the facts that support seizing those items. To satisfy the particularity requirement of the fourth amendment, the wording of your search warrant must be reasonably specific rather than elaborately detailed.

be charged to credit card accounts. You should seize the accounting records to identify these accounts.

- Ask your prosecutor whether your original warrant should include a "request for forensic examination." Doing so may save you the time involved in having to ask for another warrant to search hard drives and software programs after the equipment is seized.

Work closely with the prosecuting attorney in all aspects of obtaining search warrants. Case law in this area changes frequently. Depending on the suspect, you may need a "special master" (an attorney appointed by the court to review privileged or confidential information in an investigation to determine its relevancy as admissible evidence) to search the suspect's computer system. If the suspect uses the system as part of his business, case law may limit your ability to search the system. (For more about search warrants and probable cause, see pages 16–21.)

Handling Computer Equipment

- **Make sure someone with expertise and training in the seizure of computers for criminal investigations is present when you execute the search warrant.** 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. ICAC Task Forces can assist and are located throughout the nation. Local offices of federal agencies—e.g., the FBI and U.S. Immigration and Customs Enforcement (ICE)—may also provide 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. (Contact information for the FBI, ICE, and other organizations that can help is provided on pages 27–30).

- **Remember that the computer and all of its contents constitute evidence.** The computer should remain the same from the time you seize it until a forensic examiner examines it. **Never turn on a suspect's computer system until a qualified examiner can properly document the system and its contents.** Once the system is turned on, the evidence is altered. (See "Chain of Custody," page 13.)

Chain of Custody

Protecting the integrity of evidence seized in cases involving computers requires the same considerations as that seized in other cases: You must document the chain of custody of the evidence from the moment it is seized until the moment it is offered in evidence and strictly control access to evidence to avoid challenges to the admission of evidence at trial. In cases involving computers, an expert in computer forensics should be available for law enforcement teams at all stages of the investigation.

The handling of electronic evidence during processing—how it is collected, stored, and retrieved—is a new area for technical experts and brings new challenges to law enforcement. Because preservation of evidence in electronic form **as found at the scene of the crime** is essential, an expert in computer forensics should be present at the actual processing of the crime scene. This will ensure that the manner of collecting and processing the electronic evidence does not destroy, contaminate, or alter it, which would compromise the investigation.

If your agency does not have a qualified computer forensics examiner on staff, your affidavit of probable cause should request the court's permission to use expert personnel from the private sector for the execution of the search warrant. Be specific about why a private-sector expert is required and what the expert's role will be.

- **Consult qualified technical personnel before disrupting the power supply to the computer system.** Disrupting the power to the system will cause any data currently stored in the computer's random access memory (RAM) to be lost. RAM is where the computer temporarily stores data until the user saves it to a storage medium such as a hard drive, flash drive, floppy disk, or CD. Advances in technology have significantly increased the RAM in today's computers. Therefore, a system that is turned on may hold many images, video clips, and text that could be crucial evidence in an investigation. The power to the system should not be cut until qualified technical personnel have the opportunity to legally download any evidence located in the computer's RAM.

- **Do not make a printout of the contents of the screen.** If the computer is on and you find evidence on the screen, photograph or videotape the screen to create a visual record of the evidence. Your use of the computer and printer could arguably alter the electronic evidence and, therefore, change the nature of the evidence as you observed it. If you cannot visually document what you observe on the computer screen, make sure you can describe it in detail. Keep in mind the elements of the statute that the child predator's conduct violates.
- **Look for passwords to the computer system while searching the suspect's residence and/or workplace.** Most suspects use passwords for better security. Passwords 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 FBI or ICE office or ICAC Task Force for assistance in this area.
- **Keep the suspect's computer system intact.** It is best to move the system as a whole, with all components still connected together, if at all possible.
- **If you must disassemble the computer system, first take pictures of it.** Photograph the front and back of the system before you physically move it to identify how it is set up. For purposes of analysis and courtroom presentation, a computer specialist can use the photographs to put the system back together exactly as the suspect used it.

Analyzing a Computer System

- **Keep track of court-imposed deadlines.** The judge who grants the search warrant may impose a deadline for completing the forensic examination of the computer system. If your search of the computer is delayed for a valid reason (e.g., insufficient forensic laboratory resources to process the evidence in a timely manner), request an extension of the deadline before it expires. Failure to meet the court's deadline could result in suppression of the evidence recovered from the computer.
- **Only a qualified computer forensics examiner should attempt any forensic analysis of any seized computer system.** Completion of an 80-hour training course in computer forensics is usually the *minimum* requirement to qualify as an examiner. Expert computer forensic examiners usually obtain much

more training than this and have extensive on-the-job experience. **Note:** If the computer forensics examiner is from the private sector, an experienced police officer should be present during the analysis of the computer system.

- **Full examination of the computer's entire hard drive and all other storage media is absolutely necessary.** Both text files and graphics files are important evidence in a child sexual exploitation investigation. The forensic examiner analyzes the computer and its contents, but **the best people to determine what is or is not appropriate evidence in a particular investigation are the primary child sexual exploitation investigator and the prosecutor, if one has been assigned at this point.**

- **Stay within the scope of your search warrant.** If the search of the computer's files reveals evidence that was not anticipated in the warrant, do not continue to open files looking for more unanticipated evidence. Instead, use a description or printout of the first file containing such evidence as probable cause to obtain another search warrant for the new evidence.

- **An expert in recovering erased files is critical to your investigation.** With the proper software, an expert can recreate deleted text and graphics files if the suspect has not written over them 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. **At the scene, you will not be able to determine whether the suspect's computer contains recoverable erased files and should not try.**

- **The prosecuting attorney may require hard copies (i.e., paper printouts) of all the data on the suspect's computer system.** Child sexual exploitation experts can use the printouts to determine what appropriate evidence exists on the system. **Note:** Only the computer forensics examiner should make such printouts, unless the prosecutor or the court authorizes otherwise.

- **Know your jurisdiction's laws about duplicating child pornography for courtroom purposes.** Duplicating child pornography, even for courtroom purposes, may be illegal in your jurisdiction. If in doubt, consult your prosecutor before making copies of any child pornography found on the suspect's computer system.

Know the Legal Considerations in the Use of Search Warrants

Search warrants are an invaluable investigative tool, and search warrants on computers are an integral part of a comprehensive investigation of child sexual exploitation. However, the search and seizure of computers and related materials is rife with legal pitfalls. Knowing the legal principles that govern the search and seizure of computer systems can help you avoid violations that could open your criminal investigation to a successful motion to suppress evidence. Failing to observe these principles could turn the defendant in your exploitation case into the plaintiff in a civil suit that could leave you and/or your employer owing a great deal of money to the individual you were investigating.

Drafting the Affidavit of Probable Cause

Courts have a strong preference for search warrants when the evidence involves computers or other electronic devices and will scrutinize a warrantless search. Your affidavit of probable cause should contain specific articulable facts that show reasonable grounds to believe that the contents of electronic communications, records, hardware, software, or other information are relevant and material to your investigation. **The answers to the following preliminary questions should form a solid basis for the affidavit that supports your search warrant application:**

- Was the computer used to produce child pornography, store contraband (goods whose possession, importation, or exportation is prohibited by law), or disseminate materials or communications that are probative (i.e., offer evidence or proof) of criminal conduct, or to perform all three of these functions?
- What are the facts that support your conclusions about the use of the targeted computer?
- What is the suspect's expectation of privacy, if any, concerning the computer to be searched?

A frequent, significant shortcoming of affidavits of probable cause is the failure to clearly state facts that specifically describe what crime(s) are being committed. The sidebar on page 18–19 shows

what to include in an affidavit of probable cause to search a computer for evidence of child sexual exploitation.

The warrant's description of the contraband evidence contained in the computer must be specific enough to guide and control the investigator's judgment about what to seize and what not to seize. You should include any specific information about the images stored in the targeted computer or other information about the computer's contents in the affidavit to assist the court in the analysis of probable cause. Provide a narrative description of such images and describe their source. Mention that, on the Internet, the exact locations ("addresses") of such images may be in a constant state of flux. Explain that once the suspect's computer has been seized, a forensic analyst can use it to determine the exact source of the images in question.

Use of discovered images to support your affidavit

Images depicting the lascivious exhibition of a child's genitals usually are sufficient to support a search warrant. An undercover officer, posing online as a child, may receive child pornography or other criminal evidence from a suspect. Parents of children may discover such material and provide it to law enforcement. **In some jurisdictions, some of the images obtained from the investigation might be attached to the affidavit.** However, some judges are loathe to examine images of child pornography. You need to know whether the particular judge considering your application for a search warrant deems it necessary to view the images that form your probable cause to conduct a search or whether the judge prefers a description of what the images show.

In some jurisdictions, so-called sunshine statutes allow the media to view and copy attachments to an affidavit. If you are attaching images to your affidavit, you should consider filing the application under seal to prevent media access to these images. If the law in your jurisdiction does not allow you to file such images under seal, consider providing only a narrative description of the images. The court reporter's transcription of your narrative and any descriptive comments the judge makes when examining the images—including a finding that, in the opinion of the court, the images meet the legal definition of child pornography—will demonstrate probable cause while preserving the child victim's privacy.

What To Include in Your Affidavit of Probable Cause

- Introductory paragraph stating your training, knowledge, and experience in the area of investigating child sexual exploitation. Relevant information includes:
  - ❑ Current position within your department.
  - ❑ Responsibilities of your position.
  - ❑ Years on the job.
  - ❑ Specialized training/experience in searching and seizing electronic evidence.
  - ❑ Knowledge of sexual offenders generally.
  - ❑ Knowledge of sexual offenders who use computers to prey on children.
  - ❑ Other relevant information specific to the suspect or investigation.
- Information to educate and inform the court about electronic communications, the nature of the evidence, any challenges that are specific to the search and seizure of electronic evidence specific to the relevant targets, and any privileged or privacy concerns unique to the technology, including but not limited to:
  - ❑ The Internet.
  - ❑ The World Wide Web.

(continued on next page)

A few jurisdictions have not yet ruled on the issue of whether the court clerk may "possess" duplicated images of child pornography that are a part of a search warrant application once the application is filed with the court. Even though no criminal or civil actions have been filed against court clerks, law enforcement officers, judges, or prosecutors in such jurisdictions and qualified immunity probably would protect against such actions, the legal implications of attaching duplicate images to a search warrant application remain an open question.

What To Include in Your Affidavit of Probable Cause (continued)

- ❑ E-mail.
- ❑ Instant messaging.
- ❑ Hotmail or other free e-mail services.
- ❑ News groups.
- ❑ Chat rooms.
- ❑ Bulletin board services.
- ❑ Electronic communications services.
- ❑ Remote computer services.
- ❑ Any other relevant information technologies and definitions of computer terms.
- ❑ Shorthand descriptors or icons used in communicating online and what their meaning is within the context of this specific target.
- ❑ The make, model, and exact series of the targeted computer, if known. (An operating system manual may be attached as an addendum to a search warrant.)

- ✹ Factual description of where investigators will find the targeted evidence in the place to be searched.
- ✹ Trustworthy facts that demonstrate that a crime has been committed—for example, evidence of child pornography and where such evidence can be found.

Use of expert opinion

An expert's opinion regarding the behavioral characteristics of child predators may provide a basis for obtaining a warrant to search a suspect's residence, business, or computer system. You can use expert opinion to show how case-specific, documented behaviors commonly seen in known child predators apply to the suspect. If your affidavit of probable cause uses expert opinion in this way, you **must** set forth facts to support classifying the suspect as a particular type of offender. The facts you include in the affidavit in turn corroborate the expert opinion.

Avoid the use of boilerplate or generic language in describing the behavioral traits of the offender. If your affidavit uses expert opinion regarding the behavioral traits of child predators, you should clearly describe not only the characteristics of the relevant offender classification but also the particular facts about the suspect that support the conclusion that he belongs in the specified offender category. Be aware that terms such as "child molester," "situational or preferential child molester," or "pedophile" have specific clinical definitions. If you use one of these terms to describe the suspect, your evidence must meet the clinical definition of the term.

In child sexual exploitation cases, use expert opinion in search warrant affidavits only when necessary. Court decisions on such warrants have not been consistent, so the use of expert opinion in this way involves a certain amount of legal uncertainty.

Use of anticipatory search warrants

If, at the time you apply for a warrant, you do not have sufficient probable cause to determine whether the contraband you will seize is at the location specified in the warrant, you will need to apply for an anticipatory search warrant. For a judge to issue this type of warrant, you must have sufficient demonstrable evidence to support probable cause that contraband will be in the place to be searched at the particular time the warrant is to be executed. In most cases, obtaining an anticipatory warrant requires you to demonstrate precedent conditions or a pattern of criminal behavior that supports the warrant. Ideally, an anticipatory warrant states what "triggering event" will place the evidence in the location described.

Warrants for privileged and confidential communications

When gathering evidence, you may want to examine computer materials that contain privileged or confidential communications, such as the records of doctors, lawyers, and clergy. Special statutes govern searches of such materials. When you draft an affidavit for a search warrant to examine privileged and confidential communications, narrow your focus to include only data relevant to the investigation. Describe such data as specifically as possible. Generic, boilerplate affidavits are insufficient and often result in suppression of the evidence.

Before executing search warrants for privileged or confidential communications, you should ask a knowledgeable prosecutor to thoroughly brief you on the restrictions of the Privacy Protection Act of 1980 (PPA),[3] all accompanying regulations, and all applicable state privacy statutes. If your search involves communications on computers or bulletin board services, your prosecutor should brief you on the Electronic Communications Privacy Act of 1986[4] in addition to the PPA, so that you can avoid liability for violations of these laws. Note that because the PPA does allow for civil remedies, investigators who violate this statute may be liable for damages.

Conducting a Search Without a Warrant

The general exceptions to the search warrant requirement apply to computer systems. These are summarized below.

Exigent circumstances

To be considered exigent, the circumstances must be urgent—that is, 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, overwriting mechanisms, magnetic fields, "hot buttons," and "kill commands" make it vulnerable to instantaneous destruction. Exigent circumstances may apply to computers simply because of the fragile character of such evidence.

Remember: The authority to seize a container without a warrant does not necessarily authorize a warrantless search of its contents. While exigent circumstances may justify seizing a computer and/or component attachments, you may not be authorized to *search* that computer unless you obtain a warrant after the seizure.

Evidence in plain view

Evidence of a crime may be seized without a warrant if the investigator is in a lawful position to observe the evidence and if its criminal character is immediately apparent. 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

[3] 42 U.S.C §§ 2000aa–2000aa-12 (2002).

[4] 18 U.S.C. §§ 2510–2521, 2701–2711, 3121–3127 (2002).

images but also access codes or notes taped to the computer that are in plain view. **You may not, however, search a computer seized under the plain view exception and should not print the contents of the screen.** (See "Handling Computer Equipment," pages 12–14.) Obtain a warrant to search the hard drive, disks, peripherals, manuals, or other items, based on the probable cause that the computer contains visual depictions of child pornography.

Consent to search

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

- The age of the person giving consent.
- That person's mental capacity—including educational level and intelligence—and physical condition.
- Whether the person was advised of his right to withhold consent.
- Whether the person giving consent had the proper authority to allow a search of a particular place or item.
- Whether law enforcement exceeded the scope of consent given.

Multiple users. If more than one person has access to a computer, you can usually rely on the consent of any person who has full authority over the computer. If portions of the computer have restricted access, then consent from each party with a restricted account is needed. The test to determine whether a person has the authority to consent is an objective one: Would the facts available to you at the time consent was given cause a person of reasonable caution to believe that the person who gave consent had authority over the premises and, therefore, the authority to grant consent to the search? (See sidebar, page 23.)

Scope of a consent search. A search based on voluntary consent can raise any number of issues, depending on the context of the search. Any person who consents to a search may expressly limit

Consent To Search a Computer Used by More Than One Person

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 data from the scrutiny of others. The defendant's creation of a separate directory on the computer may not provide the exclusivity necessary to prevent a search consented to by a co-user. However, if the defendant guarded the separate directory with a secret password, the court may hold that the officer needed the defendant's consent to search that particular directory.

For example, if a wife and husband use the same computer and the desk on which it is located, then the wife can consent to the search of the desk and computer by virtue of her authority by use. However, if the husband protects his files on the computer with passwords that he has not shared with his wife, then her ability to consent to the search of the computer stops at the password-protected files.

However, if the wife knows that her husband keeps his passwords to the protected files in a spiral notebook in the top drawer of the desk, she can give consent to the investigating officer to seize and examine the passwords contained in the notebook because she is a co-user of the desk. However, without a search warrant, the officer may not use those passwords to open the husband's password-protected files. Based on the discovered passwords and other probable cause, the officer can file an affidavit to obtain the search warrant necessary to open the husband's files.

As a user of the computer, the wife also can give consent to the officer to seize the computer itself. If the officer, in good faith, perceives that the computer and the evidence it contains are at risk of being destroyed or moved, exigent circumstances justify the officer's seizing the computer without the consent of the wife. However, in either of these circumstances, the officer is still prohibited from conducting a warrantless search of the husband's password-protected files.

the scope of the search to a specified area, expand the scope of the original consensual search, or withdraw their consent to the search at any time. If a person attempts to prevent you from seeing a password to encrypted data, that act limits the scope of consent to data available without the use of the password.

Permission to look around the house does not constitute, by itself, sufficient consent to search a computer in the house. If you observe Web addresses such as "lolita.com," "preteensex.com," or "altsex.com" on the computer screen in the defendant's house, that observation, by itself, does not authorize you to seize or search the computer, regardless of your training and experience. Note that a suspect's signing of a generic consent form only proves voluntary consent and is not relevant to the scope of the search.

No-knock warrant

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 alone are not sufficient to dispense with the knock and announce rule. In the majority of jurisdictions, law enforcement will need to explain specifically to the court why particular premises and/or people made it dangerous or unwise to knock and announce before a search ensued. Boilerplate computer-related concerns are not sufficient, and their use will result in suppression of any evidence obtained.

Undercover agents

Undercover agents may, without a warrant, infiltrate computer child pornography rings or bulletin board services (BBSs) that facilitate illegal activities involving the sexual exploitation of children. BBSs grant varying levels of access: (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 BBS to which they have not been granted access. A court would suppress any evidence obtained by hacking into levels that the

BBS operator has not authorized because such actions constitute a warrantless search with no recognized exception to the warrant requirement. There would also be significant civil exposure for such activities.

Summary

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. Many of the legal issues regarding searching and seizing computer evidence cannot be addressed in the space provided by this guide. However, 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 accountable for their behavior.

Contributing Authors

Daniel S. Armagh, J.D.
Director of Legal Education, Criminal Justice Division
Child Protection Training Center
Fox Valley Technical College
Appleton, WI
and
Legal Advisor, Internet Crimes Against Children Working Group
920–915–8491
darmagh@aol.com

Sergeant Nick L. Battaglia
Supervisor, Child Exploitation Unit/ICAC Task Force (retired)
San Jose Police Department
San Jose, CA
currently
Training Coordinator
Internet Crimes Against Children Task Force Program
408–690–2540
NickB1706@aol.com

Supplemental Reading

Armagh, D. 1998. A safety net for the internet: Protecting our children. *Juvenile Justice* 5(1):9–15.

Armagh, D. 2002. Virtual child pornography: Criminal conduct or protected speech? *Cardozo Law Review* 23:1993.

Child Safety on the Information Highway (pamphlet). 2005. Alexandria, VA: National Center for Missing & Exploited Children.

Federal Agency Task Force for Missing and Exploited Children. 2004. *Federal Resources on Missing and Exploited Children: A Directory for Law Enforcement and Other Public and Private Agencies*. 4th ed. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention.

Finkelhor, D., Mitchell, K.J., and Wolak, J. 2000. *Online Victimization: A Report on the Nation's Youth*. Alexandria, VA: National Center for Missing & Exploited Children.

Finkelhor, D., Mitchell, K., and Wolak, J. 2001. *Highlights of the Youth Internet Safety Survey*. (Fact Sheet.) Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention.

Medaris, M., and Girouard, C. 2002. *Protecting Children in Cyberspace: The ICAC Task Force Program*. (Bulletin.) Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention.

Thornburgh, D., and Lin, H.S., eds. 2002. *Youth, Pornography, and the Internet*. Washington, DC: National Academy Press.

U.S. Department of Justice. 2001. *Electronic Crime Scene Investigation: A Guide for First Responders*. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

U.S. Department of Justice. 2001. *Internet Crimes Against Children*. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office for Victims of Crime.

Webopedia.com (www.webopedia.com/). Online dictionary of computer terminology.

Wolak, J., Mitchell, K., and Finkelhor, D. 2003. *Internet Sex Crimes Against Minors: The Response of Law Enforcement.* Alexandria, VA: National Center for Missing & Exploited Children.

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

Organizations

Internet Crimes Against Children (ICAC) Task Force Program
Office of Juvenile Justice and Delinquency Prevention
Office of Justice Programs
U.S. Department of Justice
Washington, DC
202–305–9838
www.ojjdp.ncjrs.gov/programs/ProgSummary.asp?pi=3#Resources

ICAC Task Force Training and Technical Assistance Program
Office of Training & Technical Assistance
University of New Hampshire
Crimes against Children Research Center
Durham, NH
877–798–7682
www.icactaskforce.org

The ICAC Task Force Program helps state and local law enforcement agencies develop an effective response to Internet- and computer-related cases of child sexual exploitation. The program, which is funded by DOJ's Office of Juvenile Justice and Delinquency Prevention, encompasses forensic and investigative components, training and technical assistance, victim services, and community education. There are currently 45 regional Task Force agencies.

Federal Bureau of Investigation (FBI)
Crimes Against Children (CAC) Program
www.fbi.gov/hq/cid/cac/crimesmain.htm
(Contact the CAC coordinator at your local FBI field office.)

The FBI's CAC Program provides a quick and effective response to all incidents of crimes against children. The CAC Program investigates online child pornography/child sexual exploitation violations through the **Innocent Images National Initiative** (www.fbi.gov/innocent.htm), which enforces statutes involving possession, production, and/or distribution of child pornography facilitated by an online computer; interstate travel for sexual activity with a minor facilitated by the use of an online computer; and sexual exploitation.

U.S. Immigration and Customs Enforcement (ICE)
Office of Investigations: Investigative Services Division
Cyber Crimes Center
866–DHS–2ICE
www.ice.gov/about/investigations/services/cyberbranch.htm

The mission of the Cyber Crimes Center includes combating the exploitation of children, child pornography, and child sex tourism by targeting individuals and organizations involved in the exploitation of children via the Internet. ICE Computer Forensic Agents (CFAs) in field offices throughout the United States assist case agents and can provide support to state and local law enforcement.

National Center for Missing & Exploited Children (NCMEC)
Alexandria, Virginia
800–THE–LOST (800–843–5678)
703–274–3900
www.missingkids.com
www.cybertipline.com

NCMEC operates a 24-hour hotline and the **CyberTipline,** an online service for reporting Internet-related child sexual exploitation. NCMEC also provides a wide range of free services, including technical case assistance, link and pattern analysis on cases, forensic assistance, and educational material and publications. NCMEC's training series called Protecting Children Online offers courses designed specifically for investigators, unit commanders, and prosecutors.

U.S. Secret Service
Forensic Services Division (FSD)
www.secretservice.gov/forensics.shtml
(Contact the field office in your state.)

FSD provides forensic/technical assistance to federal, state, and local law enforcement agencies, the Morgan P. Hardiman Task Force, and NCMEC. FSD forensic examiners provide analysis for questioned documents, fingerprints, false identification, credit cards, and other related forensic science areas. The division coordinates photographic, graphic, video, and audio and image enhancement services and voice identification and forensic hypnosis programs. FSD also manages the Secret Service's polygraph program nationwide.

U.S. National Central Bureau (USNCB) of INTERPOL
U.S. Department of Justice
Washington, DC
202–616–9000
www.usdoj.gov/usncb/

USNCB serves as a point of contact for both American and foreign police seeking assistance in criminal investigations that extend beyond their national boundaries. USNCB extends assistance equally to all U.S. federal, state, and local enforcement agencies, as well as to police authorities in INTERPOL member countries.

U.S. Postal Inspection Service
www.usps.com/postalinspectors/
(Contact your local Postal Inspector's office.)

The U.S. Postal Inspection Service conducts undercover operations to investigate individuals who use the Internet or a bulletin board service to exchange child pornography or who correspond with others who do the same.

Child Exploitation and Obscenity Section (CEOS)
Criminal Division
U.S. Department of Justice
Washington, DC
202–514–5780
202–514–1793 (fax)
www.usdoj.gov/criminal/ceos/index.html

CEOS 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. Section attorneys work with U.S. Attorneys on child exploitation cases across the country, providing litigation and support services.

National Clearinghouse on Child Abuse and Neglect Information (NCCAN)
Washington, DC
800–394–3366
703–385–7565
nccanch.acf.hhs.gov/

NCCAN houses the nation's largest collection of information on child maltreatment and related child welfare issues. The Clearinghouse offers summaries and analyses of state laws concerned with child abuse and neglect and child welfare and access to searchable databases. NCCAN publications are available both online and in print.

Titles in This Series

Currently there are 14 Portable Guides to Investigating Child Abuse. To obtain a copy of any of the guides listed below, order online at puborder.ncjrs.gov or call the National Criminal Justice Reference Service at 800–851–3420.

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

Burn Injuries in Child Abuse, NCJ 162424

Child Neglect and Munchausen Syndrome by Proxy, NCJ 161841

Criminal Investigation of Child Sexual Abuse, NCJ 162426

Diagnostic Imaging of Child Abuse, NCJ 161235

Forming a Multidisciplinary Team To Investigate Child Abuse, NCJ 170020

Interviewing Child Witnesses and Victims of Sexual Abuse, NCJ 214124

Investigating Child Fatalities
NCJ 209764

Law Enforcement Response to Child Abuse, NCJ 162425

Photodocumentation in the Investigation of Child Abuse, NCJ 214123

Recognizing When a Child's Injury or Illness Is Caused by Abuse, NCJ 214125

Sexually Transmitted Diseases and Child Sexual Abuse, NCJ 160940

Understanding and Investigating Child Sexual Exploitation, NCJ 162427

Use of Computers in the Sexual Exploitation of Children, NCJ 214167

Notes

Additional Resources

American Bar Association (ABA) Center on Children and the Law
Washington, D.C.
202–662–1720
www.abanet.org/child/home.html

American Humane Association
Englewood, Colorado
303–792–9900
www.americanhumane.org

American Medical Association (AMA)
Chicago, Illinois
800–621–8335
www.ama-assn.org

American Professional Society on the Abuse of Children (APSAC)
Charleston, South Carolina
877–402–7722
apsac.fmhi.usf.edu

Federal Bureau of Investigation (FBI)
202–324–3000
www.fbi.gov

National Center for the Analysis of Violent Crime
www.fbi.gov/hq/isd/cirg/ncavc.htm

Crimes Against Children Program
www.fbi.gov/hq/cid/cac/crimesmain.htm

Juvenile Justice Clearinghouse (JJC)
Rockville, Maryland
800–851–3420
www.ojjdp.ncjrs.gov/programs/ProgSummary.asp?pi=2

Kempe Children's Center
Denver, Colorado
303–864–5300
www.kempecenter.org

Missing and Exploited Children's Training Program
Fox Valley Technical College
Appleton, Wisconsin
800–648–4966
dept.fvtc.edu/ojjdp

National Association of Medical Examiners
Atlanta, Georgia
404–730–4781
www.thename.org

National Center for Missing and Exploited Children (NCMEC)
Alexandria, Virginia
800–THE–LOST
703–274–3900
www.missingkids.com

National Center for Prosecution of Child Abuse
Alexandria, Virginia
703–549–4253
www.ndaa-apri.org/apri/programs/ncpca/ncpca_home.html

National Children's Alliance
Washington, D.C.
800–239–9950
202–548–0090
www.nca-online.org

National Clearinghouse on Child Abuse and Neglect Information
Washington, D.C.
800–394–3366
703–385–7565
nccanch.acf.hhs.gov

National SIDS Resource Center
McLean, Virginia
866–866–7437
www.sidscenter.org

Prevent Child Abuse America
Chicago, Illinois
312–663–3520
www.preventchildabuse.org

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

OJJDP Portable Guide

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