Volume 11 Number 4 Winter 1998

# APSAC ADVISOR

AMERICAN PROFESSIONAL SOCIETY ON THE ABUSE OF CHILDREN

# SPECIAL ISSUE: CHILDREN AND THE INTERNET

## Introduction

by Debra Whitcomb, MA
Editor in Chief

With the advent of new technology come new ways to abuse it. Polaroid cameras and home video cameras have long been used to record sexual exploits, legal and illegal, deviant and mainstream. Computers are no different. As technology becomes more sophisticated and accessible, techno-savvy individuals are finding the dark side and using it to fuel illegal activities. Among the most heavily publicized criminal uses of computer technology are the production and transmission of child pornography; the distribution of pornographic, obscene, and otherwise objectionable material to children; and online solicitation of children for sexual purposes.

The threats to children are quite real but poorly understood. The phenomenon is relatively new and there are not yet published studies to describe its magnitude, define the characteristics of victims and perpetrators, understand the impact on children, or recommend strategies for prevention or intervention. Current thinking suggests, however, that "cyber-molesters" are not a new breed of offender, but rather the same individuals who are simply using a new medium.

In this special issue of *The Advisor*, we have compiled a selection of articles exploring online threats to children from several angles.

- The Perspectives column, contributed by Shari Steele, staff attorney with the Electronic Frontier Foundation, explains why civil liberties and free speech advocates are troubled by the First Amendment issues raised by government's attempts to protect children from unwanted material online.
- Michelle Jezycki, Internet Crimes Against Children coordinator with the National Center for Missing and Exploited Children, provides an overview of the topic and current federal initiatives to combat these crimes.
- Ken Lanning, Supervisory Special Agent with the FBI, examines offender and victim characteristics.
- Former prosecutor Patricia Toth and Kathy McClure, of the US Department of Justice Child Exploitation and Obscenity Section, summarize some of the legal issues that differentiate computer cases from other cases of child sexual abuse and exploitation.
- Danielle Gallo, senior technical associate at AT&T Labs-Research, explains the benefits and limitations of several software tools that are available to block or filter children's access to online material.
- Deirdre Mulligan, staff attorney with the Center for Democracy and Technology, reviews online threats to children's privacy and current efforts to establish effective and constitutionally valid protective mechanisms.

Also, the Case Conference, which was submitted by Det. Jim McLaughlin of the Keene (NH) Police Department, is a composite case involving an adolescent male who is arrested for sending child pornography to an undercover investigator. Responding to this case are Daniel Armagh, Director of the National Center for Prosecution of Child Abuse, and forensic psychologist Craig Latham.

Finally, the Policy Watch column reports on the status of federal efforts to legislate protections for children.

These articles present an array of issues that together represent contemporary understanding of online threats to children. We hope this issue of *The Advisor* can serve as a valuable reference for APSAC members and other readers as we venture onto the information superhighway and strive to make it safe for children.

# Why Child Welfare Professionals Should Think Twice Before Calling for Online Censorship

by Shari Steele, Staff Attorney, Electronic Frontier Foundation



It seems that whenever society identifies a potential threat, there are a number of people who have the knee-jerk reaction of calling on the government to make that threat illegal. Unfortunately, one of the first sacrifices people are willing to make is in the area of freedom of speech.

And so it is right now on the Internet. Under the guise of protecting children, several pieces of legislation have been passed by Congress and state legislatures, and many software products have been developed, to limit access to Internet speech. But neither the legislation nor the software protect our children from any actual threat, and the basic right to free speech for adults is in jeopardy. This article attempts to illustrate why we should be reluctant to support legislation that limits the rights of adults to access protected speech on this vital medium.

### The Wrong Solution to the Wrong Problem

Congress has come up with two strategies for combating online threats to children. The first involves legislation geared toward requiring Internet content providers to restrict access when their materials are "indecent" (under the Communications Decency Act, or CDA) or, more recently, "harmful to minors" (under the Child Online Protection Act, or CDA II). Congress's second strategy involves legislation requiring schools, libraries and other public facilities that regularly provide Internet access to children to install software that filters out offending materials. Neither of these strategies is appropriate.

The main deficiency with all of the legislative fixes that have been designed to protect our children on the Internet is that the initial problem has been improperly identified. Our societal goal is to protect children from online sexual exploitation. This includes protection from online predators, child pornography and obscene materials. But these things are already illegal, and law enforcement has been doing a good job of locating and prosecuting those who violate the law through the FBI's Innocent Images Operation [see article by Special Agent Ken Lanning] and other initiatives.

Yet in spite of what you have probably heard, neither the CDA nor CDA II do anything to increase the capability of law enforcement officers to protect children from these evils. In fact, the Justice Department told Congress that the passage of CDA II would **impede** its ability to combat child exploitation. In a memo to the House Commerce Committee before it passed CDA II, the Justice Department stated that enforcement "could require an undesirable diversion of critical investigative and prosecutorial resources that the Department currently invests in combating traffickers in hard-core child pornography, in thwarting child predators, and in prosecuting large-scale and multi district commercial distributors of obscene materials." (Sutin, 1998.)

Now you may ask, "If the enforcers of the law are saying this law will impede their ability to combat online child exploitation, what is the purpose of the law?" That is a good question. From the legislative history, it appears that Congress may have thought it was helping children, in spite of the Department of Justice's comments. (See House Report, October 5, 1998)

### A Solution Looking for a Problem

Even if we were to concede that Congress's intention was not protecting children from exploitation but rather protecting children from speech that is constitutionally protected for adults but that may be inappropriate for children, the laws are still problematic. The legislative requirements are both overbroad and under-inclusive, and the net effect is that children are still unprotected and adult speech is unacceptably burdened.

Before I continue, I want to define "indecent speech" and speech that is "harmful to minors." The provisions of the CDA and CDA II that my organization and other civil liberties groups have been challenging are not about child pornography. They are not about obscenity. They are not about sexual perversion or violence. We are concerned about efforts to limit access to material that is constitutionally protected for adults but that may be inappropriate for children, such as:

- political speech, including reports of torture;
- birth control information, including instructions for putting on a condom;
- women's health issues, including how to do a breast self-examination;
- sexual orientation information, including information for and about gay men and lesbians;
- newsworthy speech, including the Starr Report;
- sexually explicit information, including Howard Stern's books and the Kama Sutra; and
- other speech that is constitutionally protected for adults but that may be inappropriate for children.

Before crafting the CDA, Congress looked to existing legal models to help it create new law to solve the new problem of children accessing adult materials on the Internet. Congress adopted the "broadcast model" of speech regulation for Internet speech when it passed both the CDA and the CDA II. The broadcast model holds that speech that is inappropriate to minors but protected for adults can only be broadcast during times of the day when children are unlikely to be in the audience. For broadcast, this limitation was constitutionally acceptable because of the

continued on next page

continued from page 8

intrusive nature of the media, i.e., a child could flip channels and happen upon inappropriate materials accidentally. *(FCC v. Pacifica Foundation*, 1978). But Internet searches are not accidental; one has to specifically access particular materials. And since materials placed on the Internet are there 24 hours a day, a restriction on the time of day could not work for Internet communications. So Congress required Internet content providers to either screen users as they entered sites to make sure that children were not accessing adult materials or remove adult materials from their sites altogether.

But these limitations on Internet content providers go to the very heart of the First Amendment. These providers are engaging in constitutionally protected speech. There is no reasonable way to ascertain whether someone accessing a site is a minor. (CDA II suggests requiring credit cards or digital certificates for age verification, but both of these suggestions are unworkable. Many of the content providers affected by these laws have much free information available at their sites and do not require people to make a purchase before they can access a site. Credit card companies do not do verification in the absence of a transaction. Further, there is no reasonable digital certification system in place for individuals that would provide age verification at no cost. Finally, these requirements do not account for the constitutional right to anonymously access these sites.) The only way to be in compliance with the law, then, is to remove all controversial material. This dumbs down the Internet to that which is acceptable to children. And the Supreme Court has held that such dumbing down is unconstitutional in that it "burns down the house to roast the pig." (*Reno v. ACLU,* 1997, citing *Sable Communications of Cal., Inc. v. FCC*, 1989).

Requiring schools, libraries and other public facilities to install filtering software is equally problematic. There is not a single filtering software program available today that filters out every single pornographic site, let alone sites that are not pornographic but may be unsuitable for children. Furthermore, filtering software producers will not reveal their lists of blocked sites, citing trade secret concerns. But without being accountable for the sites that are being blocked, filtering software producers can block out sites for no obvious purpose, such as the Quaker Home Page that was blocked in *Mainstream Loudoun v. Board of Trustees of the Loudoun County Public Library*. [See the complaint at http://Loudoun.net/mainstream/library/complaint.htm]

## Teach Your Children Well

The Internet is an amazing source of knowledge, and the wide variety of available information enables adults and children to broaden their horizons, increasing their understanding and cultural experiences. The Supreme Court found, when striking down the first CDA, that the Internet enables everyone to have a voice in ways no other medium has done before, and therefore deserves the highest level of protection. *(Reno v. ACLU*, 1997). The beauty of the Internet is that quality of giving everyone a voice. It is that same quality that leads to calls for censorship.

Absent protection for children from online predators, child pornographers, and access to hard-core obscenity, it seems to me that this debate really comes down to how we choose to teach our children and who we choose to make those decisions. It is true that there are materials on the Internet I would not want my young children to view. I would probably be more comfortable permitting my children access to those same materials when they reached high school age. But I want to empower my children from the beginning of their Internet usage, teaching them what to do when they encounter "bad" things online, just as I teach them what to do when they encounter "bad" things on the street. The responsibility for determining what materials are appropriate for children to view should rest with the parents of those children. Taking away parental rights in exchange for government censorship is not the right way to handle this "problem."

Government intervention, while a quick fix, comes at too high a cost. Freedom of speech is simply too valuable a sacrifice. Freedom of speech enables each member of society to express his or her thoughts and realize his or her full human potential. Freedom of speech is necessary to understand all sides of a debate and know the truth. Without freedom of speech, other fundamental rights, such as the right to participate in our democracy, are meaningless (ACLU, 1997). Freedom of speech is the foundation of our government. Yet freedom of speech seems to be the first forfeiture we are willing to make when we hear frivolous claims regarding the need to protect our children.

The best way we can ensure the safety of our children is by bequeathing them a world where they are encouraged to think and speak freely. Without the ability to expose our society for its wrongs, we diminish the very lives we seek to protect.

**References**

ACLU Briefing Paper #10, 1997. http://www.aclu.org/library/pbp10.html.
FCC v. Pacifica Foundation, 438 U.S. 726 (1978).
House Report 105-775, Child Online Protection Act. (October 5, 1998)
Reno v. ACLU, 117 S. Ct. 2329 (1997).
Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 127 (1989).
Sutin, L. Anthony. (1998.) Letter to Representative Thomas Bliley, October 5,1998. Internet address: http://www.aclu.org/court/acluvrenoII_doj_letter.html.

# Letters to the Editor

# LETTERS

**To The Editor:**

I would like to congratulate Seth Goldstein and Toby Tyler on their excellent article in the Advisor (Volume 11, No. 3, 1998) on "Sexual Abuse Allegations in Custody Visitation Cases: Difficult Decisions in Divisive Divorces." As a medical expert in the evaluation of examination findings in children with suspected sexual abuse, I whole-heartedly agree with their recommendations as to how to proceed with an investigation of sexual abuse allegations.

However, I think that their recommendations should apply to ALL investigations, not just those involving custody disputes. Every worker who is charged with investigating a case of child sexual abuse should cut out this article, read it, and carry it with them.

I especially applaud the recommendation concerning medical examination: "..immediate medical examinations with colposcopic, photographic documentation are a must in every case." And: "Forensic medical evaluations should be conducted by professionals who are identified as forensic medical examiners in the child sexual abuse field."

Unfortunately, I am probably in the minority among other physicians and nurse practitioners in the field of child sexual abuse medical evaluation in this opinion. Many people feel that colposcopic examinations are not necessary, and that an adequate examination can be done without magnification. Others are not convinced that photo-documentation is necessary in every case, and that anyone who has had at least some training in examining children's genitalia can do a sexual abuse examination. A significant number of "experts" don't think there should be any certification required for forensic examiners, and do not see the need for formal subspecialty training in child sexual abuse. (See Adams, 1997).

In my experience as a consultant for attorneys on sexual abuse cases, I find that there are too many clinicians who are doing sexual abuse examinations without adequate supervision, and who obviously have not kept up with the advances in research in this field. Normal and non-specific genital and anal findings are still being called abnormal and conclusive for abuse. In cases where the child cannot give a history of what may have happened, these medical "findings" are used as evidence, and are given great weight by the courts. This is a tragedy for families equal to the tragedy of real abuse.

At the very minimum, every child who has symptoms of genital or anal pain or bleeding associated with an allegation of abuse should be examined immediately by an expert, with magnification, and with photo-documentation. Abnormal findings can be photographed, and these photographs can then be shown, mailed, or e-mailed to an expert for a second opinion before proceeding with a report (if there is no history of abuse). Every center which does forensic examinations on alleged victims of child sexual abuse should have a system for obtaining a second opinion on the presence of abnormal genital or anal findings on children they examine.

It is just as important to prevent a child from being injured by an erroneous report of abuse as it is to protect a child from further abuse.

*Joyce A. Adams, MD*
*Associate Clinical Professor of Pediatrics, University of California, San Diego*

**References**

Adams, J. (1997). The role of photo documentation of genital findings in medical evaluations of suspected child sexual abuse. *Child Maltreatment*, V.2, n.4.

---

**To The Editor:**

Goldstein and Tyler's (*Advisor*, V. 11, n. 3) description of the "types of cases" where false allegations of sexual abuse are made during the course of matrimonial litigation overlooks a major class of cases. The authors posit that a report of abuse is either "sincere, legitimate and valid" or "a deliberately malicious false allegation." In many cases, the report is neither sincere and legitimate nor deliberately false. It is, rather, based on a strategic or tactical decision to take evidence which the reporter knows or believes could evidence abuse, although the reporter has every reason to believe it does not do so in the particular case, and report it so as to prejudice the other party to the matrimonial litigation. This does not qualify as a "deliberately malicious false allegation," because the reporter has some evidence suggestive of abuse and has elected to interpret that evidence broadly rather than realistically. The party is, however, motivated, at least in substantial part by personal advantage rather than the protection of the alleged victim, making it difficult to claim this as a "sincere, legitimate and valid" report.

It is these cases which pose the most serious problem for the child protection system and which impose the greatest hardship on those subject to the allegations. It is important for the investigator not to assume "good motives" on the part of the reporters simply because the allegations are not clearly and deliberately false in all

continued on next page

continued from page 4

respects. It is the tactically exaggerated fears of the active litigant that pose the greatest danger of victimizing both the child and the accused adult, depriving them of a legitimate continuing relationship during the course of investigation and litigation of the allegations. These cases leave the accused parent without even the limited remedies that may exist in the context of maliciously false allegations.

*James B. Boskey, Professsor of Law*
*Seton Hall Law School, Newark, NJ*

**The authors respond:**

The comments of Dr. Adams and Professor Bosky demonstrate just how important it is to have interdisciplinary discourse in a forum such as the APSAC *Advisor.* Here, the medical and legal professions come together to emphasize points we were unable to cover in the body of our short article.

Yes, medical examinations should be done in all child abuse cases - the extent and depth of which to be left up to the examining medical professional. Unfortunately, medical examinations are often either ignored or prematurely discounted because of the mistaken belief that "it's too late" to conduct one, or because of distance or cost prohibitions. For the protection of children, we can't afford *not* to do medical examinations. The potential results and dispositive information they provide are too important to miss.

Yes, people do manipulate the facts in custody cases. That is what we meant by maliciously false allegations, intended to gain advantage. We use the Black's Law Dictionary definition of Malice: "Malice in law is not necessarily personal hate or ill will, but it is that state of mind which is reckless of law and of the legal rights of the citizen"(Fifth ed, 1979). Professor Bosky is also correct that one shouldn't assume that all allegations are valid, regardless of the context in which they arise. What is important to recognize, however, is that the likelihood (based upon statistical research and the personal experience of the authors) that the allegation is maliciously created is lower than most people think. One should not jump to the conclusion that the allegation is false simply because it arises in this context, a result that often happens when there is an insufficient investigation conducted. Once again, for the sake of the children, we can't afford to make improper conclusions because of insufficient investigations. Dr. Adams really said it best: "It is just as important to prevent a child from being injured by an erroneous report of abuse as it is to protect a child from further abuse."

*Seth Goldstein, Esq. and Lt. Toby Tyler*

**To the Editor:**

In the Perspectives article entitled "Religion-Based Medical Neglect and Corporal Punishment," in Vol. 11, no. 1 of the *APSAC Advisor*, Rita Swan made several statements about HHS's implementation of the Child Abuse Prevention and Treatment Act (CAPTA) prior to the 1996 reauthorization by the Congress. I would merely point out that Ms. Swan's interpretation of HHS regulations and the reasons for those regulations is inaccurate. I was Director of the National Center on Child Abuse and Neglect during the period 1991-1995. The discussions within HHS on this topic reflected the complexity of shaping policy within the context of competing interests. These included such issues as the fundamental human right of parents to rear their children, the parens patriae obligation of government to protect vulnerable children, the impact of federal laws affecting disabled persons, the impact of the federal Religious Freedom Restoration Act, the increased diversity of religious practices due to increased immigration, and the continuing development of new medical treatments for infants and children.

*David W. Lloyd*

**To the Editor:**

I was pleased to see the well-deserved congratulations to Richard Gelles, Ph.D. and Kathryn Turman in the Association News article, "APSAC Searches for New Leadership," Vol. 11, no. 3 of the *APSAC Advisor*. However, I was dismayed to see the statement that Ms. Turman's kind of energy and enthusiasm is "so rare but so needed, in our federal agencies overseeing programs designed to assist children who have been victimized."

I have been a federal employee in two such agencies for the last seven years, and a practitioner in the area of child victimization with federal employees in the Washington, DC area for at least a decade previously. I can attest to the fact that such energy and enthusiasm, and competence are not rare among such agencies at all.

*David W. Lloyd*
*U.S. Dept. of Defense*

***Editor's Note:*** *We apologize to Mr. Lloyd and any other federal employees who may have been offended by this comment. We intended only to recognize Ms. Turman's excellence and professionalism, and not in any way disparage the outstanding work done by thousands of federal employees, many of them APSAC members, on behalf of children and families. Our sincere apologies.*

# ASSOCIATION NEWS

## Board Election - Call for Nominations

APSAC is fortunate to have many wonderful volunteers who support the organization in myriad ways. Some of our most talented and dedicated volunteers are the 25 individuals who serve on APSAC's Board of Directors. Do you know of a leader in the field of child maltreatment who has the time and interest to dedicate to a leadership position with the nation's largest interdisciplinary association for professionals in the field of child abuse and neglect? Included in this issue of the *Advisor* is a nomination form for candidates to stand for election to the board, for a three-year term beginning in June 1999. Please take a moment to consider whether you would be willing to serve, or if you know colleagues who may be interested, and complete the nomination form. Nominations must be received in the APSAC office by February 19, 1999. For more information, contact Beverly Bradley, Acting Executive Director at 312-554-0166.

## Search Committee Update

The search for APSAC's new Executive Director is making excellent progress. The ten-member Search Committee, chaired by former APSAC Board President Linda Williams, has narrowed the field of more than 70 applicants to a pool of top candidates. The Board is carefully reviewing these applicants to find an Executive Director with the right combination of skills and experience to lead the organization into its next stage of growth and development. We hope to make an announcement soon about the new leadership, and as always, thank our members for their ongoing support and assistance in locating the best possible candidate for this critically important position.

## Remember The Colloquium! Seventh National Colloquium to Meet in San Antonio

Join us in San Antonio June 2-5, 1999 in San Antonio Texas for APSAC's Seventh National Colloquium. This is one of the leading training opportunities for professionals in the field of child abuse and neglect, with more than 100 research and practice presentations on all topics related to child maltreatment. A pre-conference institute will examine the role of culture in the identification, assessment and treatment of child maltreatment. Brochures will be mailed in January – the early registration deadline (which offers a $50 discount on fees) is March 12, 1999.

## Two New Forensic Interviewing Clinics Scheduled for 1999

APSAC's Child Forensic Interview Training Clinic is a 40-hour course designed to build and improve professional skills in interviewing children. Participants learn state-of-the-art forensic interview theory, research, and techniques from nationally recognized experts and have the opportunity to practice interviewing children and receive feedback in small group settings. Two new Forensic Interview Clinics have been scheduled for the upcoming months. On March 7-13, 1999, APSAC will present a forensic interview clinic in Huntsville, Alabama in conjunction with the National Symposium on Child Sexual Abuse, sponsored by the National Children's Advocacy Center. A second clinic will be held in conjunction with the Seventh National Colloquium in San Antonio, May 30 – June 5. Both clinics will be "wrapped around" the host conference, and the registration fee includes both training events. The early registration deadline for the Huntsville clinic is January 29, 1999. Please complete the mailing list coupon on page 25 of this issue of the *Advisor*, or call APSAC at 312-554-0166.

## APSAC Launches New Member Recruitment Campaign

You know how valuable your APSAC membership is to you. Wouldn't you like to spread the word to your colleagues in the field? Our membership survey data has consistently shown that word of mouth and colleague referrals are our most successful recruiting tools. APSAC has begun a new membership drive and we are offering an incentive to members who can help us spread the word about the benefits of joining APSAC. The member who brings in the most new members between December 1 and May 31, 1999 will receive a free one year renewal, plus an APSAC t-shirt in your choice of purple or white. When recruiting new members, please have the member write your name on their application form on the "referred by" line. And remember, there is a 5% discount for five or more applications from the same agency at the same time. The winner of this membership recruitment contest will be announced at the annual Membership Luncheon, held at the 7th National Colloquium in San Antonio. For more information, please contact Beverly Bradley at 312-554-0166, or e-mail at APSACExec@aol.com.

## APSAC Advanced Training Institutes To Be Held In Atlanta

Each January, in conjunction with the San Diego Conference on Responding to Child Maltreatment, APSAC offers six-hour intensive advanced level training institutes taught by leading experts in the field. On Sunday, July 25 APSAC will offer these high quality training events in Atlanta, Georgia, in partnership with the Georgia Council on Child Abuse's 15th Annual Training Symposium. Eight concurrent six-hour sessions will be offered. For more information, please call the Georgia Council on Child Abuse at 404-870-6565.

## Call For Nominations for APSAC Awards

Included with this issue of the Advisor is a nomination form for APSAC's annual awards. These awards honor the outstanding work done by professionals in the field of child abuse and neglect. Winners of the awards will be announced at the Membership Luncheon, held at the Colloquium in San Antonio. The deadline for the awards nominations is April 1, 1999.

## Call for Comment - Investigative Interviewing Practice Guidelines

The APSAC Task Force on Investigative Interviewing has drafted proposed Practice Guidelines which are now available for member comment. These guidelines address such issues as the requisite training and discipline of the interviewer, the timing and location of the interview, documentation of the interview, the use of interview aids and other important areas. APSAC members play a critical role in the development of Practice Guidelines, and we invite all interested members to request a copy of this draft for review and comment. To request a copy, please call the APSAC Publications department at 312-554-0166, or fax a written request to 312-554-0919. You may also e-mail APSACPubls@aol.com, or download the draft Guidelines from the APSAC Web site at www.apsac.org. All comments must be received by February 28, 1999.

# A Glossary of Internet and Online Terms

Adapted and reprinted with permission from the National Criminal Justice Reference Service

**BBS** (Bulletin Board System): A computerized meeting and announcement system that allows people to carry on discussions, upload and download files, and make announcements without the people being connected to the computer at the same time. There are many thousands (millions?) of BBS's around the world, most are very small, running on a single IBM clone PC with I or 2 phone lines. Some are very large and the line between a BBS and a system like CompuServe gets crossed at some point, but it is not clearly drawn.

**BPS** (Bits-Per-Second): A measurement of how fast data is moved from one place to another. A 28.8 modem can move 28,800 bits per second.

**Browser:** A Client program (software) that is used to look at various kinds of Internet resources.

**Chat:** A system that allows for real-time communication between users of a computer, who may be logged onto the Internet (using Internet Relay Chat, or IRC) or onto an online service, such as American Online, which has "chatrooms".

**Cyberspace:** Term originated by author William Gibson in his novel *Neuromancer.* The word Cyberspace is currently used to describe the whole range of information resources available through computer networks.

**E-mail** (electronic mail): Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses (mailing lists).

**FAQ** (Frequently Asked Questions): FAQs are documents that list and answer the most common questions on a particular subject. There are hundreds of FAQs on subjects as diverse as Pet Grooming and Cryptography. FAQs are usually written by people who have tired of answering the same question over and over.

**FTP** (File Transfer Protocol): Internet protocol (and program) used to transfer files between hosts.

**Hit:** As used in reference to the World Wide Web, "hit" means a single request from a web browser for a single item from a web. "Hits" are often used as a very rough measure of popularity of a particular document or site, e.g, "Our website has been getting 300,000 hits per month."

**Home Page** (or Homepage): The most common meaning refers to the main web page for a business, organization, person.

**HTML** (HyperText Markup Language): a language (or format) used for creating hypertext documents on the World Wide Web. This is the format used to create Web pages.

**HTTP** (HyperText Transport Protocol): an information retrieval mechanism for HTML documents.

**Internet:** A collection of networks interconnected by a set of routers which allow them to function as a single, large virtual network.

**IRC** (Internet Relay Chat): Basically a huge multi-user live chat facility. There are a number of major IRC servers around the world which are linked to each other. Anyone can create a channel and anything that anyone types in a given channel is seen by all others in the channel. Private channels can (and are) created for multi-person conference calls. A user can log onto the IRC anonymously, and "chat" with other users without any identifying personal information being obvious. IRC chatrooms are one place where pedophiles meet to trade stories, and it is also a place where children may be at risk of being "lured".

**ISP** (Internet Service Provider): An institution that provides access to the Internet in some form, usually for money.

**Listserv:** The most common kind of mail list, Listservs originated on BITNET but they are now common on the Internet.

**Login:** Noun or a verb. Noun: The account name used to gain access to a computer system. Not a secret (contrast with Password), Verb: The act of entering into a computer system, e.g. Login to America Online and then go to the GBN conference.

**Mail List** (or Mailing List): A (usually automated) system that allows people to send e-mail to one address, whereupon their message is copied and sent to all of the other subscribers to the maillist. In this way, people who have many different kinds of e-mail access can participate in discussions together.

**Modem:** A device that you connect to your computer and to a phone line, that allows the computer to talk to other computers through the phone system, Basically, modems do for computers what a telephone does for humans.

**Newsgroup:** The name for discussion groups on USENET.

**Online:** To be connected, by way of a modem, to the Internet or other networks, such as American Online. While online services such as American Online, CompuServ and Prodigy now offer access to the Internet, they also provide their own content, chatrooms, newsgroups and other material which is accessible only to other subscribers of that online service.

**Password:** A code used to gain access to a locked system. Good passwords contain letters and non-letters and are not simple combinations such as virtue7. A good password might be: Hot$1-6

**USENET:** A world-wide system of discussion groups, with comments passed among hundreds of thousands of machines. Not all USENET machines are on the Internet, maybe half. USENET is completely decentralized, with over 10,000 discussion areas, called newsgroups.

**WWW** (World Wide Web): Two meanings - First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers) which are the servers that allow text, graphics, sound files, etc. to be mixed together.

# POLICY WATCH

## Protecting Children Online: The Congressional Response

by Thomas L. Birch, J.D., Legislative Counsel, National Child Abuse Coalition

Legislation to protect children's safety on the Internet had high visibility on the 1998 congressional agenda. While the legislative record on children's issues this year may be remembered as indifferent at best, legislators persisted in pushing measures to guard children from connecting to sexually oriented Web sites or falling prey to sexual predators on line.

Two years ago, Congress pursued some of the same issues. Enacted in 1996, the Communications Decency Act (CDA) established a national indecency standard for enforcement on Internet material that the Supreme Court then struck down as unconstitutionally vague and overly broad. Several of the current measures addressing the issue of children's safety online aim at imposing regulations on Internet material without running up against constitutional objections.

### Blocking Pornography

In the last week of October 1998, Congress passed the Child Online Protection Act, a bill designed to restrict minors' access to adult sexual material on the Internet. The new legislation, sponsored by Rep. Michael G. Oxley (R-OH) and Sen. Dan Coats (R-IN), would replace the CDA's broad "indecency" standard with what legislators claim is a more widely recognized standard, "harmful to minors". The Child Online Protection Act would make it a crime for commercial Web site operators to post "material that is harmful to minors" without blocking access to the site through a credit card requirement or other adult verification. Violators risk penalties of up to $50,000 in fines and six months in prison.

According to Rep. Oxley, more than 60,000 Web sites featuring sexually explicit and obscene material are available to children. Speaking in support of the bill on the House floor, Oxley explained, "While the Internet can be a positive tool for the education and entertainment of our children, it can also be a window to the dark world of pornography. Minors can readily access obscene material intentionally or unintentionally and be lured into dangerous situations. Children cannot safely learn in a virtual red light district. A child may innocently search for key words like 'dollhouse,' 'toys' or 'pet,' and be led into numerous sexually explicit sites."

The Child Online Protection Act defines harmful material as anything of a sexual nature that is obscene or that "the average person, applying contemporary community standards" finds, "with respect to minors", appeals to "the prurient interest", and taken as a whole, lacks serious literary, artistic, political, or scientific value "for minors."

Supporters of the Child Online Protection Act suggest that the now widespread availability of the Internet presents opportunities for minors to access materials through the World Wide Web "in a manner that can frustrate parental supervision or control." The bill's sponsors claim that the online industry's efforts to help parents and educators restrict potentially harmful material have not provided a "national solution to the problem of minors accessing harmful material on the World Wide Web." Rep. Oxley argued for the sanctions despite the availability of blocking software, which he said was useful but "cumbersome and frequently ineffective."

Although the House of Representatives passed the online protection measure by voice vote, even some of its supporters, such as Rep. Edward J. Markey (D-MA), expressed doubts about the bill's practical application: "The standard in the bill before us today is `harmful to minors,' much narrower than the Communications Decency Act. Yet like the CDA, the bill would propose a national standard rather than a community-based standard of what harmful to minors means. The legislation before us raises a number of difficult policy questions, such as whether a policy of community-by-community-based standards of harmful to minors is at all possible in a global medium, and whether the Internet requires national treatment for what is harmful to minors across the country." (For more details about The Child Online Protection Act, see Toth and McClure's article on page 19.)

### Protecting Personal Information

In addition to provisions designed to restrict children's access to adult Web sites, the Child Online Protection Act includes a second set of protections authored by Markey prohibiting the public posting of children's identifying information in chat rooms and other online forums, such as a home page of a website, a pen pal service, or a message board. The bill requires that online operators prominently announce on their sites what information they are collecting, with parental consent, from children and how they will use it. Operators would also be barred from inducing children through games and contests to provide personal information. The new law would allow children to seek and receive information without parental consent provided the information is only used for the purpose of answering a child's inquiry. (See Mulligan's article in this issue for details on privacy concerns online.)

### Constitutional Questions Raised

While the privacy of information proposals generally enjoyed universal support from online service providers and free speech advocates, the legislative proposal to restrict online speech that is "harmful to minors" is more controversial. Civil liberties groups warn that the measure would chill free speech. It is argued that defining a national, "harmful to minors" standard for Internet speech would wrongfully replace local authority to determine what materials are appropriate for minors, putting the federal government in the position of deciding what people should be able to see online. Commercial online providers complain

continued on next page

## Policy Watch

continued from page 7

that the provisions are too broad and would unintentionally block a wide range of otherwise innocent information. As soon as the legislation passed Congress, online technology interest groups vowed to go back to court to challenge the new law as was done successfully with the Communications Decency Act.

The U.S. Department of Justice, in a letter to the chair of the House Commerce Committee with jurisdiction over the legislation, expressed the Clinton administration's concerns about the Child Online Protection Act. For one, the enforcement of a new criminal prohibition would require, according to the Justice Department, an "undesirable diversion" of investigative resources. Through the "Innocent Images" online undercover operation begun by the FBI in 1995, agents are already assigned, according to the Justice Department's letter, to combat traffickers in child pornography and other commercial distributors of obscene materials and in thwarting child predators by going online to investigate predators victimizing children through the Internet and online service providers.

***As soon as the legislation passed Congress, online technology interest groups vowed to go back to court to challenge the new law as was done successfully with the Communications Decency Act.***

The Justice Department also anticipates the likelihood of constitutional challenges to the new law. Because the Child Online Protection Act proposes the establishment of a commission to study the ways in which the problem could be most effectively addressed, the Justice Department advised Congress to wait until the commission is established and has completed its study, with legislative recommendations, before determining whether a criminal statute would be necessary.

**Issues Persist**

Other measures protecting children's safety online were proposed in Congress this year:

The Internet School Filtering Act, S. 1619, authored by Sen. John McCain (R-AZ), would require schools and libraries to install filtering software if they received federal subsidies for computer links. The bill easily passed the Senate, but it also drew opposition from civil liberties groups and from educators and librarians. The American Library Association advised against a federal mandate to require local filtering or blocking software and opposed linking the requirement to eligibility for the telecommunications subsidy program. Opponents argued that the mandated safeguards proposed by McCain usurp the ability of local communities to set standards reflecting their own values.

An approach proposed by Sen. Christopher Dodd (D-CT) fared better, enjoying support from all sides. Dodd's measure would require Internet providers to make screening software available whenever Internet access is purchased.

The Protection of Children from Sexual Predators Act, S.2491, sponsored by Sen. Orrin Hatch (R-UT), would require Internet service providers to report to law enforcement officials any information regarding the transmission of child pornography. The measure also proposes criminal fines and imprisonment for individuals found to use the Internet or electronic mail to entice children to engage in sexual activity. Recognizing the difficulty of drafting federal restrictions on Internet communications that meet constitutional requirements, the Hatch bill also mandates a study by the National Academy of Sciences on the ability to develop blocking technologies which can effectively control the transmission of pornographic images.

The effort to protect children's safety online will no doubt remain a legislative issue in the coming year, especially with a lack of consensus and agreement around the most effective approaches for shielding children from pornography and enticement to sexual activity over the Internet. The National Center for Missing and Exploited Children has developed a CyberTipline to serve as a national reporting service for leads on the sexual exploitation of children in cyberspace. Still, the industry balks at legislation which would require service providers to report suspected violations to the police, similar to child abuse reporting laws which mandate various professionals, including film processors in some states, to report suspected cases of child maltreatment to protective services. At present, the only action taken is removal of the offending Web site from the Internet provider's service.

All agree that the use of credit cards and related techniques would help to protect children from adult materials. There is also general agreement on the need for more sophisticated filters and blocking systems, which could include the creation of new domain names for "adult" material, leading to more effective filtering of other information produced during a search on the World Wide Web. However, much remains to be done if children are to be kept safe, especially from predators who stalk the chat rooms and entice children through email, where filtering systems have no impact.

## MOVING?

Please notify the office in plenty of time so you don't miss any issues of the *APSAC Advisor* or *Child Maltreatment.*

Now you can e-mail us your change of address: APSACmems@aol.com

# How Safe is Cyberspace: An Overview

Michelle Jezycki, National Center for Missing and Exploited Children

FEATURE

- *Child Lured By Predator Online.*
- *Feds Seize Computers and Software In International Child Porn Sting.*
- *Computer Repair Shop Reports Kiddie Porn to Local Authorities.*

Headlines like these are all too common in this, the Information Age. Rarely can one open a newspaper and not find an article detailing the illicit use of computers and the Internet. While this new medium has offered opportunities for children and adults alike to search libraries, peruse international galleries, chat with friends and family, and purchase books, music, and games with a click of the mouse, it has also availed its strengths to those who prey on children. This "darker side" of the Internet has allowed criminals to meet, network, and commit crimes stretching across state and even international boundaries. The Information Superhighway is not patrolled by a local police department preventing crimes within its jurisdiction. The speed of modems, incredible advances in modern technology, and the number of users online have blurred traditional jurisdictional boundaries. With these new challenges facing law enforcement, thousands are left asking, "Whose job is it to protect our children online?"

***Forecasters predict approximately 45 million households will have Internet access by the Millennium, and recent figures indicate that currently 10.5 million children use online services.***

It is estimated that approximately 30 million U.S. households have computers in their homes. Of these, 10 to 15 million have the capability to go online. Forecasters predict approximately 45 million households will have Internet access by the millennium, and recent figures indicate that currently 10.5 million children use online services. The usage time by teens 16-17 years of age illustrates that 32% of these youth spend five or more hours online per week. (Pike, 1998).

In a time when parents are relying on children to program VCRs, online usage by children often goes misunderstood by adults. Many parents' inability to operate a computer, let alone navigate the Internet and World Wide Web, has created an electronic daycare for children worldwide. Many parents believe that their children are safe in their own home while on the computer; however, the growing number of Internet crimes against children indicates a need to reevaluate that sense of security.

Online subscribers can now establish electronic mail accounts (e-mail) free of charge and use them to send and receive messages with users worldwide, reaching into the living rooms, bedrooms, and homes of families around the globe. "Chat" rooms attract millions of visitors daily, with every topic from Fans of Barney to Adult Sexual Encounters, and virtually no one "checking for ID" at their doors. Many people believe that children are safe in rooms with more juvenile topics, such as Teen Idols and Barbie Chat, when in fact predators can be lurking in these seemingly benign "neighborhoods" on the Internet. Newsgroups and, Bulletin Boards, and the World Wide Web are flooded daily with postings of "free pics" and "teenage sex" topics, luring the curious to download or trade the files, or engage in further conversation. One may scroll through the thousands of listings in these news groups or in chat rooms as early as 6:00 am and find people from all over the world, engaged in a particular, explicit, perversion online. Has the Information Age created a new type of criminal that law enforcement must combat? Has it created a new crime that traditional law enforcement is ill-equipped to handle? The answer, simply put, is no.

Crimes against children have occurred for decades, if not centuries. For years children have been dubbed as "perfect victims." They are often too trusting, seeking attention, affection, or material possessions, and most of all are often not viewed as credible witnesses. The same assumptions apply today. The online predator now has the ability to invisibly or anonymously lure children from the confines of his or her own home, collecting information from children online, searching profiles of potential victims, and gathering an arsenal of personal information on specific children within a few moments. The process of victimization, however, remains the same. Using information gathered online, the perpetrator targets a child victim. An online friendship is initiated with the child, which includes shared hobbies and interests, and possibly leads to the sending of gifts and pictures. The online predator may groom the child, all the while building trust until eventually even attempting to arrange for a meeting. Child Exploitation Units in law enforcement have battled this traditional grooming process for years, long before the emergence of the Internet and World Wide Web. The new challenge is simply applying the same investigative, interviewing, and interrogation skills to Internet crimes against children, where playgrounds must now include chat rooms. Same crime, different medium.

Understanding this assimilation, it becomes apparent that law enforcement must have the support of communities, businesses, technology, parents, and state, local and federal government to successfully make this electronic transition. Many blocking and screening tools have been created (see the article in this issue by Gallo); however, the rapid growth of the Information Age makes it virtually impossible to keep

continued on next page

continued from page 10

these devices adequately updated. Many communities have applied a multi-disciplinary approach to resolving these cases, while others have relied more heavily on federal support when faced with a potential Internet child exploitation case. Several state and local task forces have been created to take a preventive approach to protecting children online, some even conduct online undercover operations. But, where else can communities turn for assistance?

**Resources For Communities**

In December 1997, approximately 650 participants representing 300 organizations gathered for the Internet Online Summit: Focus on the Children. The Summit addressed ways to make the Internet a safe and educational experience for children. Attorney General Janet Reno addressed the summit and spoke of the U.S. Department of Justice's commitment to assist local, state, and federal initiatives to enhance the safety of children online. Since the summit much progress has been made.

The National Center for Missing and Exploited Children (NCMEC) created the Exploited Child Unit (ECU) as a cooperative agreement between the U.S. Department of Treasury and NCMEC. ECU maintains and has access to several databases containing valuable information, including law enforcement personnel with expertise in the field of child exploitation, state and federal task forces, public records, and private sector resources.

Another function of the ECU is to operate NCMEC's CyberTipline, www.missingkids.com/cybertipline, funded by the U.S. Department of Justice. The CyberTipline, established in March 1998, handles online leads from individuals reporting the sexual exploitation of children. The reports coming from children and adults alike have totaled more than 2,600 to date. Reports include information on child pornography, child prostitution, child sexual tourism, extra-familial child sexual exploitation, and online enticement of children. The form at this site enables the user to report information on the inappropriate behavior of an online user, a particular web site, or any incident where the individual is or believes that someone else may be in danger. Once completed, the form is sent electronically to ECU analysts who review and validate the reports before submitting them to the appropriate law enforcement agency for investigation and follow-up. The ECU has developed software programs to help law enforcement agencies obtain investigative information on the Internet. The ECU has also produced informative publications for children, parents, and communities nationwide on the topic of child and teen safety on the Information Highway.

NCMEC has developed two training programs to assist professionals with the identification and investigation of Internet crimes against children. Protecting Children Online is a four and one-half day course administered by Fox Valley Technical College, and delivered regionally throughout the country. The Protecting Children Online-Unit Commander course is a two and one-half day course offered at NCMEC in Arlington, Virginia. The course is directed towards developing or enhancing child exploitation units to include Internet crimes against children.

The Office of Juvenile Justice and Delinquency Prevention (OJJDP) of the U.S. Department of Justice has also made a commitment to help local law enforcement address the problem of Internet crimes against children. OJJDP recently awarded ten communities grants of up to $300,000 each to create or enhance local and state task Forces to combat Internet crimes against children.

Additional federal responses and resources for protecting children online include the FBI, U.S. Customs Service, and the U.S. Postal Inspection Service. Each of these federal law enforcement agencies works in concert with NCMEC's CyberTipline.

The FBI's Innocent Images Operation located in Calverton , Maryland, has been designated as the FBI's central operation for all online child pornography/child sexual exploitation investigations. The United States Customs Service International Child Pornography Investigation and Coordination Center acts as the front line defense to combat the illegal generation, importation, and proliferation of child pornography. The U.S. Postal Inspection Service also assists in the fight to protect children online by dealing with the transmission of child pornography by use of the United States mail. With the emergence of illicit web sites advertising child pornographic material for sale, the U.S. Postal Service has been instrumental in tracking down such purchases that are sent by mail.

With such emphasis being placed on the importance of combating crimes against children online at the local, state, and federal levels, it is crucial that these efforts exist and progress collaboratively with one another. Clearly the responsibility of preventing and resolving Internet crimes against children is not merely a federal or a local issue. Technology has demonstrated it to be a global responsibility, a border-less crime. By utilizing the available training initiatives, drawing from the experience of successful task forces and units, informing communities and agencies about the many existing resources available, and having parents taking a more active role, perhaps we can make the journey through cyberspace safer for children.

**Reference**

Pike, J. (1998), Cyberstats, Federation of American Scientists. www.fas.org/netstats.htm

# Cyber "Pedophiles": A Behavioral Perspective

By Supervisory Special Agent Kenneth V. Lanning
FBI Academy
Quantico, VA

## Introduction

Throughout history, individuals who sexually victimize children have frequented the places where children gather. School yards, parks, and malls have been prime contact places. Offenders have also used technological advancements (e.g., cameras, telephones, automobiles, etc.) to facilitate their sexual interests and behavior. In the 1990's, home computers, online services, and the Internet have become new points of contact and new technological tools. We have historically warned our children about the dangers associated with strangers, but often neglected to help them understand that sex offenders are often people they have come to know either in person or now online.

***Some offenders use the computer primarily to collect and trade child pornography, while others also seek online contact with other offenders and children.***

Like many molesters, individuals attempting to sexually exploit children through the use of computer online services or the Internet tend to gradually seduce their targets with attention, affection, kindness, and gifts. They are often willing to devote considerable amounts of time, money, and energy to this process. They will listen to and empathize with the problems of children. They will be aware of the music, hobbies, and interests of children. Unless the victims are already engaged in sexually explicit computer conversation, offenders will usually lower any inhibitions by gradually introducing the sexual context and content. Some offenders use the computer primarily to collect and trade child pornography, while others also seek online contact with other offenders and children.

Children, especially adolescents, are often interested in and curious about sexuality and sexually explicit material. They will sometimes use their online access to actively seek out such material. They are moving away from the total control of parents and trying to establish new relationships outside the family. Sex offenders targeting children will use and exploit these characteristics and needs. Adolescent children may also be attracted to and lured by online offenders closer to their age who, although not technically "pedophiles," may be dangerous.

## Illegal Sexual Activity

Computer-related sexual exploitation of children usually comes to the attention of law enforcement as a result of citizen/victim complaints, referrals from commercial service providers, or inadvertent discovery during other investigations. Cases are also proactively identified by undercover investigations that target high risk computer sites or utilize other specialized techniques.

Sexual activity involving the use of computers that is usually illegal and therefore the focus of law enforcement investigations includes:

1. Producing or possessing child pornography
2. Uploading and downloading child pornography
3. Soliciting sex with "children"

Using the computer to solicit sex with "children" could include communicating with actual children as well as with law enforcement officers taking a proactive investigative approach and pretending to be children or pretending to be adults with access to children. After using the computer to make contact with the "child," other illegal activity could involve traveling to meet the child or having the child travel to engage in sexual activity.

One problem area for the criminal justice system are cases involving adolescents who use the computer to solicit sex with other adolescents and to traffic in child pornography that portrays pubescent "children." For purposes of child pornography and illegal sexual activity, the Federal statutes and many local statutes define children or minors as individuals who have not yet reached their eighteenth birthday. Therefore, such behavior may be technically illegal, but may not be sexually deviant.

## Legal Sexual Activity

Sexual activity involving the use of computers that is usually legal includes:

1. Validating sexually deviant behavior and interests
2. Reinforcing deviant arousal patterns
3. Storing and sharing sexual fantasies
4. Lying about one's age and identity
5. Collecting adult pornography that is not obscene
6. Disseminating "indecent" material, talking dirty, providing sex instructions, "cyber-sex," etc.
7. Injecting oneself into the "problem" of computer exploitation of children to rationalize one's interests

Although many might find much of this activity offensive and repulsive, and special circumstances and specific laws might even criminalize some of it, it is for the most part legal activity.

## Understanding Behavior

The investigation of child sexual exploitation cases involving computers requires knowledge of the technical, legal, and behavioral aspects of computer use. However, because each of these areas is so complex, investigators must also identify experts and resources available to assist in these cases. Exploitation cases involving computers present many investigative challenges, but they also present the opportunity to obtain a great deal of corroborative evidence and

continued on next page

# Cyber Pedophiles

continued from page 12

investigative intelligence. This discussion will focus primarily on the dynamics of offender and victim behavior in the computer exploitation of children.

## Offenders

The general public, the media, and many child abuse professionals sometimes simplistically refer to all those who sexually victimize children as pedophiles. There is no single or uniform definition for the word "pedophile." For mental health professionals and as defined in the DSM-IV, it is a diagnostic term referring to those with recurrent, intense sexually arousing fantasies, urges, and behaviors involving prepubescent children (American Psychological Association, 1994). For most, however, it is just a fancy word for a child molester. Are all child molesters pedophiles? Are child molesters with adolescent victims pedophiles? Are individuals who use the Internet to collect and obtain both child and adult pornography pedophiles?

As I use the term, pedophiles are individuals whose erotic imagery and sexual fantasies focus on children. They do not "settle" for child victims, but, in fact, prefer to have sex with children.

***To avoid confusion with a mental health diagnosis and possible challenges in court, use of the term "pedophile" by law enforcement should be kept to a minimum.***

Not everyone using a computer to facilitate having sex with children or trafficking in child pornography is a pedophile. There is no legal requirement to determine that a subject or suspect in a case is a pedophile and often it is irrelevant to the investigation or prosecution. As will be discussed, such a determination may be useful in developing a variety of investigative approaches. To avoid confusion with a mental health diagnosis and possible challenges in court, however, use of the term "pedophile" by law enforcement should be kept to a minimum. In my work and case analysis, a pedophile is just one example or sub-category of what I refer to as a "preferential sex offender." The term preferential sex offender is merely a descriptive label used only to identify, for investigative purposes, a certain type of offender.

The advantages of law enforcement using the term preferential sex offender include: (1) it is descriptive, not diagnostic; (2) it is probative, not prejudicial; (3) it can include both offenders who sexually molest children and those who "just" collect child pornography; (4) it can include offenders whose child pornography is only a small portion of their large pornography collections; and (5) it can include those with preferences for adolescent victims and for adolescent pornography (e.g., hebephiles, ephebophiles). How to recognize and identify such offenders will be discussed shortly.

## Computer Offenders

Offenders using computers to sexually exploit children usually fall into two broad categories:

1. Situational Offender (Dabbler) - Usually either a typical adolescent searching online for pornography and sex or an impulsive/curious adult with a newly found access to a wide range of pornography and sexual opportunities. When they break the law, such dabblers can obviously be investigated and prosecuted, but their behavior is not as long-term, persistent, and predictable as that of preferential offenders.

2. Preferential Offender - Usually either a sexually indiscriminate with a wide variety of deviant sexual interests or a "pedophile" with a definite preference for children. The main difference between them is that the pornography/erotica collection of the sexually indiscriminate preferential offender will be more varied, usually with a focus on their particular sexual preferences or paraphilias, whereas a pedophile's collection will focus predominantly on children. Also, the sexually indiscriminate offender is less likely to directly molest children, especially prepubescent children.

Other miscellaneous "offenders" include: media reporters who erroneously believe they can go online and traffic in child pornography as part of a news expose; pranksters who disseminate false or incriminating information to embarrass the targets of their "dirty tricks"; older "boyfriends" attempting to sexually interact with adolescent girls or boys; and concerned citizens who go overboard doing their own private investigations into this problem. As will be discussed, investigators must be cautious of all overzealous citizens offering their services in these cases. Only law enforcement officers involved in official, authorized investigations should be conducting proactive investigation or downloading child pornography on a computer.

Although a variety of individuals sexually victimize children, preferential sex offenders are the primary sexual exploiters of children. They tend to be serial offenders who prey on children through the operation of child sex rings and/or the collection, creation, or distribution of child pornography. Using a computer to fuel and validate interests and behavior, to facilitate interacting with child victims, or to possess and traffic in child pornography usually requires the above average intelligence and economic means more typical of preferential sex offenders. The computer sex offenders discussed here tend to be white males from a middle class or higher socioeconomic background.

## Recognizing Preferential Sex Offenders

An important step in investigating sexual exploitation of children is to recognize and utilize, if present, the highly predictable sexual behavior patterns of these preferential sex offenders. If the investigation

continued on next page

continued from page 13

identifies enough of these patterns, many of the remaining ones can be assumed. However, no particular number constitutes "enough" - just a few 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.

You cannot hope to determine the type of offender with whom you are dealing unless you have the most complete, detailed, and accurate information possible. The investigator must understand that doing a background investigation on a suspect means more than obtaining the date and place of birth and credit and criminal checks. School, juvenile, military, medical, driving, employment, bank, and sex offender and child abuse registry records can also be valuable sources of information about an offender.

***Understanding sexual ritual (i.e., need-driven behavior) is the key to investigating preferential sex offenders.***

A preferential sex offender can usually be identified by the following behaviors:

1. Long-Term and Persistent Pattern of Behavior
   - A) Begins pattern in early adolescence
   - B) Is willing to commit time, money, & energy
   - C) Commits multiple offenses
   - D) Makes ritual or need-driven mistakes
2. Specific Sexual Interests
   - A) Manifests paraphiliac preferences (may be multiple)
   - B) Focuses on defined sexual interests and victim characteristics
   - C) Centers life around preferences
   - D) Rationalizes sexual interests
3. Well-Developed Techniques
   - A) Evaluates experiences
   - B) Lies and manipulates, often skillfully
   - C) Has method of access to victims
   - D) Is quick to use modern technology (e.g. computer, video) for sexual needs & purposes
4. Fantasy-Driven Behavior
   - A) Collects pornography
   - B) Collects paraphernalia, souvenirs, videotapes
   - C) Records fantasies
   - D) Acts to turn fantasy into reality

On an investigative level, the presence of paraphilias often means highly repetitive and predictable behavior focused on specific sexual interests that goes well beyond a "method of operation" (MO). The concept of MO — something done by an offender because it works and will help him get away with the crime — is well known to most investigators. An offender's MO is fueled by thought and deliberation. Most offenders change and improve their MO over time and with experience.

Preferential sex offenders' repetitive patterns of behavior involve some MO, but are more likely to also involve the less-known concept of sexual ritual. Sexual ritual is the repeated engaging in an act or series of acts in a certain manner because of a sexual need; that is, in order to become aroused and/or gratified, a person must engage in the act in a certain way. Other types of ritual behavior can be motivated by psychological, cultural, or spiritual needs. Unlike MO, ritual is necessary to the offender but not to the successful commission of the crime. In fact, instead of facilitating the crime, it often increases the odds of identification, apprehension, and conviction because it causes the offender to make need-driven mistakes.

Ritual and its resultant behavior is fueled by erotic imagery and fantasy and can be bizarre in nature. Most important to investigators, offenders find it difficult to change and modify ritual, even when their experience tells them they should or they suspect law enforcement scrutiny. Understanding sexual ritual (i.e., need-driven behavior) is the key to investigating preferential sex offenders.

Investigators must not over- or under-react to reported allegations. They must understand that not all computer offenders are stereotypical "pedophiles" who fit some common profile. Keeping an open mind and objectively attempting to determine the type of offender involved can be useful in minimizing embarrassing errors in judgment and developing appropriate interview, investigative, and prosecutive strategy. For example, the fact that preferential offenders as part of sexual ritual are more likely to commit similar multiple offenses, make need-driven mistakes, and compulsively collect pornography and other offense related paraphernalia can be used to build a stronger case.

In computer cases, especially those involving proactive investigative techniques, it is often easier to determine the type of offender than in other kinds of child sexual exploitation cases. When attempting to make this determination, it is important to evaluate all available background information. The following information from the on-line computer activity can be valuable in this assessment. This information can often be ascertained from the online service provider and through undercover communication, pretext contacts, informants, record checks, and other investigative techniques (i.e., mail cover, pen register, trash run, surveillance, etc.).

- Screen Name
- Screen Profile
- Accuracy of Profile
- Length of Time Active

continued on next page

# Cyber Pedophiles

continued from page 14

- Amount of Time Spent Online
- Number of Transmissions
- Number of Files
- Number of Files Originated
- Number of Files Forwarded
- Number of Files Received
- Number of Recipients
- Site of Communication
- Theme of Messages & Chat
- Theme of Pornography

A common problem in these cases is that it is often easier to determine a computer is being used than to determine who is using the computer. It is obviously harder to do a background investigation when multiple people have access to the computer. Pretext phone calls can be very useful in such situations.

Exaggerated Example: An investigation determines that a suspect is a 50-year-old single male who: does volunteer work with troubled boys; has two prior convictions for sexually molesting young boys in 1974 and 1986; has an expensive state-of-the-art home computer; has a main screen name of "Boylover" and one screen profile that describes him as a 14-year-old; has for the last five years daily spent many hours online in chat rooms and the "alt.sex.preteen" newsgroup justifying and graphically describing his sexual preference for and involvement with young boys; and brags about his extensive pornography collection while uploading hundreds of child pornography files all focusing on preteen boys in bondage to dozens of individuals all over the world. If such a determination were relevant to the case, these facts would constitute more than enough probable cause to believe this suspect is a preferential sex offender.

Knowing the kind of offender with whom you are dealing can go a long way in determining investigative strategy. For example, it might be useful in developing offender interview strategy, evaluating the consistency of victim statements, proving intent, assessing the admissibility of prior acts, learning where and what kind of corroborative evidence might be found (i.e., the existence and location of other victims and child pornography or erotica), etc. It might even be included in a search warrant affidavit to add to the probable cause, to expand the nature and scope of the search, or to address legal staleness problems.

With either of the preferential types of computer offenders (the sexually indiscriminate offender or the pedophile), the characteristics, dynamics, and techniques (i.e. expert search warrant) previously discussed concerning preferential sex offenders should be considered.

### "Concerned Citizens"

Many individuals who come to authorities to report deviant sexual activity they have discovered on the Internet must invent clever excuses for how and why they came upon such material. They often start out pursuing their own sexual or deviant interests, but then decide to report to the police either because it went too far, because they are afraid they might have been monitored by authorities, or because they need to rationalize their perversions as having some higher purpose or value. Rather than honestly admitting their own deviant interests, they make up elaborate explanations to justify finding the material. Some claim to be journalists, researchers or outraged, concerned citizens trying to protect a child or help the police. In any case, what they find may still have to be investigated.

***Many individuals who come to authorities to report deviant sexual activity they have discovered on the Internet must invent clever excuses for how and why they came upon such material.***

Investigators must consider that these "concerned citizens" reporting such activity may:

1. Be motivated by a need to rationalize or deny their deviant sexual interests and so have embellished and falsified an elaborate tale of perversion and criminal activity on the Internet.
2. Whatever their true motivations might be, have uncovered individuals using the Internet to validate and reinforce their bizarre, perverted sexual fantasies and interests (a common occurrence), but who are not engaged in criminal activity.
3. Whatever their true motivations might be, have uncovered individuals involved in criminal activity.

One especially sensitive area for investigators is the preferential sex offender who presents himself as a concerned citizen reporting what he inadvertently "discovered" in cyberspace or requesting to work with law enforcement to search for child pornography and to protect children. Other than the obvious benefit of legal justification for their past or future activity, most do this as part of their need to rationalize their behavior as worthwhile and to gain access to children. When these offenders are caught, instead of recognizing this activity as part of their preferential pattern of behavior, the courts sometimes give them leniency because of their "good deeds." Preferential sex offenders who are also law enforcement officers sometimes claim their activity was part of some well-intentioned, but unauthorized investigation.

### Use of Computers

The great appeal of a computer becomes obvious when you understand sex offenders, especially the preferential sex offender. The computer provides preferential sex offenders with an ideal means of filling their needs to: (1) organize their collections, correspondence, and fantasy material; (2) communicate with victims and other offenders; (3) store, transfer,

continued on next page

# Cyber Pedophiles

continued from page 15

manipulate, and create child pornography; and (4) maintain financial records. The sex offender using a computer is not a new type of criminal. It is simply a matter of modern technology catching up with long-known, well-documented behavioral needs. In the past they were probably among the first to obtain and use, for their sexual needs, new inventions such as the camera, the telephone, the automobile, the Polaroid camera, and the video camera and recorder. Because of their traits and needs, they are willing to spend whatever time, money, and energy it takes to obtain, learn about, and use this technology.

### Organization

Offenders use computers to organize their collections, correspondence, and fantasy material. Many preferential sex offenders seem to be compulsive record keepers. A computer makes it much easier to store and retrieve names and addresses of victims and individuals with similar interests. Innumerable characteristics of victims and sexual acts can be easily recorded and analyzed. An extensive pornography collection can be catalogued 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 computer 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 there are individuals who believe that cyberspace is a new frontier where the old rules of society do not apply. They do not want this "freedom" scrutinized and investigated. There is no easy solution to this problem. Meticulous analysis and investigation are the only answers.

### Communicate to Fuel and Validate

Many offenders are drawn to the Internet and other online activity as a way to communicate and validate their interests and behavior. This is actually the most important and compelling reason that preferential sex offenders are drawn to online services. 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 computer may also enable them to obtain active validation (i.e., from living humans) with less risk of identification or discovery. The great appeal of this type of communication is its perceived anonymity and immediate feedback. They feel protected as when using the mail, but get immediate response as when meeting face to face.

Like advertisements in "swinger magazines," computer online services are used to identify individuals with mutual interests 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 or participate in other surreptitious or underground online bulletin boards.

In addition to adults with similar interests, offenders can sometimes get validation from the children they communicate with online. Children needing attention and affection may respond to an offender in positive ways. They may tell the offender he is a "great guy" and that they are grateful for his interest in them. In communicating with children, and in a few cases with adults, offenders frequently assume the identities of children.

***Sadly, I have come to suspect that some individuals with potentially illegal, but previously latent sexual preferences have begun to criminally act out when their inhibitions are weakened after their arousal patterns are fueled and validated through online computer communication.***

Validation is also obtained from the fact that the offenders are utilizing the same cutting edge technology used by the most intelligent and creative people in society. In their minds, the time, technology, and talent it takes to engage in this activity is proof of its value and legitimacy.

Sadly, I have come to suspect that some individuals with potentially illegal, but previously latent sexual preferences have begun to criminally act out when their inhibitions are weakened after their arousal patterns are fueled and validated through online computer communication.

Offenders' need for validation is the foundation on which proactive investigative techniques (e.g. stings, undercover operations, etc.) are built and the primary reason they work so often. Although their brain may tell them not to send child pornography or not to reveal details of past or planned criminal acts to a stranger they met online, their need for validation often compels them to do so.

### Child Pornography

Because of computers utilizing 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 now use a computer to transfer, manipulate, and even create child pornography. With the typical home computer and modem, still images can easily be digitally stored, transferred from print or videotape, and transmitted, with each copy being as good as the original. Visual images can be stored on hard drives, floppy disks, CD-ROM's, or DVD's. With newer technology, faster modems, digital cameras, and

continued on next page

# Cyber Pedophiles

continued from page 16

better computers, similar things can now be done with some moving images. For now, however, it is still difficult to transmit the most preferred child pornography format—high quality, lengthy moving images (e.g. videotape, films).

The other invaluable modern inventions for pornographers, the video camera and recorder, are now being integrated into and through the computer. Multimedia images with some motion and sound and virtual reality programs can provide an added dimension to the pornography. The information and images stored and transmitted can be encrypted to deter detection.

Some of these uses are now small problems that can eventually become big problems. Computer software and hardware is being developed so rapidly that the potential of these problems is almost unlimited. In the future, most communication systems in a home (e.g., telephone, television, fax, videotape, music, newspapers, financial records, etc.) may be funneled through a computer.

The ability to manipulate digital visual images may make it difficult to believe your own eyes. Television commercials now make it appear that Paula Abdul is dancing with Gene Kelly and John Wayne is talking to a drill sergeant. Halfway through the movie "Forrest Gump," Lt. Dan's legs are no longer visible. With computer graphics programs, images can be easily changed or "morphed." This is similar to the technology that is used to "age" the 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 child pornography laws.***

Computer-manipulated and, soon, computer-generated visual images of "children" engaging in sexually explicit conduct may call into question the basis for child pornography laws. Under the Child Pornography Prevention Act of 1996, the Federal definition of "child pornography" has been expanded to include not only a sexually explicit visual depiction using a minor, but also 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 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. This law is currently being challenged in a variety of cases and jurisdictions, which will ultimately establish its constitutionality (see article by Toth and McClure in this issue). If this law is found unconstitutional, only existing obscenity laws may apply to such manipulated/simulated child pornography.

Investigators must also recognize and understand that not all collectors of child pornography physically molest children, and not all molesters of children collect child pornography. Not all children depicted in child pornography have been sexually abused. For example, some have been photographed without their knowledge while undressing, others were manipulated into posing nude. Depending on the use of the material, however, all can be considered exploited. For this reason, even those who "just" download or collect child pornography produced by others play a role in the sexual exploitation of children, even if they have not physically molested a child.

Computer offenders who "just" traffic in child pornography are committing serious violations of the law that do not necessarily require proving that they are also child molesters. If it is relevant and the facts support it, such individuals can be considered preferential sex offenders because such behavior is an offense. Some computer offenders who traffic in child pornography, especially the sexually indiscriminate preferential sex offender, may have significant collections of adult pornography as well. In some cases, they may even have far more adult than child pornography. Such offenders may not be "pedophiles," but can still be preferential sex offenders.

### 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. Lists of customers, 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, there may be an increase in profit-motivated distribution.

### 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 sometimes make identifying the actual perpetrator difficult. On the computer, the offender can assume any identity or characteristics he wants or needs. Children from dysfunctional families and families with poor communication are at significant risk for seduction. Older children are obviously at greater risk than are younger children. Adolescent boys confused over their sexual orientation are at particularly high risk of such contacts. By no reasonable definition can an individual with whom a child has regularly communicated online for months be called a "stranger."

The child can be indirectly "victimized" through

continued on next page

## Cyber Pedophiles

continued from page 17

conversation ("chat") and the transfer of sexually explicit information and material or can be evaluated for future face-to-face contact and direct victimization. The latest technology even allows for real-time group participation in child molestation by digital teleconferencing by computer.

Investigators must recognize that many of the children lured from their homes after online computer conversations are not innocents who were duped while doing their homework. Most are curious, rebellious, or troubled adolescents seeking sexual information or contact. Investigation will sometimes discover significant amounts of adult and child pornography and other sexually explicit material on the computer of the child victim. Nevertheless, they have been seduced and manipulated by a clever offender and do not fully understand or recognize what they were getting into.

***Investigators must recognize that many of the children lured from their homes after online computer conversations are not innocents who were duped while doing their homework.***

Investigators and prosecutors must understand and learn to deal with the incomplete and contradictory statements of many seduced victims. The dynamics of their victimization must be considered. They are embarrassed and ashamed of their behavior and rightfully believe that society will not understand their victimization. Many adolescent victims are most concerned about the response of their peers. Investigators who have a stereotyped concept of child sexual abuse victims or who are accustomed to interviewing younger children molested within their family will have a difficult time interviewing adolescents molested after online seduction. Many of these victims will be troubled, even delinquent children from broken homes.

Although applicable statutes and investigative or prosecutive priorities may vary, officers investigating computer exploitation cases must generally start from the premise that the sexual activity is not the fault of the victim even if the child:

- Did not say no
- Did not fight
- Actively cooperated
- Initiated the contact
- Did not tell
- Enjoyed the sexual activity
- Accepted gifts or money

Investigators must also remember that many children, especially those victimized through the seduction process, often:

- Trade sex for attention, affection, or gifts
- Are confused over their sexuality and feelings
- Are embarrassed and guilt-ridden over their activity
- Describe victimization in socially acceptable ways
- Minimize their responsibility & maximize offender's
- Deny or exaggerate their victimization

All these things do not mean the child is not a victim. What they do mean is that children are human beings with human needs and not necessarily "innocent angels God sent us from heaven." Sympathy for victims is inversely proportional to their age.

When law enforcement officers are pretending to be children as part of authorized and approved proactive investigations, they must remember that the number of potential offenders is proportional and the appeal of the case is inversely proportional to the "age" of the "victim." Because there are far more potential offenders interested in older children, pretending to be a 15- or 16-year-old will result in a larger online response. The resulting case, however, will have far less jury appeal.

After developing a relationship online, offenders who are arrested attempting to meet with children (or individuals they believe to be children) to engage in illegal sexual activity, often claim that they were not really going to have "sex." They claim the discussed sex was just a fantasy, was part of an undercover "investigation," or was a means of communicating with a troubled child. In addressing this issue of intent or motivation, investigators must objectively weigh all the offender's behavior (i.e., past history, honesty about identity, nature of communications, who was notified about activity, overt actions taken, etc.). Ultimately, a judge or jury will decide this question of fact.

### Summary

Investigators must be alert to the fact that any offender with the intelligence, economic means, or employment access might be using a computer in any or all of the above ways, but preferential sex offenders are highly likely to do so.

As computers become less expensive, more sophisticated, and easier to operate the potential for abuse will grow rapidly.

#### References

American Psychiatric Association. (1994). *Diagnostic and statistical manual of mental disorders* (4th ed.). Washington, DC: author.

## Call for Nominations
## APSAC Board of Directors

APSAC is seeking nominations of members to stand for election to the Board of Directors for three-year terms beginning on June 1, 1999 and ending on May 31, 2002. Nominees must have been APSAC members for at least one year, and must have agreed to be nominated before their nominations are submitted.

Board member's contributions of time, energy, and talent play an enormous role in APSAC's success. To remain effective and powerful, APSAC needs the active participation of all members of the Board of Directors. Members who are enthusiastic and supportive but unable to perform the duties of a Board member are highly valued and can serve APSAC in many capacities, but should not be nominated for Board service unless they can devote the time necessary to fully discharge a Board member's duties. These duties include, but are not limited to:

- attending at least one Board meeting each year;
- chairing a committee or subcommittee;
- waiving speaking fees for a minimum of two APSAC-sponsored training events each year; and,
- actively working to generate members and revenue for the association.

APSAC's Nominating Committee (consisting of all members of the Executive Committee not standing for re-election, and five members at large appointed by the President) will select nominees based on a number of criteria, including:

1) diversity in discipline, area of expertise, culture, and geography
2) a consistent record of service to APSAC
3) excellence in professional reputation and practice
4) stature in and contributions to the field

Nominations are due at APSAC's offices on February 19,1999. Complete nominations consist of a nomination form (see enclosed), 200- to 400-word letters of nomination from two people outlining the candidate qualifications for service on the Board of Directors, and a copy of the candidate's resume or and/or curriculum vita.

**Nominations may be sent to**
**APSAC Board Nominations**
**407 S. Dearborn Street, Suite 1300**
**Chicago, IL 60605**
**312-554-0166**

**Candidate Nomination Form**
**Board of Directors**
**American Professional Society on the Abuse of Children**

Candidate Name and Degree:

Candidate Discipline:

Candidate Work Address:

Candidate Work Telephone, Fax, and Email (if available):

Current Position Title:

Years in the Field: Years of membership in APSAC:

Service To APSAC (circle all that apply, and provide detail in space provided and/or on additional sheets)

o Former Board Member o Writing for the Advisor or Child Maltreatment Journal
o Membership Recruitment o Task Force o Teaching o State Chapter
o Child Maltreatment Journal Review or Editor o Advisory Board Member
o Other

Explanation:

Candidate Areas of Specify (circle no more than 5):

o Adult Survivors o Child Victims o Perpetrators o Families
o Research o Policy o Prevention o Physical Abuse
o Neglect o Civil Law o Diversity Issues o CPS Investigation
o Program Administration o Non-Offending Parents o Psychological Maltreatment
o Medical Evaluation and Treatment o Criminal Investigation o Case Management
o Criminal Law o Other (Please Discuss)

NB: To complete the nomination procedure, attach a brief statement (200-400 words) of formal nomination outlining the candidate's qualifications to service on APSAC's Board. Your formal nomination indicates that you have spoken with the nominee and he or she has agreed to stand for election to APSAC's Board of Directors.

Nominator Signature:

Date:

# Call for Nominations
# APSAC Annual Awards

APSAC's Annual Awards will be presented at the Seventh National Colloquium in San Antonio, TX, June 2-5, 1999. Nominations are sought for the following categories:

**Outstanding Service**
Recognizing a member who has made substantial contributions to APSAC through leadership and service to the Society.
Former Recipients: Jon Conte, PhD (1992); David Corwin, MD (1993); John E. B. Myers, JD (1994); David Chadwick, MD (1995); Joyce Thomas, RN, MPH (1996); Barbara Bonner, PhD (1997); Kathleen Coulborn Faller, ACSW, PhD (1998).

**Outstanding Professional**
Recognizing a member who has made outstanding contributions to the field of child maltreatment and to the advancement of APSAC's goals.
Former recipients: Ann Wolbert Burgess, DNSc (1992); Lucy Berliner, MSW (1993); Kee McFarlane, MSW (1994); David Finkelhor, PhD (1995); Ken Lanning, MS (1996); Robert M. Reece, MD (1997); Anne Cohn Donnelly, DPH (1998).

**Research Career Achievement**
Recognizing an APSAC member who has made repeated, significant, and outstanding contributions to research on child maltreatment over his or her career.
Former recipients: Gail Goodman, PhD (1992); Norman Polansky, PhD (1993); Murray Strauss, PhD; William Friedrich, PhD (1995); Byron Egeland, PhD (1996); Dante Cicchetti, PhD (1997); Susan Zuravin, PhD (1998).

**Outstanding Research Article**
Recognizing the authors of a research article or book published in the previous calendar year judged to be the most significant contribution to the field of child abuse in that time period.

**Outstanding Doctoral Dissertation**
Recognizing the doctoral dissertation completed within the last calendar year that made the most outstanding contribution to research on child maltreatment.

**Outstanding Media Coverage**
Recognizing a reporter or team of reporters in print or electronic media whose coverage of child maltreatment issues in the previous calendar year shows exceptional knowledge, insight and sensitivity.

**Outstanding Research Study**
Former Recipients: Roy Herrenkohl, PhD, Ellen Herrenkohl, PhD, Brenda Egolf, MA, Lehigh University (1998)

**Nomination Procedure:**
Send a completed copy of the attached form and brief letter of nomination to the Chair of the Awards Committee. For Outstanding Research Study and Outstanding Doctoral Dissertation awards, please include a copy of the nominated article or an abstract of the nominated dissertation. For Outstanding Media Coverage, please include five copies of the nominated article(s) or program(s).

Deadline for Awards Nominations is May 1, 1999. Nominations may be sent to:

APSAC
407 S. Dearborn Street, Suite 1300
Chicago, IL 60605
312-554-0166

**Nomination Form**
**1998 Awards**
**American Professional Society on the Abuse of Children**

Award Category: (Please check one)

Outstanding Service

Outstanding Professional

Research Career Achievement

Outstanding Research Article

Outstanding Doctoral Dissertation

Outstanding Media Coverage

Nominator Information:

Name:

Address:

Telephone:

Fax:

Email:

Nominee Information:

Name:

Address:

Telephone:

Fax:

Email:

Title of article or dissertation: (if applicable)

Published in:

Please attach a 200-400 word letter of nomination.
Include supportive materials as required.
Send materials to:

APSAC Awards
407 S. Dearborn Street, Suite 1300
Chicago, IL 60605
312-554-0166

# FEATURE

# An Overview of Selected Legal Issues Involved in Computer Related Child Exploitation: Many Questions, Few Answers

by Patricia Toth, J.D. and Kathy McClure, J.D., U.S. Department of Justice Child Exploitation and Obscenity Section

Scenario #1. A concerned parent calls the local police department because her 12-year- old child has received "suggestive" e-mail messages on the computer at home. She wants the police to "do something" about it.

Scenario #2. A 16-year-old teenager is several hours late returning home from school, and her parents are worried. They have copies of e-mail messages received by the teen from "Bob," suggesting that they meet and "get to know each other better." Attached to these messages are images of what appears to be adult pornography.

Scenario #3. While 'surfing the Net,' a teacher comes across sites offering "hot pics" of "preteens." He downloads some of these images, and contacts the local police department. He describes some of them as "drawings"(e.g.,cartoons), and others as appearing to be photographs.

These scenarios represent cases involving potential child exploitation which are increasingly coming to the attention of law enforcement throughout the country. What can the police do in each of these situations? Have any crimes been committed? The answers to these questions are not necessarily clear nor well-settled, and may depend, in part, on the state (or states) in which the events happened. Traditional notions of jurisdiction in criminal matters are difficult to apply to such cases, since computer communication can so quickly and easily cross state and national boundaries. Two observations are evident in these scenarios: first, more information is needed to make a reasonable decision; and second, there is reason to be concerned about the use of computers to facilitate harm to children under each of the circumstances described above.

***Though it is nearly impossible to fully anticipate how computer technology will evolve and be used in the future, a number of states have crafted legislation addressing the use of computer-related technology to exploit children.***

While computer technology has developed very rapidly, applicable laws have lagged behind. And though it is nearly impossible to fully anticipate how computer technology will evolve and be used in the future, a number of states have crafted legislation addressing the use of computer-related technology to exploit children. By the end of 1997, at least 18 states[1], as well as the U.S. Congress, included language in their child pornography statutes which specifically mentions the use of computers, computer tape or disks, or visual depictions by electronic means. Many of these laws prohibit the use of computers to produce, disseminate, sell or possess child pornography. At least seven states[2], in addition to the federal law, also have specific provisions which ban the use of computers to solicit or lure children into engaging in sexual activity.

### Federal Statutes

The federal statutes commonly invoked to charge computer-related child pornography offenses are found in 18 U.S.C. §§ 2252 and 2252A. Section 2252 prohibits the transportation, shipment, distribution, receipt, reproduction, and sale, or possession with the intent to sell, of any visual depiction of a minor engaging in sexually explicit conduct[3], by any means, including by computer, and also prohibits the possession of 3 or more items, as discussed below, which contain a sexually explicit visual depiction. The federal possession offense, found in 2252(a)(4)(B), criminalizes the knowing possession of "3 or more books, magazines, periodicals, films, video tapes, **or other matter** which contain any visual depiction ...". (Emphasis added.) Three computer diskettes, as well as 1 hard drive and 2 diskettes, have been the subject of successful federal prosecutions as "other matter." There are two grounds for federal jurisdiction found in this statute: 1) that the visual depictions themselves traveled in interstate or foreign commerce; or 2) that the materials used to produce the visual depictions traveled in interstate or foreign commerce.

Section 2252A, effective September 30, 1996, added another possession offense which prohibited the possession of three or more images (on any one medium, for example one hard drive or one CD-Rom) of "child pornography." As of October 30, 1998, possession of even a single image is banned by statute (18. U.S.C. 2252(a)(4)(b) and 18 U.S.C. 2252A(a)(5)(B)). (The new Protection of Children from Sexual Predators Act of 1998 contains a number of provisions which change federal law in this area. For a listing of some of the key provisions, see the box

continued on next page

[1]Arizona, Arkansas, California, Florida, Idaho, Illinois, Indiana, Kansas, Maryland, Michigan, Mississippi, Montana, Nevada, New Jersey, New Mexico, Pennsylvania, Texas, Virginia. (*Child Abuse and Neglect State Statute Series*, Computer Crimes, December 31, 1997.)

[2]Alabama, Florida, Illinois, Indiana, New Mexico, North Carolina, Oklahoma. *(Child Abuse and Neglect State Statute Series,* December 31, 1997). Burns Ind. Code Ann. § 35-42-6 (1997); 98 N.M. ALS 64, 1998 N.M. Laws 64, N.M. Ch. 64, 1998 N.M. SB 127; N.C. Gen. Stat. § 14-202.3 (1997).

[3]"Sexually explicit conduct" is defined in 18 U.S.C. § 2556(2), and includes the "lascivious exhibition of the genitals or pubic area of any person."

## Overview of Selected Legal Issues

continued from page 19

accompanying this article.) "Child pornography" is defined in 18 U.S.C. § 2256(8) as encompassing any visual depiction, to include a computer or computer-generated image, which "is, **or appears to be**, of a minor engaging in sexually explicit conduct". (Emphasis added.) Federal law also criminalizes conduct related to the production of a sexually explicit visual depiction when the image(s) have been transported in interstate or foreign commerce or mailed, or the offender has reason to know the image(s) will be so transported. (18 U.S.C. 2251.)

Other federal law provisions prohibit individuals who themselves travel, or who transport a child, across state or national lines intending to engage in prohibited sexual acts with a child (18 U.S.C. § 2241, 2243, 2422, and 2423). The use of computers to communicate with a child (or someone whom the offender believes to be a child) is often an integral part of these crimes, despite the fact that the statutes themselves do not make specific reference to computers. Depending on the particular provision being considered, the age of the child may be important: some provisions require that the child be younger than 12 years, while others refer to crimes as defined by state law ("sexual activity for which any person can be charged with a criminal offense") (18 U.S.C. §§ 2422 (a) and (b), and 2423 (a)).

The following section will examine each of the examples provided at the beginning of this article and discuss legal considerations related to possible criminal prosection of the described activity.

### Scenario #1

In this scenario, the content of the e-mail messages received by the 12-year-old will be crucial. If the messages reveal an attempt by the sender to solicit, lure or entice the child to engage in any sexual act, a state criminal violation may have occurred, particularly if venue lies in one of the seven states indicated above, which have statutes addressing solicitation by computer. Even a more general 'luring' statute which does not make specific mention of computers, if it exists, should apply. In order to proceed in most states, there would have to be some indication that the individual who sent the e-mail messages knew the recipient's age, and hence, intended to entice a child/minor. In this investigation, law enforcement might want to assume the identity of the 12-year-old, continue communicating with the sender, and further explore his or her intentions, allowing the sender to graphically describe the expected encounter with the child. Often at this juncture, the sender's actual identity is unknown. To establish or confirm the individual's real name and address, investigators can subpoena account information from the sender's e-mail service provider, and/or can "chat" with the sender about at least general information (e.g., what city s/he lives in, where s/he works, etc.). If the sender lives in a state different than the 12-year-old's, and intends to travel interstate to engage in sexual activity with the child, federal prosecution is a possibility.

If, instead of e-mail messages sent to the 12-year-old, the "suggestive" material which upset the parent was adult pornography posted on a Web site visited by the child, there may be limits as to what law enforcement can do. The portion of the federal Communications Decency Act of 1996 ("CDA") which attempted to prohibit the display of "patently offensive" materials to persons under 18 was deemed by the U.S. Supreme Court to be vague, overbroad and an unconstitutional infringement of free speech (*Reno v. American Civil Liberties Union et al*, 1997).

Some states have attempted to regulate content on the Internet. For example, the legislature in New Mexico, in a statute which became effective July 1, 1998, has outlawed the "dissemination of material that is harmful to a minor by computer," when it "depicts actual or simulated nudity, sexual intercourse or any other sexual conduct." (New Mexico Stat. Ann., 1998). Defenses are provided in this New Mexico statute if efforts have been made to restrict access to the material by minors. Alabama law prohibits the transmission of "obscene material to a child" by means of computer, (Alabama Code. Code 13A-6-111) and Georgia's statutes include the crime of "electronically furnishing obscene materials to minors."(Ga. Code Ann. 16-12-100.1.) It remains to be seen whether such statutes adequately address the concerns about unconstitutional vagueness and overbreadth found to exist in the federal CDA statute. (See Birch's article in this issue of the *Advisor* for an update on new federal legislation designed to regulate content online.)

### Scenario #2

In this scenario involving a missing 16-year-old girl, law enforcement would clearly want to take immediate steps to find the teenager and be sure she is safe. Obviously, an assault, kidnaping, forcible sexual contact, or other criminal activity could be prosecuted. However, if the girl met with "Bob" voluntarily, even if they engaged in sexual activity, criminal sanctions may not necessarily apply. Under this scenario, the state in which the sexual contact takes place makes all the difference in whether and what criminal sex offense charge(s) could be filed. For example, if the

continued on next page

[4]The "age of consent" is 14 in Hawaii; 15 in Colorado; and 16 in Alabama, Alaska, Arkansas, Connecticut, Delaware, Georgia, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Vermont, Washington, and West Virginia. (Phipps, 1997).

[5]The "age of consent" is 17 in Illinois, Lousiana, Missouri, New Mexico, New York, Texas; and 18 in Arizona, California, Florida, Idaho, Mississippi, North Dakota, Oregon, Tennessee, Utah, Virginia, Wisconsin, and Wyoming. (Phipps, 1997).

## Overview of Selected Legal Issues

continued from page 20

investigation revealed that there was consensual sexual contact with Bob, the 16-year-old would be at, or older than, the "age of consent" in 32 states[4]. In 18 states where the "age of consent" is either 17 or 18[5], Bob could potentially be charged with a relatively serious sex offense. In states where the age of consent is 16 or lower, Bob's conduct may still violate statutes which prohibit 'corrupting the morals of a minor,' 'contributing to the delinquency of a minor,' or an equivalent offense, since a minor is generally considered to be someone under the age of 18. However, such crimes are typically classified as misdemeanors, and treated as less serious than "traditional" child sex offenses.

Bob's sending of adult pornography to the teen, unless the images could be found to be "obscene,"[6] is also likely to be difficult to prosecute. Absent a special statute which outlaws the transmission of such material to someone under 18, if it could legally be provided to adults, it can also be made available to the 16-year-old, unless law enforcement and the prosecutor are willing to pursue a 'contributing' or 'morals' charge, as discussed above.

***The overwhelming majority of state child pornography crimes appear to require the involvement of a real child, whether the crime is possession, production, or distribution.***

**Scenario #3**

The third scenario involves the discovery of what is, or could be, child pornography on the Internet. To the extent possible, law enforcement would want to evaluate whether the "helpful" teacher was himself a collector of child pornography. Undoubtedly, investigators would be wise to advise the teacher to cease any "investigative" efforts, and provide all copies of suspect images to law enforcement, retaining none. Otherwise, the teacher would technically be in violation of federal laws prohibiting the receipt and possession of child pornography.

While almost every state bans the production, sale, distribution, exchange and possession with intent to distribute or sell, of child pornography, there were 11 states, as of 1997, whose statutes did not prohibit the simple *possession* of child pornography[7]. As a result, unless a suspect who has child pornography on his or her computer or other media (e.g., diskettes, zip disks, CD ROMs) can be shown to have produced, sold, disseminated, or possessed with the intent to sell or disseminate, then prosecution under state law in those 11 jurisdictions would be unlikely.

A federal criminal charge for possession is possible under §2252(a)(4)(B) when, assuming the other elements are met, "... the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct ...". This provision has led to defenses which assert either that the person in the depiction may be over the age of 18 and thus not a minor, or that the image itself could have been "manipulated" and thus does not involve an actual minor, a real person. Computer programs which allow for the manipulation, or "morphing", of digital images are easy to use and widely available today. The quality of this software continues to improve and it can be difficult, if not impossible, to detect whether an image has been manipulated, particularly if done well and when there is no known "original" image for comparison.

The Child Pornography Protection Act of 1996 was passed, in part, to address the manipulation issue. That Act added 18 U.S.C. § 2252A to the federal law, which for the first time uses the term "child pornography," defined to include images which are or "appear to be" of minors engaging in sexually explicit conduct, or are presented in a manner which "conveys the impression" that the material contains such a depiction (18 U.S.C. §2256(8). As a result, images which may have been manipulated, as long as they appear to be child pornography, could be the subject of federal prosecution. Application of this statute has, to date, led to differing results in the federal courts. For example, in *U.S. v. Hilton*, the District Court in Maine declared 18 U.S.C. § 2252A(a)(5)(B)[6], and the incorporated definition found in § 2256(8)(B), unconstitutionally overbroad (*U.S.v. Hilton*, 1998). In the Northern District of California, the Court in *The Free Speech Coalition, et al. v. Reno*, found the same statute constitutional. Both of those cases are pending appeal. Under these circumstances, the ability to use this portion of the new definition of "child pornography" found in § 2256(8)(B) may vary, depending on the federal district in which the case is heard.

The overwhelming majority of state child pornography crimes appear to require the involvement of a real child, whether the crime is possession, production, or distribution. In fact, Kansas law regarding possession of child pornography states that the image involved must show "a real child under 16 years of age... ." (Kansas. Stat. Ann. §21-3516.) Our research located only one state with language similar to the federal provision, Indiana, where knowing possession of an image which "depicts or describes sexual conduct by a child who is less than 16 years of age, **or appears to be** less than 16 years of age, ... " (emphasis added) is defined as a crime (Ind. Code §35-42-4-4). Ohio law allows for an inference "that a per-

continued on next page

[6]For the federal obscenity standard, see *Miller v. California*, 1973.

[7]Alaska, Arkansas, Connecticut, Maine, Massachusetts, Mississippi, Missouri, New Mexico, Rhode Island, South Carolina, Vermont. *Child Abuse and Neglect State Statute Series,* Child Pornography, December 31, 1997.

## Overview of Selected Legal Issues

continued from page 21

son in the material or performance involved is a minor if the material or performance, through its title, text, visual representation, or otherwise, represents or depicts the person as a minor." (Ohio Rev. Code Ann. §2907.321.) Both of these statutes still arguably require the involvement of an actual identifiable person, albeit one whose true age is misrepresented. The manipulation defense, therefore, is one that can be expected with regularity in state prosecutions of computer child pornography cases. In addition, cartoons which are sexual in nature may not be subject to criminal prosecution based on similar reasoning, unless state law specifically includes drawn images as a prohibited item. Because the language of state statutes varies widely, whether a particular case falls within the protection of any jurisdiction's law, will depend on the interpretation of professionals and courts within that state.

One final consideration in the response to the third scenario is that law enforcement will almost certainly be interested in ascertaining the source of the child pornography. Both state and federal criminal prosecutions of the originator of the child pornography are possible, depending on the specific facts discovered. In order to gather the information necessary to build a case in either state or federal court, investigators should be familiar with provisions of federal wiretap law (18 U.S.C. §§2510 - 2522), the Electronic Communications Privacy Act and the Privacy Protection Act. These federal laws require special care to be taken when intercepting electronic communications, when obtaining information from service providers, and when seizing information which could be considered to be work product or documentary materials if intended for public dissemination or publication. Violation of the dictates of these statutes can lead to possible personal civil liability for law enforcement investigators. In addition, state laws regarding privacy (especially involving computer communications) and wiretaps may apply, and be even more restrictive.

There is no doubt that those who exploit children will continue to take increasing advantage of available technology to facilitate their crimes. In order to respond to these situations in the most effective way, investigators and prosecutors will need to educate themselves about this complicated area, take advantage of specialized training opportunities, and increase efforts to implement federal and state coordination. (See Jezycki's article, this issue of the *Advisor,* for more information on training opportunities. See also Whitcomb and Eastin, 1998 and the Education Development Center and the Massachusetts Child Exploitation Network, 1995.) The legal system will continue to evolve as it deals with more cases, and new and better legislation can be expected, leading to greater justice for exploited children.

**References**


Alabama Code § 13A-6-111. August 1, 1997.

Child Abuse and Neglect State Statute Series, Volume V- Crimes, No. 36, Computer Crimes, current through December 31, 1997, National Clearinghouse on Child Abuse and Neglect Information and National Center for Prosecution of Child Abuse.

Child Abuse and Neglect State Statute Series, Volume V- Crimes, No. 30, Child Pornography, current through December 31, 1997, National Clearinghouse on Child Abuse and Neglect Information and National Center for Prosecution of Child Abuse.

Electronic Communications Privacy Act 18 U.S.C. §§2701 - 2711. October 21, 1986

Communications Decency Act of 1996 97 USC § 223 (a) (1).

Education Development Center and the Massachusetts Child Exploitation Network. (1995). Child Sexual Exploitation: Improving Investigation and Protecting Victims: A Blueprint for Action. Washington, DC: Office for Victims of Crime.

The Free Speech Coalition, et al. v. Reno, 1997 WL 487758 (N.D. Calif. Aug 12, 1997), appeal pending, No. 97-16536 (9th Cir.) (argued Mar. 10, 1998).

Georgia Code Ann. § 16-12-100.1. (1993)

Indiana Code § 35-42-4-4. (1996)

Kansas. Stat. Ann. § 21-3516. (1995)

Miller v. California, 413 U.S. 15 (1973).

New Mexico Stat. Ann. § 30-37-3.2. July 31, 1998

Ohio Rev. Code Ann. § 2907.321. (1989).

Phipps, C. (1997). Children, Adults, Sex and the Criminal Law: In Search of Reason. *Seton Hall Legal Journal, Volume 22*, No. 1.

Privacy Protection Act (42 U.S.C. § 2000aa.) (September 30, 1996)

*Reno v. American Civil Liberties Union et al.*, 117 S.Ct. 2329 (1997).

*U.S. v. Hilton*, 999 F. Supp. 131 (District of Maine, Mar. 30, 1998), appeal pending, No. 98-1513 (1st Cir.)

Whitcomb, D. and Eastin, J. (January, 1998). Joining Forces against Child Sexual Exploitation. Washington, DC: Office for Victims of Crime.


## "PROTECTION OF CHILDREN FROM SEXUAL PREDATORS ACT OF 1998"

**Passed by U.S. Senate on 10/9/98, Passed by U.S. House of Representatives on 10/11/98**
**Signed by President Clinton 10/30/98**

- ***"Zero Tolerance" for Possession of Child Pornography,"*** amending 18 U.S.C. 2252(a)(4) by replacing '3 or more' with '1 or more,' and adding subsection (c) "Affirmative Defense." Amending 18 U.S.C. 2252A(a)(5) by replacing '3 or more images' with 'an image,' and adding subsection (d) "Affirmative Defense."
- New 18 U.S.C. § 2425 "Use of interstate facilities to transmit information about a minor."
- Adding another jurisdictional base for production of child pornography, 18 U.S.C. § 2251(a) and (b).
- New 18 U.S.C. § 1470 "Transfer of obscene material to minors." Where minor is an individual who has not attained the age of 16 years. Sentence: not more than 10 years.
- Adding to 42 U.S.C. 13001, a § 227 "Reporting of Child Pornography by Electronic Communication Service Providers."
- New 18 U.S.C. § 3486A "Administrative subpoenas in cases involving child abuse and child sexual exploitation."

# Filtering Tools, Education, and the Parent: Ingredients for Surfing Safely on the Information Superhighway

Danielle M. Gallo
Senior Technical Associate, AT&T Labs-Research

FEATURE

Each day more and more people are going online to tap the Internet's rich resources. Many Internet users are children, and unfortunately, the Internet is not always a safe haven for children and teenagers.

Keeping children safe online is an arduous task that parents and educators must undertake with great intensity and enthusiasm. Lack of familiarity with the medium may serve as the largest obstacle. Many parents admit that their children know more about computers than they do. Parents' lack of knowledge may cause them to fear machines and allow the child free reign while online. In addition, parents may not be aware of the weaknesses of the filtering/blocking tools they utilize. Children, especially teenagers, may be aware of such weaknesses and find ways around them. Regardless of what filtering/blocking tool is employed, parents need to educate themselves about the Internet and sit with their children while they are online.

***This is a recurring problem with filtering/blocking tools. If the child can obtain the password and maneuver his way around the system, he can easily control the content accessed.***

Children's online safety is a serious business that has led to the development of a multitude of filtering/blocking tools. Currently, there are more than 40 parental empowerment tools available, including blocking/filtering tools, access control features available through the Internet Service Provider (ISP), and Web sites specifically geared toward children. Although each tool functions in a different way, the main goal is the same: to provide children with appropriate content and deter them from anything that could possibly be harmful to them. Although pornography is perceived as the greatest source of harm, there are other situations parents need to be aware of that may prove risky for their children. One example is chat rooms. Pedophiles often lurk in chat rooms, attempting to lure children into providing information that may cause a safety risk, or, more seriously, persuade the child to arrange a physical meeting. Chat rooms are covered under the scope of many blocking tools, but pedophiles may find ways that allow the child to supply information without raising a flag from the filtering device.

The most important ingredient in protecting children online is parental education and involvement. Unfortunately, there are no products that will fill all needs or be impossible to disable. Therefore, parents must educate themselves, become comfortable with the Internet and communicate with their children about these risks.

In the following paragraphs, the characteristics, both positive and negative, of four blocking tools will be discussed. This information will further clarify that a combination of technology and parental involvement is the most useful strategy in protecting children online.

Some filtering/blocking tools block content that appears on a "bad for kids list," such as sites that contain sexual content, violence, or the Federal Communication Commission's "seven dirty words." Other tools filter out all content unless it appears on a "good for kids list." Parents must first be aware that filtering/blocking tools are not a completely reliable source. Many tools utilize a keyword-blocking scheme that will block any content that contains certain words. Therefore, pages with the words "sexually linked trait" or "asexual reproduction" may be blocked. Important information about safe sex and sexually transmitted diseases will also go unseen. Unfortunately, children may miss out on educational content due to this technique.

The examples used in the following paragraphs do not encompass the entire list of available filtering/blocking tools. For the sake of brevity, a small group has been chosen to demonstrate the function of filtering/blocking tools and their characteristics.

The first example is **Access Management Engine,** or AME. AME is supplied by Bascom Global Internet Services, Inc., with a website at http://www.bascom.com. AME software allows parents and libraries to provide content that custom fits their educational needs. The "good for kids list," which contains content selected by the parent, teacher or librarian, is the only content accessible to the child. If the child requests content that does not appear on this list, a "not allowed" Web page is generated. One of the positive aspects of this tool is its scope. AME applies to Web sites, chat services, inbound and outbound e-mail, as well as newsgroups. In addition, this tool may be easier for parents and teachers because there is no software installation involved; AME products reside on the network center of the Internet Service Provider. AME allows designated users to create fully customizable "allow lists" and apply them to individual computers or groups. The weakness with this product lies in the accessibility of designated users' passwords. Each designated user requires a password; therefore, if a child were to obtain an adult's password, he could easily bypass the "allow list" and gain access to all Internet content. This is a recurring problem with filtering/blocking tools; each product described here is susceptible to this problem. If the child can obtain the password and maneuver his way around the system, he can easily control the content accessed. Other products similar to AME are Bess (http://www.n2h2.com) and I-Gear (http://www.urlabs.com).

**America Online Parental Controls** (http://

continued on page 24

## Filtering Tools

continued from page 23

www.aol.com) is a tool that comes as a feature of the ISP service. All AOL users have access to Parental Controls, and they are easy to configure and apply to children's accounts. Parental controls are custom controls that limit children's access to the Internet and other AOL content. Controls are divided into three categories, Kids Only, Young Teen, and Mature Teen. Kids Only accounts allow limited access to Internet content while they have full access within the Kids Only portion of AOL. A positive aspect of this account is that an account designated as Kids Only will not be able to send or receive instant messages. Instant messages are private messages sent between users of the service who are logged on at the same time. Similar chat room restrictions are also applied. Young Teen accounts are limited to some AOL content and features. Young Teen accounts will not be able to send or receive email attachments unless otherwise customized. Mature Teen accounts can go anywhere on the AOL service and use all AOL features, but mature content will be blocked. These controls have a wide range of coverage, which is a positive feature parents should take advantage of. A similar product is Mayberry USA Filtered Internet Access Accounts (http://www.mayberryusa.net/).

**Cyber Snoop** (http://www.pearlsw.com), priced at $49.95, is an Internet monitoring and control software that produces a complete trail of all Internet activity. The password holder is able to read contents of e-mail, see Web sites visited, and read chat communication. Cyber Snoop's customizability allows the parent/educator many different options, such as controlling access to the Web while allowing unlimited access to e-mail. Keyword blocking prevents users from supplying names, addresses, etc. if they arrive at a Web site that requests such information. One of Cyber Snoop's strengths is the flexibility of configuration. The combination of options available to the administrator should easily meet any parent or librarian's needs. Cyber Snoop also has some technological features that make it difficult for even a techno-savvy child to disengage the device. The log will also be useful to administrators, as it is available for future reference and may allow guardians to set useful guidelines based on content the child has previously viewed. Other products that operate in a similar manner are The SafeSurf Rating Standard (http://www.safesurf.com) and Net Shepherd World Opinion Rating Service (http://www.netshepherd.com). Products similar to Cyber Snoop in structure and usage are Cyber Patrol (http://www.learningco.com) and GuardiaNet (http://www.guardianet.net).

The last tool is **Net Nanny** (http://www.netnanny.com). Net Nanny is priced along the same lines as Cyber Snoop, and is designed for security purposes in the home, school and business. The consumer has complete control over all content that passes through the PC. Net Nanny also has the unique feature of BioPassword technology, which is able to identify who is typing on the keyboard. The software will work with all browsers, email programs, newsgroups, ISPs and chat services. It should be noted that BioPassword is a fairly new technology. Configuration options on Net Nanny are similar to those provided by Cyber Snoop. The user can choose to establish a log that monitors all sites visited, programs used and words and phrases typed or received. Net Nanny can also be configured to block out words/phrases decided to be inappropriate, such as "where do you live?" or "what is your name?" This is probably the tool's best feature, as it may help to decrease the child's risk of finding himself in a dangerous situation while chatting. The BioPassword feature may also alleviate the risk of children overriding the password and gaining access to the configuration options. If the password is compromised, the BioPassword technology will be able to further identify the user and conclude he is not the administrator. Concerning classification content, Net Nanny's "can go" and "can't go" lists are researched and updated using information from CyberAngels Internet Safety Organization, Safeguarding Our Children, United Mothers and other organizations which seek to rate online content for the protection of children. Lastly, Net Nanny differs from other products on the market in that it allows its customer to have access to their "block lists", so parents can know specifically what materials is being screened out. Most companies that produce filtering tools keep their block lists proprietary and do not release them to the public. A similar product is CYBERsitter (http://www.cybersitter.com).

***Unfortunately, parents and educators are not guaranteeing safety for their children through the tool itself.***

The above filtering/blocking tools will provide the parent with a greater sense of security than if the child were allowed to freely utilize the Internet, email, and chat rooms. The most apparent weakness of each tool is the child's ability to disable the tool or find ways around its control. If technology such as BioPassword becomes very reliable, however, it will be harder for children to assume administrator status and change configuration options. Until such technology is advanced, it is important for parents to supplement a filtering/blocking tool with other resources. Unfortunately, parents and educators are not guaranteeing safety for their children through the tool itself. Children are still at risk of being abducted or harassed as a result of online communication. Simple guidelines set by the parent, however, may alleviate this problem and create a greater sense of trust between parent and child.

Larry Magid, a *Los Angeles Times* writer who has authored numerous columns on children's safety, advises "the best way to assure that your children are

continued on page 25

## Filtering Tools

continued from page 24

having positive online experiences is to stay in touch with what they are doing." (Magid, 1998). This is probably the most useful approach a parent/educator can take in making their children's online experiences safer and more enjoyable. Of course, parents are not able to be at their child's side each and every time they interact online. However, procedures such as sharing an email account with your child or monitoring any files downloaded to the computer may alleviate some worry on the part of the parent.

Parents need not overreact in their guidelines; simply establish a mutual trust that will govern the child's online interactions. Essentially, the same parenting skills used in the real world can be applied to the cyber world. If adamantly told not to do something, a child may rebel and do it regardless of the warning. The same principles apply to online interaction. Therefore, parents/educators should allow the child enough freedom on the Internet but also protect safety and privacy.

There is much to be learned from children. If you are a parent who is uncomfortable around computers or are an inexperienced Internet user, ask your child to help you log on and point out certain things while surfing. You can inquire as to what content they usually access or how to better utilize your online service. When getting started online, try to visit sites centered on children, such as Bonus.com's SuperSite for Kids (http://www.bonus.com) or Disney's Blast Online (http://www.disney.com). These sites provide children with a contained environment that features a multitude of fun and educational activities. Bonus.com boasts more than 900 activities all in one place, and is a free site accessible to those who have World Wide Web access. Disney, for a small monthly fee, provides D-Mail and D-Browser, which are powerful communication tools that allow different levels of communication settings for each member of the family. As you become an experienced Internet user, you will naturally become increasingly more active in your child's online experiences. If you are having trouble getting started, try reading Donna Rice Hughes' new book, *Kids Online: Protecting Your Children in Cyberspace*. If you are familiar with the Web and looking for useful information, try Barbara Feldman's syndicated column, "Surfing the Net with Kids" at http://www.surfnetkids.com. The column reviews five Web sites each week, and the online archive is useful for accessing previous columns by subject or date. By establishing a plan of action and spending time with your children, you are accomplishing two goals: becoming more educated and establishing a mutual trust.

**References**

Hughes, D.R. and Campbell, P. T. (1998). *Kids Online: Protecting Your Children in Cyberspace.* Grand Rapids, MI: Fleming H Revell Co.

Magid, L. (1998) Child Safety on the Information Highway. http://www.safekids.com/child_safety.htm. October 22, 1998.

*The author is a Senior Technical Associate at AT&T Labs-Research in Florham Park, New Jersey. She co-authored the Technology Inventory: A Catalog of Tools that Support Parents' Ability to Choose Online Content Appropriate for their Children. Some of the content appearing in this article was taken from the Inventory, and further information can be found at http://www.research.att.com/projects/tech4kids/.*

## APSAC's Five Day Child Forensic Interview Clinic

**March 7-12, 1999 (in conjunction with Huntsville Symposium on Child Sexual Abuse)**
**May 30 - June 5, 1999 (in conjunction with APSAC's 7th National Colloquium, San Antonio, TX)**

APSAC's comprehensive interview clinic is an intensive forty-hour training experience which provides personal interaction with leading clinicians, researchers, and trainers in the field of child forensic interviewing. The interview practicum component provides participants with experience interviewing actual children in a supportive environment with constructive feedback offered to build and improve specific professional skills.

To add your name to the Forensic Clinic Mailing List, please complete and return this form by fax to 312-554-0919.

Name _____ Title _____

Agency Name _____ Address _____

City _____ State _____ Zip _____

Phone _____ Fax _____ E-mail _____

# Protecting Children's Privacy on the Internet

By Deirdre Mulligan, Staff Attorney Center for Democracy and Technology

FEATURE

The Internet offers children a tremendous opportunity to exchange ideas and participate in a world outside their window. Using the Internet, children can learn about faraway places, communicate with each other, and publish their own Web pages with the help of their parents and teachers.

However, the interactivity provided by the Internet raises some troubling issues too. The ease with which children can reveal information about themselves to others – through the click of their mouse, or through participation in games, chatrooms, penpal programs, and other online activities – raises concerns. As a child "surfs" from one Web site to another their movements leave behind a trail, much like the footsteps one leaves in the beach sand. This information can be used by Web site operators to improve the content of their site, or to target advertisements based on a child's activities. Unlike television and other passive media, the Internet allows children to interact with others without ever leaving their room. And alarmingly for many, these interactions often occur without parental knowledge or supervision.

***Only 7% of sites collecting information from kids notified parents of the practice, and only 23% even suggested that children speak to their parents before giving information.***

This has particularly troubling ramifications for children's privacy. The Federal Trade Commission's "Privacy Online: A Report to Congress," delivered to Congress in June 1998, detailed some troubling practices by commercial Web sites targeted at children. The survey found that while 89% of children's sites were collecting detailed personal information from children, only half had an information practice statement of any kind, and fewer than a quarter had a privacy policy notice. Only 7% of sites collecting information from kids notified parents of the practice, and only 23% even suggested that children speak to their parents before giving information. The FTC's survey documented that online businesses have failed to respond to parents' concerns about their children's privacy and safety online.

At hearings held by the Federal Trade Commission in June 1997, law enforcement officials discussed the risks to children posed by chat rooms, bulletin boards, and other forums that allow those on the Internet, including children, to post information about themselves. Officials stated that a child's ability to disclose personal information – such as their e-mail address, name, home address, school, and phone number —to a wide array of strangers posed a risk to the child's safety.[1]

Privacy, consumer, and child advocacy organizations participating in the hearings focused on business practices which undermine adults' and children's privacy. Advocates emphasized that the transactional information generated during a child's visits to Web sites and participation in other Internet activities offers an unprecedented opportunity to monitor and analyze a child's activities and behavior. Through games, contests, and other lures, Web sites targeted at children are requesting — or requiring — that children provide personal information such as name, address, e-mail, information on likes and dislikes, and information on their families and friends, as the cost of participating in online activities. Through both passive and active information collection, online content providers create detailed individual profiles on children which can be used and disclosed for a variety of purposes.

Advocates, law enforcement officials and industry all agreed that protecting children's privacy and safety online was critical. Participants largely agreed that the ongoing collection of personally identifiable information from children undermined their privacy and, based on survey data presented at the workshop, was likely to scare parents into keeping their children off the Internet.[2]

**Rules to protect children's privacy**

With consensus on the need to protect children's privacy, one might assume that crafting such rules would be simple. But, as is often the case, the process of developing rules – in this case legislation – to accomplish a generally shared goal is far from simple. Fundamental questions about what is meant by privacy, and defining who is a child, as well as more complex questions such as what it means to "collect" information in an environment that generates data every time we "click" must be answered before appropriate rules can be crafted.

Simply stated, protecting information privacy requires developing a set of rules that ensure that limited data is collected for specific purposes and that this data is not used for other purposes unless the individual consents to such uses. This standard is used to govern information gathering practices in a variety of settings. For example, such rules provide that information collected during a doctor visit is used for your treatment but is not used to send you marketing materials or reassess your insurance premium.

How does this work for children in the online environment? A proposal to protect children's privacy

[1] *See Federal Trade Commission Web site, Comments and Transcripts of the Online Privacy Workshop. http://www.ftc.gov*

[2] *Id.*

continued on next page

## Protecting Children's Privacy

continued from page 26

must take into account the inability of young children to comprehend and consent to the collection and use of personal information; the need for parental involvement in children's online activities involving personal information; the potential risk to children posed by the public posting of information that facilitates contact (both online and offline) with a child; and the need to ensure that business practices and privacy protections do not inappropriately interfere with children's ability to access information and receive information that they have requested.

**First efforts**

Initial proposals to protect children's privacy in the online environment recommended that personal information of those 16 and under only be collected with the knowledge and consent of a parent.[3] It also created a parental right to gain access to information held by Web sites about their child

By requiring all Web sites to treat children differently from the rest of the population, this first proposal created an expectation that Web sites should request information about age. Because the rules applied to activities as simple as responding to an e-mail request for information, the proposal could have led to rules that actually increased the collection of data as people sought to comply.

The proposal didn't reflect the needs, and rights, of older minors to have privacy from their parents in certain limited circumstances. For example, if parents are required to have notice and give consent every time their 15-year-old gives out his or her e-mail address, these older teens may be reluctant to seek out information and ask questions about matters that they wish to keep confidential from their parents. Couple this with the rule that provides parents with access to any information their teenager provides to a Web site and we can imagine some rather unappealing results.

For example, there are Web sites that offer teens information about contraceptives, health concerns, sexuality, child abuse, drug abuse and other controversial topics. Many of these Web sites respond to specific questions via e-mail and some collect information to provide children with resources in their community. Some Web sites offer interactive tests and quizzes that help teens assess their knowledge of health and other issues. While the Web sites at issue may be quite concerned about and respectful of teens' privacy, they would be bound under the proposal to provide parents with information about their children's search for potentially controversial information and provide parents with access to sensitive information their child might have revealed in seeking out information or services. Certainly, this should not be the outcome of a proposal to increase protections for teens' privacy.

The proposal, if implemented, would have chilled the protected First Amendment activities of older minors, and undermined, rather than enhanced, teenagers' privacy. While we agree that parents have an important role in protecting their teenagers' privacy, it seems that the proposal's emphasis on parental access may overlook older minors' interests.

Finally, the proposal treated all information that identified a child the same. While this makes sense at first blush, in application it would have limited children's ability to request and receive information in a timely fashion. The Internet allows information to be exchanged in a variety of ways. Some information is posted at Web sites for all to see, other information is tailored to the individual's request through search engines, the capability to request information through e-mail, etc. If children cannot request information through e-mail without their parent's consent, their use of the Internet may be limited. A loose analogy would be limiting children's ability to use the telephone to request information because in so doing they reveal their phone number.

**Recently Passed Federal Legislation**

Through the work of many interested and affected parties, the issues raised above have been sorted out. The Children's Online Privacy Protection Act, which was passed by Congress last October, represents a proposal to protect children's privacy and safety in a way that preserves First Amendment and privacy values and reflects the workings of the Internet. The bill is focused on commercial Web sites directed at children 12 and under and Web sites that collect information about age. It generally requires parental consent prior to the collection of personal information from children 12 and under. It also allows children to ask for and receive information via e-mail without parental involvement, provided that the Web site uses the information the child provides only to respond to the child's specific request. The bill is a major step forward for children's privacy and safety online, and it signals that Congress is serious about ensuring privacy in this new interactive medium.

[3] *See guidelines for protecting children's privacy submitted to the Federal Trade Commission by the Center for Media Education and the Consumer Federation of America; and also the initial Children's Online Privacy Protection Act (S. 2326) introduced by Senator Bryan (D-NV) that provide for parental notice and opt-out for those between 13 and 16.*

## The Case: Matt

Matt is a 17-year-old male who lives with his parents in a rural area. Both parents are employed in professional occupations requiring a lot of time away. When Matt was 16, he was expelled from an exclusive private school after he was found with marijuana. Matt entered public school and his grades dropped significantly, from being an honor student to barely passing. Matt was arrested with other adolescent males who were found in possession of alcohol at a party.

Matt has a history of shallow relationships with peers. Since the age of 14, he has experienced anxiety and uncertainty regarding his sexual orientation. While in boarding school at age 15 he shared adult pornography with a roommate, hoping it would lead to sexual contact. The boy allowed Matt to perform fellatio, but would not reciprocate. No further sexual contact or conversation about what happened ever occurred. Matt experienced limited sexual satisfaction, but was troubled over his activities and about the possibility of being discovered and labeled as a homosexual.

Matt had access to the Internet through a home computer, and plenty of unsupervised time to use it. He initially used the Internet to explore issues regarding different sexual orientations. Matt eventually discovered male pornography, which he found arousing. Matt soon found himself masturbating to many of the images he viewed. This led to Matt going into chat rooms and engaging in real-time conversations with others. Eventually, Matt was engaging in chat for five or six hours a day. Matt found himself turning down social events and time with friends so he could go home to "chat" and trade pornography.

Many of those in the chat rooms would send pornographic images and exchange pictures of themselves with their friends over the system. Matt found himself collecting images of males his age and eventually of boys considerably younger than his seventeen years. Matt got access to a digital camera and took his own picture, including pictures of his naked body.

Matt eventually met a man who was a few years older than him, who lived nearby and was willing to meet for sex. Matt was nervous and the sex was not as satisfying as he hoped. Although he could have met with the same man again he decided not to. Matt next met a person online who was 14 years old. Matt engaged in a few conversations over a five-day period and found the conversations stimulating. Matt sent his facial pictures and then his naked pictures. He asked the boy if he wanted to meet for sex and the boy agreed. Matt arranged to meet the boy, crossing state lines to do so.

The day came to meet the 14-year-old and, as arranged, Matt drove into a fast food parking lot. Instead of meeting the boy, Matt was confronted by police detectives and placed under arrest. Matt was charged with attempting to meet an under-aged person for sex. His computer was seized and found to contain hundreds of child pornographic photographs.

## Case Response

Craig Latham, PhD
Forensic Psychologist
Boston, MA

This case presents a number of challenging clinical and forensic issues, as well as numerous opportunities for mental health professionals to be involved.

Matt reminded me of "Bobby," a clinical case example in *The Subtle Seductions*, Gertrude Blanck's wonderful book about object relations (Blanck, 1987, pp. 91-127). In it, she describes the impact on a child's development when parents are too busy or otherwise emotionally uninvolved. Although Matt undoubtedly had excellent childcare, I assume that as a child he had little contact with his parents because they were too busy with their careers. Later, he had even less contact when they sent him to boarding school. This is a recipe for pathological narcissism, an excess of self-love to make up for the absence of real love. Little information is given about Matt's life at boarding school. I am guessing that he was searching for interpersonal intimacy that was absent from his life but settled for sexual contact with a roommate. When that proved unsuccessful, he was confused, worried about his sexual identity, and still lonely. He also turned to drugs and alcohol, possibly for the excitement, possibly to help medicate the beginnings of depression.

When Matt returned home, he began to use the Internet, at first just to relieve boredom. He discovered the possibilities of chat rooms to fill time, and they also served as another avenue in his search for some emotional connection. Matt soon discovered pornography, which he used to stimulate his masturbation fantasies. Communication over the Internet—trading pictures and sexual fantasies—and masturbation became his substitute for relationships. When Matt needed more, he sought sexual contact a second time, thinking that would fill the void. Once again, he did not find the sex satisfying since it was emotional intimacy he sought, and he found none with an older man he hardly knew. Matt then began to focus on communicating and trading pictures with younger boys, most likely because they looked up to him and

continued on next page

continued from page 28

did not threaten his competence. Putting his own needs first, he sought sexual contact a third time, overlooking the fact that his intended partner was too young to consent, and he was arrested by an undercover officer.

Matt has several major treatment needs that I will arbitrarily divide into five areas. First and foremost when working with any child who has engaged in sexual behavior that could harm another, the treatment plan must include enough supervision and structure to effectively prevent the child from repeating the behavior. This obviously is necessary for the safety of potential victims, but it also is necessary for treatment purposes. A child who is allowed to continue sexually abusive behaviors will not take treatment seriously and will have little incentive to change. When he was arrested, Matt was preoccupied with sexual fantasies, seeking sexual materials, or seeking sexual contact. Appropriate supervision must include blocking his access to the Internet and pornography, as well as preventing him from having sexual contact with inappropriate partners. It seems unlikely that his parents—or any other parent for that matter—would be able to provide that level of supervision twenty-four hours per day. Even if an after school program could be arranged, there are still evenings and weekends to worry about. Due to the pervasive, obsessive quality of Matt's sexual behavior, I would recommend a residential treatment program that specializes in sexual behavior problems, as this is the only setting where adequate supervision could be assured around the clock.

Matt's second treatment need concerns the fact that he feels empty, alone, and disconnected. This is worthy of treatment in its own right, but it also represents a major risk factor for additional inappropriate sexual behavior. Long-term, dynamically-oriented therapy has been the traditional treatment of choice, especially to deal with feelings of deprivation and abandonment in children and adolescents. Recent work with sex offenders, however, suggests that significant gains also can be made in much less time with cognitive/behavioral groups that emphasize social skill training, empathy, and analysis of individual behavior patterns that serve as obstacles to genuine relationships. I would recommend a sex offender-specific residential treatment program that could provide both forms of treatment.

The third treatment issue is that Matt's preoccupation with sex, which originally began as a search for emotional intimacy, now has been reinforced repeatedly through orgasm. Even if the personality deficits that led to this behavior were remedied, it is very likely that Matt would continue his preoccupation with sexual matters because it feels good. Therefore, he also needs cognitive/behavioral treatment to deal with the addictive, physiologically gratifying aspect of his sexuality that is disrupting the rest of his life. Residential treatment programs that specialize in sexual behavior problems would also have treatment groups that teach a relapse-prevention approach to behavioral control, positive replacement behaviors, and empathy training. Although a thorough discussion is beyond the scope of this commentary, I would not recommend specific interventions to deal with the possibility of deviant arousal at this point due to Matt's age, the absence of sexual abuse in his history, and the relatively minor history of his own sexually abusive behavior. His interest in young children is still much more likely due to emotional factors rather than physiological conditioning, and treatment addressing those deficits probably would be more effective.

Matt's fourth treatment need, or potential need, is that he may be depressed and in need of medication. It is also possible that some anti-depressants, particularly the class known as selective serotonin reuptake inhibitors (SSRIs), would lessen the obsessive quality of his sexual thoughts and make it easier for him to participate in the other aspects of his treatment. This plan should be evaluated by a child psychiatrist, preferably one with some experience treating sexual behavior disorders.

Finally, Matt may have a problem with substance abuse, which shares many similar dynamics with inappropriate sexual behavior. If it appears he does have such a problem after an evaluation, a twelve-step program for substance abuse would fit nicely with cognitive/behavioral models of sex offender treatment.

My intervention as a forensic psychologist would depend on which of several possible roles I could be asked to play by various parties in the case. Since Matt was arrested, I assume there would be either a plea negotiation or a trial. I could be hired by the defense (essentially Matt and his family), the Court, or the prosecution, either to do an evaluation and make recommendations about treatment or to provide the treatment. My clinical formulation would be the same in each case, but the point at which it would be legally and ethically appropriate to see Matt and the nature of privileged communications, if any, would depend on who hired me.

**References**

Blanck, G. (1987). *The Subtle Seductions* (pp 91-127). Northvale, NJ: Jason Aronson Inc.

continued on page 30

# Case Conference

continued from page 29

# Case Response

Daniel Armagh
National Center for Prosecution of Child Abuse
Alexandria, VA

**What are the key issues from a prosecutor's perspective?**

The factual scenario presents circumstances under which Matt could be considered both a victim and an offender. In analyzing potential crimes of which he may have been a victim, as with any potential criminal conduct of a sexual nature involving children, it is important to determine the statutory age of consent under relevant local, state, and federal statutes. Because Matt is 17, he is over the age of consent under some state laws for crimes involving otherwise legal sexual activity between consenting adults, and therefore, the prosecutor may be left with pursuing federal charges, if appropriate, for some of the offenses committed by and against Matt discussed herein. Other crimes committed by Matt clearly are actionable in either state or federal court. The prosecutor should be aware of all charging options, to include selection of jurisdiction before an appropriate determination can be made as to disposition of the case.

A second issue a prosecutor must resolve is whether to certify Matt as an adult for prosecution, or whether it is appropriate under the circumstances to proceed under the juvenile code and attempt to have Matt adjudicated delinquent. Given Matt's history, a prosecutor may want to determine how cooperative Matt can be in assisting an investigation against adult perpetrators who may have victimized him. Only after an appropriate assessment by a qualified therapist as to whether Matt is emotionally and psychologically ready to participate in such an investigation can the prosecutor make an informed decision. In addition, law enforcement should be aware of any unique legal requirements regarding the interview or interrogation of a juvenile target of an investigation, such as whether an adult or parent need be present during the advisement of rights before questioning begins.

Matt's possession of adult pornography may constitute an offense, depending on the standards set by his community regarding obscene pornography, however, in most communities in the United States this would not be a viable charge. It may, however, provide the basis of charges against an adult for corruption of a minor (Matt) or other similar charges if one could prove that the pornography was supplied to Matt by an adult as a grooming device for sexual exploitation of Matt.

Matt's act of fellatio on his roommate is a violation of a deviate sexual intercourse with a minor statute or a similar statute in most jurisdictions, even if the roommate was "allowing" or "consenting" to the act. At the age of 15, the roommate was not legally competent to consent to the act and most statutes read "any person commits a felony when he engages in ...with a person under sixteen." This charge is probably still viable under any statute of limitations analysis, although it may not be a strong case to bring to a jury if the roommate is a "reluctant victim" or his testimony fails to make a case against Matt that a jury would consider credible beyond a reasonable doubt.

The images Matt initially found on the Internet involving male pornography are disturbing but probably not criminal unless they include child pornography. Access by children to otherwise legal material on the Internet is thus far not criminal. However, Matt may in fact have committed a crime when he began trading pornographic images over the Internet if those images were:

1. visual depictions of children under the age of 18 engaging in sexually explicit conduct.
2. efforts by adults to act on or in furtherance of chat room conversation of a sexual nature and/or solicitation of a minor over the Internet to attempt a face to face meeting for the purpose of acting on those sexually explicit conversations.
3. If possession of those materials and sending same to other minors corrupted them in violation of statutes prohibiting the sexual abuse of a minor by dissemination of such materials if such images were child pornography or could be linked to grooming actions directed at children.

Federal law regarding sexual exploitation of minors also criminalizes such behavior under Title 18 U.S.C. Sections 2251 et seq. and 2422, 2423 et seq. as well as other statutes.

When Matt began collecting and sending images of child pornography, he violated both state and federal laws against possession and transmission of child pornography. Moreover, when he began photographing himself in the nude and sending those pictures to other children for the purpose of luring them over the Internet, he became a producer of visual depictions of children engaging in sexual acts, in violation of numerous state and federal statutes.

The factual scenario does not indicate whether Matt met the adult male who sexually exploited him over the Internet or at choir practice. It matters only in that certain crimes committed over the Internet must have a federal nexus to invoke criminal sanctions under federal statute. The abuse is a criminal offense unless Matt is deemed under state law to be at the age of consent and no other act committed is a violation of law per se. Even if Matt's abuser cannot be charged under state law, if a federal nexus can be proven, charging options under federal statutes should be considered because federal law regards anyone under the age of 18 a child, irrespective of what state law provides. This aspect of the case can be a point of nego-

continued on next page

## Case Conference

continued from page 30

tiation for the prosecution team with Matt and his parents/attorney in identifying and prosecuting this individual, who more likely than not has many more child victims presently unknown to law enforcement.

When Matt crossed state lines in furtherance of his online suggestive conversations with a 14-year-old boy, he again violated federal law (and state law in most jurisdictions) by enticing a "minor" over the Internet to commit an unlawful sexual act and attempting to meet for the purposes of committing child sexual abuse. Matt had the requisite intent to engage in sexually explicit conduct with his victim, and the possession of child pornography on his computer is powerful corroborating evidence of Matt's criminal intent, indeed his criminal lifestyle.

The search and seizure of evidence documenting Matt's computer-assisted sexual exploitation of children is concerning beyond the usual fourth amendment analysis. Questions about who else uses the target computer and for what purposes are important in conducting a lawful search and seizure of the computer and its peripherals. Does the computer contain work protected by the Privacy Protection Act? Has law enforcement complied with the Electronic Communications Privacy Act, in addition to the usual protections afforded citizens such as Matt, under federal and state constitutions? What is the legal exposure to the prosecutor, law enforcement and allied child abuse professionals if these laws were violated in the search and seizure of Matt's computer? What is a best practice protocol for securing the chain of custody of electronic evidence and does it ensure meeting the best evidence requirements once the unique nature of this electronic evidence is introduced at any proceeding involving Matt? How old was the e-mail evidence that was seized and was law enforcement aware that the age of the e-mail dictates what due process was required? Were the chat room conversations and session logs with Matt by the undercover police officer properly documented to challenge the most popular defense used by offenders in online cases: government entrapment?

The complexity of these issues demonstrates how training and expertise are critical to the successful investigation and prosecution of computer-assisted crimes against children. The victims of these cases are children, not computers, and this focus must not be lost. Computer-assisted child exploitation cases still involve predators stalking children with the same criminal designs they have always harbored, only now with an instrument of technology that is more secretive and insidious than the lures used before the computer. Because of the multi-jurisdictional issues that crimes committed on the Internet involve, the optimal approach is through a functional and competently maintained task force comprised of state and federal agencies. This is not always possible for a multitude of reasons outside the scope of this case response.

Matt is a victim. He is also a criminal predator. The wise prosecutor will consult Matt's victims for their input, the all important multidisciplinary team for their assessment, and an appropriate therapist qualified to address the long-term implications for every option the prosecutor must weigh in the pursuit of justice for everyone.

# JOURNAL HIGHLIGHTS

*The purpose of Journal Highlights is to inform readers of current research on various aspects of child maltreatment. APSAC members are invited to contribute to Journal Highlights by sending a copy of current articles (preferably published within the past six months), along with a two or three sentence review to Rochelle F. Hanson, Ph.D., National Crime Victims Research & Treatment Center, Medical University of South Carolina, Charleston, SC 29425 (FAX 843 792-2945) e-mail: hansonrf@musc.edu.*

## Sexual and/or Physical Abuse

### Medical Examinations of Sexually Abused Children: Legal Implications

This article discusses the socio-legal implications of medical examinations of sexually abused children and adolescents. The effect of these examinations on criminal vs civil court cases is discussed, and recommended research directions and barriers to be overcome are addressed.

**De Jong, A.R. (1998). Impact of child sexual abuse medical examinations on the dependency and criminal systems. Child Abuse & Neglect. Vol 22(6), 645-652.**

### The Link Between Childhood Sexual Abuse and Adult Alcohol Abuse in Women

Though a relationship between childhood sexual abuse and later alcohol use among women has been documented, little is known about the pathways that link these 2 variables. A tension reduction hypothesis posits that emotional distress precedes substance usage. The posttraumatic stress disorder (PTSD) symptomatology resulting from childhood sexual abuse is examined as a possible source of emotional distress that may cause subsequent alcohol use. A sample of 2,994 adult women was selected and interviewed on 2 occasions 1 year apart and childhood rape history, lifetime PTSD symptoms, and lifetime alcohol use were assessed. Path analytic techniques were used to evaluate the mediating role of PTSD symptoms on the relationship between childhood rape and subsequent alcohol use. A history of childhood rape doubled the number of alcohol abuse symptoms that women experienced in adulthood. Path analysis and cross-validation results demonstrated significant pathways connecting childhood rape to PTSD symptoms and PTSD symptoms to alcohol use. Results suggest that PTSD symptomatology that develops after childhood rape may be one of many variables that affect alcohol abuse patterns in women who were victims of childhood sexual abuse.

**Epstein, J.N., Saunders, B.E., Kilpatrick, D.G., & Resnick, H.S. (1998). PTSD as a mediator between childhood rape and alcohol use in adult women. Child Abuse & Neglect. Vol 22(3), 223-234.**

### The Behavioral Manifestations of Child Sexual Abuse

This paper is organized into several broad areas, including an update on research assessing the behavioral manifestations resulting from sexual abuse, the explication of a model that can be useful to guide future research and an examination of research that is needed to help us further understand abuse impact. Contexts examined are familial as well as reflective of an individual child or adolescent's processing of the abuse experience.

**Friedrich, W.N. (1998). Behavioral manifestations of child sexual abuse. Child Abuse & Neglect. Vol 22(6), 523-531.**

### Improving Quality and Quantity of Information Obtained from Victims of Child Sexual Abuse

This article reviews the literature on factors that influence children's competence, and discusses ways in which investigative interviewers can maximize the quality and quantity of information they obtain from alleged witnesses and victims. The authors found that children are often the only available sources of information about possible abusive experiences. Research has shown that children can, in fact, be remarkably competent informants, although the quality and quantity of the information they provide is greatly influenced by the ways in which they are interviewed. Methods by which investigative interviewers can maximize the amount and quality of information they elicit from alleged victims are described.

**Lamb, M.E., Sternberg, K.J., & Esplin, P.W. (1998). Conducting investigative interviews of alleged sexual abuse victims. Child Abuse & Neglect. Vol 22(8), 813-823.**

### Review of Literature and Current Controversies on Memories of Childhood Sexual Abuse

This article was developed by the International Society for Traumatic Stress Studies to inform professionals and the public about the complex and important issues that are involved in the current controversy about memories of childhood sexual abuse. It addresses the questions of childhood trauma, traumatic memory, the memory process, clinical issues and forensic implications pertaining to this controversy. The authors have tried to present a balanced review of these issues. As an international organization dedicated to promoting the best research and education in this field, they believe it essential that people who grapple with this controversial topic be equipped with the most accurate and comprehensive information possible.

**Roth, S & Friedman, M.J. (1998). Childhood trauma remembered: A report on the current scientific knowledge base and its applications. Journal of Child Sexual Abuse. Vol 7(1), 83-109.**

## Other Issues In Child Maltreatment

### Treating Intrafamily Abuse: The Abuse Clarification Process

One aspect of treatment for child abuse and neglect addresses the attributions that the child victim, offender, nonoffending parents, and other family members have about the occurrence of the maltreatment. This paper describes a formal approach for abuse clarification to be used with families in which maltreatment has occurred. The 4 primary components of the abuse clarification process are: (1) clarification of the abusive behaviors; (2) offender assumption of responsibility for the abuse; (3) offender expression of awareness of the impact of the abuse on the child victim and family; and, (4) initiation of a plan to ensure future safety. The process of abuse clarification is described and suggestions made for appropriate use of the procedure. Five case examples are presented as illustrations of the process.

**Lipovsky, J.A., Swenson, C.C., Ralston, M. E. Saunders, B.E. (1998). The abuse clarification process in the treatment of intrafamilial child abuse. Child Abuse & Neglect. Vol 22(7), 729-741.**

continued on next page

# Journal Highlights

continued from page 32

## The Effects of Abuse and Community Violence on Children's Symptomatology

With a sample of 188 maltreated and 134 nonmaltreated children between the ages of 7-12 years, this investigation employed a 1-year longitudinal design to conduct an ecological-transactional analysis of the mutual relationships among community violence, child maltreatment, and children's functioning over time. Indicators of children's functioning were externalizing and internalizing behavior problems and self-rated traumatic stress reactions, depressive symptomatology, and self-esteem. Rates of maltreatment, particularly physical abuse, were related to levels of child-reported violence in the community. In addition, child maltreatment and exposure to community violence were related to different aspects of children's functioning. Specific effects were observed for neglect and sexual abuse and for witnessing and being victimized by violence in the community. Finally, there was evidence that children and their contexts mutually influence each other over time. Results were discussed within the framework of an ecological-transactional model of development.

**Lynch, M., & Cicchetti, D. (1998). An ecological-transactional analysis of children and contexts: The longitudinal interplay among child maltreatment, community violence, and children's symptomatology. Development & Psychopathology. Vol 10(2), 235-257.**

## Evaluation and Review of Project SafeCare

Describes Project SafeCare, an ecobehavioral research and treatment project conducted with 116 families either reported or at risk for child abuse or neglect. Project SafeCare focuses on 3 areas of intervention: (1) home safety, (2) infant and child health care, and (3) bonding and stimulation (parent-child training). Each service component is conducted over 5 weeks. Two groups of families are served: a nonabuse, at-risk group is referred from a local hospital maternity center, and an abuse/neglect group is referred from the Department of Children and Family Services. Preliminary demographic data are reviewed along with indirect assessment data and measures including the Child Abuse Potential Inventory, the Parenting Stress Index, and the Eyberg Child Behavior Inventory. Four case studies are described to exemplify the effects of training provided to families. The implications for the current assessment data, treatment and outcome are also discussed.

**Lutzker, J.R., Bigelow, K.M., Doctor, R.M., & Kessler, M.L. (1998). Safety, health care, and bonding within an ecobehavioral approach to treating and preventing child abuse and neglect. Journal of Family Violence. Vol 13(2), 163-185.**

# CONFERENCES

## APSAC Discounts

**January 25-29, 1999.** ***San Diego Conference on Responding to Child Maltreatment.*** San Diego, CA. Sponsored by Center for Child Protection at the San Diego Children's Hospital. Call 619-495-4940.

**March 9-12, 1999.** ***Fifteenth National Symposium on Child Sexual Abuse.*** Huntsville, Alabama. Sponsored by The National Children's Advocacy Center. Call (256) 534-1328.

**June 2-5, 1999.** ***Seventh National Colloquium.*** San Antonio, TX. Sponsored by APSAC. Call 312-554-0166.

## Upcoming Conferences

**January 28-29, 1999.** ***Tenth Annual Stop The Hurt! Child Sexual Abuse Conference.*** Tupelo, Mississippi. Call Donna Benefield at (601) 841-3158.

**February 5-6, 1999.** ***The Fifth National HELP Network Conference***, Health Care Providers and Survivors Working Together for Change. San Francisco, California. Call (773) 880-3826.

**February 6-7, 1999.** ***National Human Sexuality & Health Educators Conference.*** Irvine, California. E-mail Bob Gaughran at www.robertg2@ioc.net.

**February 7-10, 1999.** ***The Governor's Conference on Best Practices in Juvenile Justice.*** Ft. Mitchell, KY. Call Cindi Miller (606) 622-2324.

**February 7-10, 1999.** ***National Network For Youth: Symposium '99.*** Washington, D.C. Call (202) 783-7949 ext. 103.

**February 8-10, 1999.** ***Second National Roundtable on Innovative Community-Based Partnerships.*** Jacksonville, Florida. Presented by the American Humane Association, Children's Division. Call Mickey Sumaker at (303) 792-9900.

**February 11-12, 1999.** ***Tenth Annual Working with Children of Color Conference.*** Sponsored by Starr Commonwealth. Albion, Michigan. Call (800) 837-5591, ext. 409; e-mail: pellw@starr.org.

**February 18-20, 1999.** ***SCPSAC Conference***. Charleston, SC. Sponsored by The South Carolina Society on the Abuse of Children. Call Rochele Hanson at (803)792 2945.

**February 24-26, 1999.** ***Imagine a Brighter Future: Providing Solutions for Children in Crisis.*** Los Angeles, California. Sponsored by Children's Institute International, LA, CA. Call Kimberly Clayton-Blaine at (213) 385-5100, extension 222.

**February 24-26, 1999.** ***Children '99 Countdown to the Millennium.*** Sponsored by the Child Welfare League of America, Washington D.C. Call (202) 638-2952.

**March 18-20, 1999.** ***The Sixth Annual Behavioral Informatics Tomorrow Conference.*** San Jose, California. Call Kevin at (650) 851-8411.

**April 7-11, 1999.** ***Claiming Our Future.*** San Antonio, Texas. Sponsored by the Association for Childhood Education International. Call (800) 423-3563.

**May 26-29, 1999.** ***First Canadian Conference on Shaken Baby Syndrome, Awareness, Prevention & Response; an Integrated Approach. Saskatoon, Canada. Hosted by The Saskatchewan Institute on Prevention of Handicaps.*** Call (306) 655-2512.

**June 2-4, 1999.** ***Imagine a Brighter Future: Providing Solutions for Children in Crisis.*** Los Angeles, California. Sponsored by Children's Institute International, LA, CA. Call (310) 274-8787, extension 116.

**June 3-4, 1999.** ***The 4th Biannual Violence Prevention Conference, Voices from the Community: Creating Solutions.*** Long Beach, California. Sponsored by The Violence Prevention Coalition of Greater Los Angeles. Call Anthony Borbon at (213) 240-8279.

**July 13-18, 1999.** ***Tenth Annual Sexual Assault Team Training.*** Rancho Bernardo, CA. Sponsored by The Pomerado Hospital Sexual Assault Team. Call 760-739-3444.

The National Data Archive on Child Abuse and Neglect will sponsor its annual Summer Research Institute on June 13-18, 1999. The Institute provides a unique opportunity for scholars to conduct secondary analyses in the field of child abuse and neglect. Participants represent a wide variety of disciplines and are selected on a competitive basis. Scholars, professionals involved in research, and advanced graduate students are all encouraged to apply. Fifteen applicants will be selected based on their previous research experience and level of commitment to following their work through to publication. For an application, contact the Archive at 607-255-7799, or on the Internet at www.ndacan.cornell.edu. Applications must be received by February 15, 1999.

ISSN 1088-3819 

# CALL FOR COMMENT

## Draft Practice Guidelines on Investigative Interviewing

APSAC's Task Force on Investigative Interviewing has drafted proposed Practice Guidelines, which are now available for member comment. Your input is critical to helping shape a final version of these important guidelines. Please call the Publications Department at 312-554-0166 to request a copy. You may also fax your request to 312-554-0919, e-mail APSACPubls@aol.com or download the draft Guidelines from our web site at www.apsac.org. The deadline for member comments is February 28, 1999.

# THANK YOU!

These APSAC members have generously made financial contributions in the last several weeks to support vital work of the organization. Their donations have strengthened APSAC's efforts to educate legislators, policymakers, reporters, and editors; to produce additional guidelines for practice; and to encourage promising student research in the field of child maltreatment. We greatly appreciate their generosity and commitment.

**Friends Level ($5-$50)**
Kathy L. Bell
Lynn Copen
Thomas W. Grove, MA
Mary Beth Phillips, PhD
Valerie Ross

**Supporter Level ($51-$150)**
Mary Ann Grochowski

**Patron Level ($151-$500)**
Raymond Shapiro
John Leventhal, MD
Samuel Gary

## The Katie Toth Memorial Education Fund

This special fund was established in memory of Mary Katherine Toth Komie, daughter of longtime APSAC volunteer Patricia Toth. Katie died at the age of 20 months and her family established the memorial fund, dedicated to the purpose of furthering professional education, in honor and memory of Katie, APSAC and the family of Katie Toth extend deepest thanks to all who support this fund.

Richard Krugman

APSAC

American Professional Society
on the Abuse of Children
407 South Dearborn Street, Suite 1300
Chicago IL 60605
P 312-554-0166, F 312-554-0919
E-mail: APSACMems@aol.com
http://www.apsac.org

Non-Profit Org.
U.S. Postage
PAID
CHICAGO, IL
Permit No. 4345