The Compiler

Illinois Criminal Justice Information Authority

Summer 1999

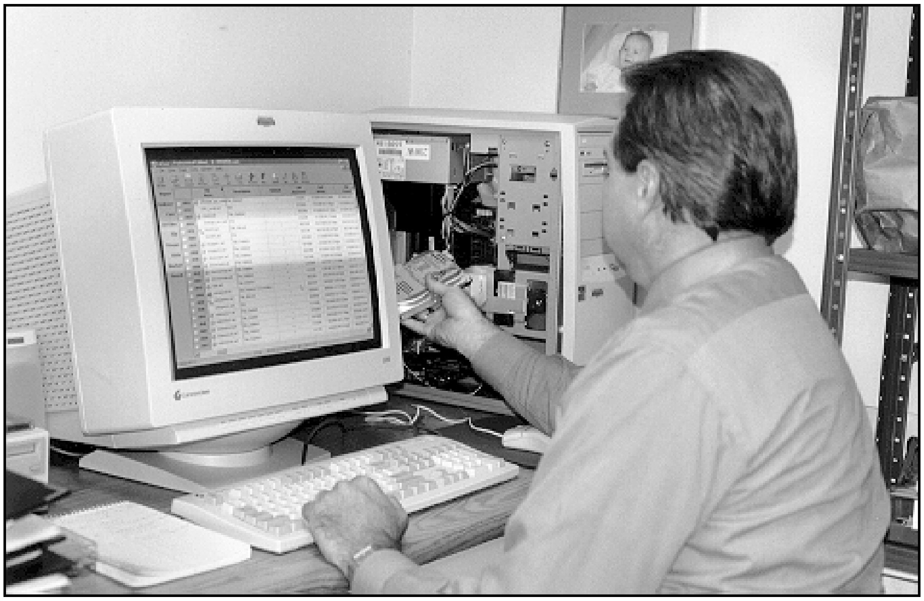
Inside

Features

Departments

Computer crime

Computers and the Internet have provided criminals ranging from pedophiles to common thieves with vast new opportunities. Meanwhile, criminal justice agencies have been finding unique ways of combating these cyber criminals. Our look at what's happening in Illinois begins on page 4.



Master Sgt. Jim Murray, of the Illinois State Police, reviews evidence retrieved from computers. Story on page 4.

The Compiler

Volume 19, Number 1
Summer 1999

THE COMPILER is published quarterly by the Illinois Criminal Justice Information Authority.

George H. Ryan
Governor

Candice M. Kane
Executive Director

Produced by the Office of Public Information

EDITOR
Daniel Dighton

ASSISTANT EDITOR
Cristin Monti

INTERN
Aurora Aguilar

Created in 1983, the Illinois Criminal Justice Information Authority is a state agency dedicated to improving the administration of criminal justice. The Authority works to enhance the information tools and management resources of state and local criminal justice agencies, and it serves as a statewide forum for criminal justice coordination, planning, and problem solving. It also is responsible for research, information systems development, and administration of federal anti-crime funds. The Authority's specific powers and duties are spelled out in the Illinois Criminal Justice Information Act [20 ILCS 3930/1 et seq.].

The Illinois Criminal Justice Information Authority is governed by a 15-member board of state and local leaders from the criminal justice system, plus experts from the private sector. Authority members help develop priorities and monitor their progress. The agency's day-to-day work is carried out by a full-time professional staff working out of the Authority's Chicago office.

E–mail Editor Daniel Dighton at <ddighton@icjia.state.il.us>

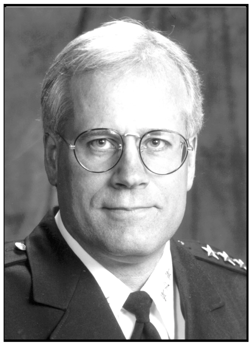
Printed by authority of the State of Illinois, August 1999. Printing order number: 00–001. Number of copies: 6,000. ISSN 1059–6569. Printed on recycled paper with soybean-based ink.

In Brief

Governor appoints Authority members

Gov. George H. Ryan recently appointed Elmhurst Police Chief John J. Millner and Kankakee County Sheriff Timothy F. Bukowski as members of the Authority.

Millner joined the Elmhurst Police Department in March 1972. He rose through the ranks and has been chief of the department since 1986. The department has a staff of more than 120 employees and an $8 million budget.



Millner

Millner earned his bachelor's degree at Lewis University in Romeoville, and he has a master's degree in law enforcement administration from Western Illinois University. He is a certified master investigative hypnotist and licensed polygraph examiner in Illinois. Millner is chairman of the Illinois Attorney General's Violence to Children Task Force, and president for Northeast Multi-Regional Training, the largest mobile training region in Illinois. He also is vice president of the Illinois Assocation of Chiefs of Police.

Millner replaces Roger Richards, the former police chief of Fairview Heights. Richards was appointed to the board in 1987 for a four-year term and was reappointed twice after that. His last term expired Jan. 18.

An eight-year veteran of the Kankakee County Sheriff's Department, Bukowski was appointed sheriff in 1996 and elected to his first four-year term in 1998. He was instrumental in researching and implementing video arraignment, which was first utilized in Kankakee County in 1994. He also introduced video visitation to the county detention center, replacing face-to-face visits between inmates and family.

Bukowski

Bukowski serves on the United States Attorney's Law Enforcement Executive Committee for central Illinois. He also is a member of the Illinois Police Training Institute Advisory Board and serves on the Attorney General's Missing and Murdered Children Committee. Bukowski replaces Robert Nall, former sheriff of Adams County.

Authority, ISP to implement new statewide records management system

The Authority announced in July that it will be working with the Illinois State Police to implement a fully integrated, statewide police records management system. The Authority has awarded ISP a grant of $873,000, including $655,000 from the U.S. Department of Justice's Byrne Formula Grant program and $218,000 in matching state funds, to begin the project, which will be conducted in close cooperation with the Illinois chiefs of police and sheriffs associations.

The new system will eventually replace existing systems used by the two agencies.

ISP has been using the Traffic Information and Planning System (TIPS) as their primary records system since 1973. The new system will provide them with improved information for allocating resources across Illinois and for combating crime.

The Authority developed and operates the Police Information Management System (PIMS), which is used by 58 county and municipal police agencies, mostly in the northern third of the state. PIMS is more than 8 years old and is in need of a rewrite, but it allows agencies to share information about enforcement and investigative activities. This model of information sharing will be a key component of a new, comprehensive, statewide system.

Federal fiscal year grants designated

The Authority recently received designations for several grants from the U.S. Department of Justice for federal fiscal year 1999, which began Oct. 1, 1998.

The **Residential Substance Abuse Treatment** (RSAT) program received $1,868,761 to continue providing residential substance abuse treatment to state prisoners. Most of the funds go to the Illinois Department of Corrections.

To be eligible for funding, programs must provide treatment for six to 12 months, offer services in a residential setting away from the general inmate population, focus on substance abuse problems, and develop inmates' social, cognitive, behavioral and vocational skills.

1999 funding for the RSAT program decreased from $1,924,928 in federal fiscal year 1998.

The **Local Law Enforcement Block Grant** program received $1,091,232 to provide equipment funding to local agencies. A request for proposals from law enforcement agencies will be issued in October. Grants are awarded for equipment purchases under $20,000.

About $8.7 million was designated for the **Juvenile Accountability Incentive Block Grant** (JAIBG) program, the same amount received last year. JAIBG funds may be used to build, expand, and renovate juvenile correction and detention facilities, administer juvenile accountability-based sanctions, and hire court and correctional personnel. Funding also may be provided for technology, equipment, and training to assist prosecutors in expediting the prosecution of violent juvenile offenders.

The **State Identification Systems** (SIS) program received $163,156 to assist the Illinois State Police in establishing, developing, or upgrading identification systems. SIS funding allows state police identification, DNA, and fingerprinting systems to integrate and remain compatible with similar programs used by the FBI

Funding for State Identification Systems decreased from $194, 711 in federal fiscal year 1998.

These awards are in addition to other programs for which federal awards have already been designated.

ISP funds livescan expansion

The Illinois State Police distributed $1.5 million toward juvenile justice efforts in the state at the close of fiscal year 1999. The funding will be used to purchase livescan fingerprint technology that allows state agencies to share juvenile criminal information.

Livescan equipment identifies juvenile offenders through a database kept by state police. More agencies will have access to criminal history records with the funding. "Police officers, state's attorney's, and all of those involved in the criminal justice system will know whether a young person is a first offender and what kind of behavior their criminal background includes," ISP Director Sam Nolen said.

Another $1.7 million is budgeted to continue livescan network expansion throughout the state in fiscal year 2000. This is in addition to federal funds available through the Authority for Livescan expansion.

Authority research presented at international conference.

Research analysts Jennifer Hiselman and Michelle Fugate were among the participants of the 6th International Family Research Conference in Durham, New Hampshire in July.

Hiselman presented information on the nature and extent of family violence in Illinois based on the Authority's family violence data collection project funded by the Administrative Office of the Illinois Courts. Fugate presented a briefing on the Chicago Women's Health Risk Study, a collaborative research project funded by the National Institute of Justice.

New publication released

The Authority launched a new publication series in July called "Trends and Issues Update." The four-page reports will provide an overview of important criminal justice trends and issues. The first four issues, which will be published over the next couple of months, are: "Trend in Illinois Crime: 1994-1998," The Juvenile Justice Reform Act," "Trends in Illinois Drug Arrests," and "Illinois Prison Population Trends."

Authority heads for the Illinois State Fair

The Authority will once again be at the Illinois State Fair this August, with a tent easily identified by the 30-foot McGruff the Crime Dog balloon outside. This year's tent will feature a storybook presentation of "A Trip to the State Fair," which was created by the Authority and has a child safety theme. In addition to the Big Book, which will be presented by guest readers, there are accompanying coloring books for children. Additional features at the tent include a new "Play It Safe" coloring book with McGruff and his nephew Scruff, and educational activities sponsored by the Illinois Coalition Against Sexual Assault. ■

High-tech evidence gathering: tapping into the computers of criminals

By Cristin Monti

Modern technology has eased the process of committing traditional crimes like embezzlement, identity theft, pornography, and extortion. Creating fraudulent documents, such as false identification cards, driver's licenses, insurance cards, and personal checks, has been simplified with desktop publishing software, scanners, and digital cameras. More serious crimes, such as murder, child exploitation, and illicit drug sales, also have been linked to a computer.

"You can have computer involvement in almost any kind of criminal case," said Master Sgt. Jim Murray, an investigator with the Computer Crimes Investigation Unit of the Illinois State Police. "Even drug dealers will use computers as repositories for information. They're businessmen like anyone else."

Once these crimes are brought to the attention of law enforcement, the process of gathering information from a computer is arduous. One false move could mean the loss of valuable evidence, and a much more difficult, if not impossible, case for prosecutors.

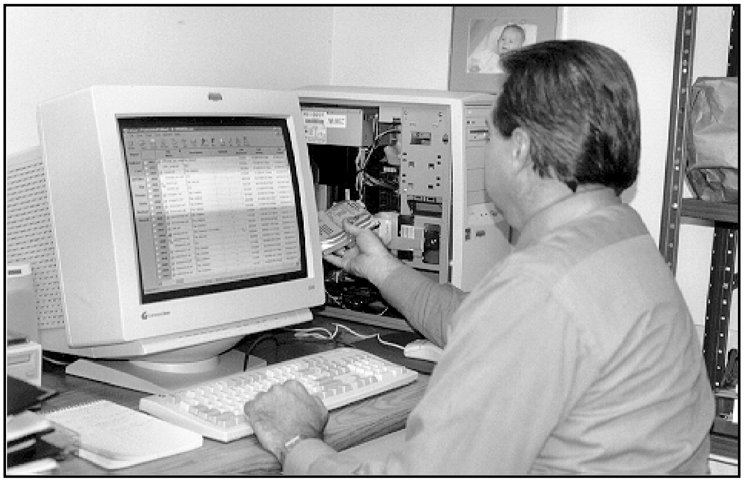


Photo by Cristin Monti

Illinois State Police Master Sgt. Jim Murray reviews evidence seized from computers.

Risky business

Preservation of the electronic crime scene requires some risky decision making: How should a suspect's computer be seized? Should a running computer be unplugged from the wall, or systematically shut down based on the unit's requirements? While these details may seem minor, they could have a significant impact on the results of an investigation.

Investigators assume that all hardware they encounter is rigged to destroy evidence, and gingerly work their way around each system. More seasoned criminals may even plant booby traps in their systems where standard commands or procedures could instruct the computer to destroy files.

Investigators' fears are compounded by the fragility of computer evidence. Cyber-crime evidence gatherers take painstaking care when approaching their investigations. In cases where a system is running, a photograph is taken of what is displayed on the monitor before taking measures to shut it down. Investigators seize the suspect's hardware, software, and manuals.

Steps are taken to ensure that both the equipment and data can be restored to the form in which it was seized. Photographs are taken of the computer's internal system and its connections. The unit also is searched for evidence of tampering, which could indicate a trap or self-destructive device.

Specially designed forensics software is used to create a mirror image of a computer's hard disk drives. Once the back-up file is created, investigators use other software programs to dig through the suspect's data — including erased, hidden, and encrypted files — in search of evidence that may be used in court.

Cristin Monti is a technical editor with the Authority's Office of Public Information.

Cracking encryption schemes presents a challenge to computer crime investigators, even with the forensics software available. At times, investigators rely on software manufacturers for assistance.

The unique nature of computer evidence means that it must be delicately handled from the moment it is seized. Equipment is stored in a cool area away from any magnetic field, which could affect potential evidence. Also, care is taken not to infect the computer with viruses from outside sources. Investigators compile documents from e-mail, word processing, database, and other software programs, such as those that could be used to enter another system without authorization.

While instances where evidence is recovered from a computer are increasing, investigators continue to rely on the paper trails a perpetrator may leave behind. "We're still a paper society," Murray said. "Rather than providing the only evidence in a case, computer evidence generally enhances the case."

Protecting equipment to preserve authenticity is a top priority in a computer crime investigation. In court, prosecutors must prove that information taken from an individual's computer was not modified; a mirror image of the files was made with a reliable mirroring process; and that the equipment was secured throughout the investigation, minimizing chances that data was altered.

Preserving the evidence

Proving the authenticity of computer-generated documents can be difficult. This evidence can be edited, intentionally or unintentionally, without leaving a trace. Like court cases that do not involve computer technology, a connection must be made between the person and the evidence. Prosecutors face the challenge of establishing who created an electronic document, its contents, the way in which it was created, and that it hasn't been altered.

"You can determine what happened and you can maybe even determine who did it, but unless you can preserve the evidence so that it is admissible in a court of law, it's not going to do you any good," Murray said.

Authentication can be proven with direct evidence, such as testimony by the creator of the electronic document, or with circumstantial evidence demonstrating the document contains information only the creator would know.

Defense attorneys also have become savvier in computer crime issues, giving investigators even more reason to be scrupulous when gathering and preserving evidence.

Training in forensic computer science is not yet widely available to investigators. The Federal Law Enforcement Training Center in Georgia, the National White Collar Crime Center in West Virginia, and the SEARCH group in California provide computer evidence training to computer specialists in law enforcement, including those in Illinois. The International Association of Computer Investigative Specialists also provides training.

While criminal activity involving computer technology has existed since the advent of the computer, the sheer number of computer crimes exploded with the introduction of the Internet, said Master Sgt. Al Manint, executive officer of the Computer Crimes Investigation Unit.

"A lot of crimes in the past were not even brought to the attention of law enforcement," Manint said. "We didn't have the laws, the knowledge, or law enforcement training in the area to handle these cases."

Advancements in computer hardware and software are seen almost daily, and technology to aid in crime investigations is improving just as rapidly. Individuals may attempt to cover their tracks by renaming and encrypting files, and they may store incriminating material on removable media, like Zip disks and CD ROMs, but investigators use their own sophisticated software to penetrate a computer system's various layers and unveil hidden evidence.

"In one case, a guy created a note to a hit man instructing him on how to kill his uncle, what to do with the evidence, and how to contact him later. He never saved the document but I found parts of it in the hard drive," Murray said.

Al Manint

The law enforcement community has heightened its awareness of the presence, use, and gathering of computer-generated evidence in recent years. Illinois has one of the highest numbers of institutions and corporations dealing with technology in the country, prompting even more local law enforcement efforts to address computer crime. "This area of criminal activity has really opened doors of communication between law enforcement and the private sector," Manint said.

Internet cases typically lead law enforcement computer specialists across the country, and at times become international investigations. Evidence may be obtained from a suspect's local computer, from equipment owned by service providers who may be located in another state, and from individuals on the other end of the case. Local, federal, and international law enforcement agents often collaborate in these situations, Murray said.

Legislation on crimes involving computer technology differs from state to state, but they are more synchronized across the United States than other boundaries, Murray said. Especially in cases of Internet-generated child pornography, trying to find legislation that fits the crime poses another challenge for investigators and prosecutors. "Legislation hasn't necessarily kept up with technology," Murray said.

On-line criminals are savvy

The actions of on-line child solicitors indicate a heightened awareness of methods to secure incriminating information and graphic images in their computers, Murray said.

"People who commit these crimes are familiar with computers," he said.

“They instruct the child not to save messages and they format information so that it is not easily available.”

Jim Murray

A hacker’s intrusion to military sites, and bank and credit bureau systems may be proven with evidence taken from his computer, but because of underreporting, it is unclear to law enforcement officials how often these crimes occur.

The theft of proprietary information from corporate computer systems is most often unreported, as many companies choose not to publicize a loss of trade secrets, customer databases, and product designs for fear it will scare off investors, Murray said. Also, confidential information may be copied, rather than removed, making it virtually impossible to know data was stolen until it is too late.

“Any time contact can be made through the Internet, there is a potential for intrusion,” Murray said. “In most cases, people are unaware they’ve been intruded upon. The best hacks are the ones you never know about because you don’t know they were there.”

Employees, not hackers, are to blame in many data theft cases, Murray said. Company workers often exceed authorized access to obtain confidential data. Many companies are too lax in the way they protect sensitive information, he said.

“You don’t have to be a programmer today to work a computer,” he said. “Software is more user-friendly. Computers are more user-friendly. You don’t need to be technically competent to commit a computer crime, and there are a lot of people doing it.”■

Identity theft can mean big headaches for consumers

By Todd Czapski

It sounds like a plot device for an espionage thriller or perhaps a science fiction novel. But identity theft — the unlawful use of another person’s name, birth date, or Social Security number to obtain credit, money, or goods and services — is an all-too-common and increasingly pervasive problem.

“It can happen all too easily, and it can happen to anybody,” said Master Sgt. Jim Murray, a computer crime investigator with the Illinois State Police. “There’s really very little way to protect yourself, if somebody gets your information — and if they steal an existing account, they don’t even need much information.”

Theft can be simple

Perpetrators of identity theft can obtain information about their victims in surprisingly simple ways. In some cases, the perpetrator may prey on someone whose personal records are close at hand — a roommate, relative, or someone employed in a household. Crooks may also salvage vital information from discarded receipts, financial statements, credit card applications, or other pieces of mail. “It’s much easier to assume an existing identity that has a credit rating, and do that successfully, than it is to create a brand new identity,” Murray said.

Todd Czapski is an administrative assistant with the Authority’s Office of Administrative Services.

On the high-tech front, vital information can be illegally intercepted through Internet transactions. Consumers can get increased security with 140-bit encryption Web browsers, and many companies guarantee protected on-line transactions. Often, however, consumers fall right into the hands of on-line crooks. Some Web sites, for instance, purportedly offer free items for information, and request visitors to give personal information through on-line forms.

“People do it. They’re very trusting,” Murray said. “People are a little *too* trusting sometimes. People will generally give [others] way more information than they should.” Some people are lulled into a false sense of security because the medium is impersonal.

But hackers can also pore through the databases of any of the nation’s credit reporting bureaus. Companies that routinely check credit histories, such as real estate firms and car dealerships, have access to credit bureaus’ databases. If printouts of this information are not disposed of properly, thieves have all the information they need to wreak havoc on their unsuspecting victims’ credit. This method of identity theft is particularly effective because it provides

thieves with a means to assess the quality of their victims' credit.

Stolen identities offer many opportunities

Once a thief has access to a victim's personal information, the offender may do any number of things in the victim's name: open bank accounts, apply for credit cards, even start up a business. Thieves can even set up accounts under different addresses, making it that much harder for victims to discover that things are awry. Some thieves may use special software to print up bogus checks using real routing numbers. The fake checks look legitimate and provide the perpetrator the added cover of having his or her own name and address on the account.

> **"Sometimes it takes years to get credit straightened out. It can really ruin somebody in a very short period of time" —** Master Sgt. Jim Murray, Illinois State Police

Unfortunately, financial institution verification systems are often lax. Although in most cases consumers are by law responsible for only $50 of unauthorized purchases, repairing blemished credit is another matter. "It's not so much the charges as the credit history that causes problems," Murray said. "Sometimes it takes years to get credit straightened out. It can really ruin somebody in a very short period of time." Some creditors maintain that corporations are the real victims in these cases, since it is the companies that ultimately must swallow the financial losses. Of course, consumers wind up paying for it in the long run.

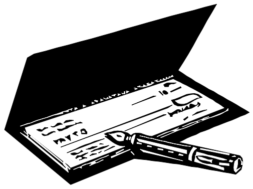
Until recently, there have been few laws specifically prohibiting identity theft. In October 1998, however, President Clinton signed a federal law that establishes identity theft as a felony and provides victims with the right to report these kinds of crimes to police and to recover damages.

State laws need to be enacted as well. For example, a bill currently pending before the General Assembly would make it a misdemeanor to use another person's name, birth date, or Social Security number unlawfully or without that person's consent.

Attempting to clear your credit after having your financial identity stolen can be an arduous affair. Victims must pay out of pocket for notarized affidavits that absolve them from responsibility for wrongfully incurred debts. Often, a victim must send a separate affidavit to each creditor. More extensive legal assistance is costly and time consuming.

Authorities lack the resources to actively investigate and prosecute cases of identity theft. Perpetrators often slip through the cracks, since identity theft is largely a paperwork crime and therefore hard to trace. Sometimes perpetrators can be tracked to a delivery address if they have ordered items through the mail using someone else's credit card. It is more difficult to track misuse of bank accounts. Murray said he knew of one case in which the victim's checks weren't used until 10 years after they were stolen.

Crimes of identity theft can be difficult to prosecute. Often thieves may defraud victims in different states or even different countries, and laws vary according to jurisdiction. "In order to have a prosecution, you have to have a victim who's willing to testify in court…people aren't going to travel unless [they've lost] a significant amount of money," Murray said.



There are some steps that consumers can take to protect themselves against identity theft:

- Keep track of bill payment schedules; familiarize yourself with the mailing dates of credit card bills.

- Tear up or shred sensitive documents before discarding them.

- When ordering via the Internet, be careful to offer information only to legitimate businesses that guarantee discreet on-line transactions.

- Check with any of the major credit bureaus — Experian, Equifax, and Trans Union are the three largest — at least once a year to verify your credit record for accuracy.■

Collaborative efforts targeting Internet crime help prevent child exploitation

By Aurora Aguilar

The unique criminal and predatory opportunities afforded by the Internet have given rise to equally unique investigative and prosecutorial initiatives by state and local agencies in Illinois.

The Illinois Attorney General's Internet Criminal Activity Unit (ICAU) and the multi-agency Internet Child Exploitation Task Force are collaborative efforts aimed at combating Internet crime in the state.

Launched in December 1997, and supported in part by a grant from the Authority, the ICAU brought a statewide prosecutorial approach to the criminal use of the Internet, primarily focusing on child sexual exploitation. The ICAU also assists and coordinates the efforts of the Internet Child Exploitation Task Force in combating two forms of child exploitation: Internet child pornographers and on-line sexual predators.

The ICAU built upon earlier efforts of several federal, state, and local departments, including the U.S. Postal Inspection Service, the U.S. Customs Service, and the Naperville Police Department. The Internet Child Exploitation Task Force brought together these and other agencies to coordinate efforts and share knowledge on computer crime.

Staffed by two assistant attorneys general and two specially trained investigators, the ICAU conducts investigations and also provides assistance to local jurisdictions as they investigate and prosecute Internet crimes. Additionally, the unit coordinates public awareness programs, drafts legislative initiatives regarding Internet crime, and provides training to prosecutors and investigators.

Computer crime institute

In conjunction with the Illinois Law Enforcement Training and Standards Board, the Attorney General's Office also operates the Illinois Computer Crime Institute, an education and training forum on computer crimes for law enforcement officers, prosecutors, and the general public.

The institute hosts a Web site that facilitates the exchange of information among officials investigating and prosecuting computer crimes in Illinois. The Web site provides information and resources to law enforcement and the general public. Members of the ICAU also serve as instructors at the Suburban Law Enforcement Academy's 40-hour training session on computer crime investigations for law enforcement officers and prosecutors.

The ICAU was developed in response to the increasing amount of Internet criminal activity, the technical nature of the offenses, and because the evidence found in these cases required specially trained investigators and prosecutors, said Keith Chval, assistant attorney general and ICAU supervisor.

Prosecuting someone for on-line child solicitation requires more sophisticated evidence gathering techniques than cases involving only child pornography, where the evidence is primarily the possession of the pornography. "From a technical standpoint, these investigations are more complex," Chval said.

The ICAU and task force investigators develop cases by posing as children on line. Pedophiles solicit the investigators by communicating in a sexually oriented chat room with someone they believe is a child. In these investigations, every proposition is made by the pedophile.

"We've charged over a dozen felony offenses in the first year, and an entrapment defense has not been raised in a single case," Chval said. The techniques taught at the Suburban Law Enforcement Academy class, and also required of members of the task force, dictate that officers be meticulous in allowing the pedophile to initiate the solicitation. "It simply isn't an issue in our cases," Chval said.

Privacy issues

Since many Internet accounts do not ask for much personal information from their clients, pedophiles retain a certain amount of anonymity until someone intervenes. Many Internet service providers implement a privacy policy that keeps personal information on their clients undisclosed. However, the Attorney General's Office can obtain much of the information that it needs on a suspected pedophile through the use of subpoenas and search warrants. Also, when an Internet service provider receives information that a subscriber is sending child pornography, the service provider is required by federal law to report the information to authorities.

"The essence of the case can usually be found in the target's computer," said Chval. Police and investigators confiscate equipment used to perform the illegal activity. The analysis of information found in computer hardware is often the final piece of evidence that closes any defenses

Aurora Aguilar is an intern with the Authority's Office of Public Information.

to a defendant and can also lead to additional charges.

"Once one of our investigators establishes a target, we'll obtain a grand jury subpoena to determine the identity of the target," Chval said. ICAU personnel will provide technical and legal assistance to investigators, participate in the execution of search and arrest warrants, and co-prosecute the case, with the pertinent state's attorney's office, through to sentencing.

Unified effort

The ability to unite and coordinate the efforts of the various federal, state, and local agencies that make up the task force is central to its success, Chval said. As of June, there were 32 agencies from throughout the state participating in the task force. Each agency devotes at least eight hours a week to the investigation of on-line predators, amounting to more than 256 hours of on-line investigation weekly. Among the agencies are six prosecutors' offices, 10 police and sheriff's departments, the U.S. Postal Inspector's Office, the United States Customs Service, and a child advocacy center.

The ICAU has identified more than 80 suspected perpetrators in Illinois and has consulted with similar units in five states about other suspects.

Investigations by task force members have led to more than a dozen arrests and five convictions. The act of crossing state lines with the intent of committing a sex crime is a federal offense, and several task force cases have resulted in federal prosecutions. "The judiciary has really recognized the seriousness of these offenses and their sentences have reflected that," Chval said.

The ICAU was instrumental in passing legislation that takes into consideration changing technology and means of communication. Last year, the Obscene Communications Act was amended as the Harassing and Obscene Communications Act to include a section that specifically addressed harassment by electronic communications rather than just by telephone. The amendment, drafted by Chval, made it possible to prosecute in cases where other methods of communication, such as the Internet were used to harass individuals.

Another wrinkle to these offenses brought on by new technologies is where a child pornographer will take an innocent picture of a child and "morph" it into a pornographic image of an adult to create a pornographic image that is part child, part adult. The old child pornography statute required a picture to be of an actual child to be prosecuted. "We couldn't prosecute in a situation where a pedophile possessed these vile pictures if we couldn't also prove that the image was of an actual child. Now we have an amended statute that proscribes these sorts of images also," Chval said.

The past legislative session saw a great deal of emphasis on updating existing statutes to reflect the changing realities brought on by the Internet and other technologies. "We were thrilled with how the legislators responded to Attorney General Ryan's initiatives. We still have work to do, but we certainly have a couple more valuable tools to use in our work to make the Internet a safer place for Illinois' children," Chval said.■

Anonymity draws many to pornography on the Internet

To date, most on-line sexual offenders charged or convicted have been middle-aged men with no prior criminal history. "Pornography may have been an interest in the past and the anonymity of the Internet allows them to act on it," said Keith Chval, an assistant Illinois Attorney General, about what he believes attracts someone to committing on-line child exploitation.

Among those who have been convicted in Illinois are two males, both 41-year-old armed forces veterans. They were recently sentenced to four years each in the Illinois Department of Corrections (IDOC) for child pornography and dissemination.

One of the perpetrators is an alumnus of the Citadel who graduated with an advanced degree. He was working as an entrepreneur of a national communications consulting business. He is married and has children.

The second perpetrator is an Air Force veteran and a divorced father of two. He was unemployed at the time of his arrest. Upon conviction, he was sentenced to four years in IDOC.

Another man was sentenced to 30 months in IDOC for possession of child pornography. He is a 42-year-old married minister with no criminal history.

And a 41-year-old divorced special education teacher was charged with aggravated criminal sexual abuse and sentenced to 42 months in IDOC. He had no previous criminal history. These are just a few of the recent prosecutions that the ICAU has been involved in.

"These aren't the guys that are creeping around in the bushes with trench coats on. They're not vagabonds. These are adult, professional, well thought of, well-educated people, and this is what they are doing," said Detective Juliet Fabbri of the Naperville Computer Crimes Unit, which is member of the Internet Child Exploitation Task Force.

Among those with a case pending is a 35-year-old married dentist with no children and no previous criminal history. He was charged with attempted aggravated criminal sexual abuse. Recently a 57-year-old municipal director of public works who was a village employee for 31 years was found guilty of child pornography possession. He is married, has adult children, and no previous criminal history. He is awaiting sentencing.

"Predators think that they can sit in their basements and no one is watching. They create a situation where they feel secure. That's a mistake," Chval said.

— Aurora Aguilar

Local Internet crime investigation unit monitors Web sites, educates community

By Aurora Aguilar

When the Naperville Police department formed its Internet Crimes Unit in 1995, Detective Mike Sullivan thought he would spend most of his time investigating computer theft and software piracy cases. "I thought we were dealing with the high-tech corridor along Highway 88," Sullivan said, referring to the concentration of technology groups in that area.

But after their first case it was evident that sexual offenses would dominate their work. In its four years of existence, the computer crimes unit has concentrated exclusively on the prevention of child exploitation.

Of the hundreds of investigations that the unit has initiated, about 30 have resulted in arrests, mostly on charges related to the possession and dissemination of child pornography, sexual assault, or sexual abuse. So far, none of the cases have gone to trial. Most have been resolved through pleas, and several cases are still pending, said Detective Juliet Fabbri, also of the Internet Crimes Unit.

The work of the investigators has brought the department's Internet Crimes Unit national attention in the media and from other law enforcement agencies. Sullivan and Fabbri have assisted agencies throughout the country with Internet crime investigations. Together, they have assisted in more than 300 computer crime cases nationwide.

Educational Web site

Today, the two detectives spend a lot of time sharing their knowledge on computer crimes with other agencies and the general public through seminars, presentations, and a Web site established in conjunction with the Microsoft Corp. (www.microsoft.com/safekids/).

The Web site education program also has attracted international attention. Officials in Chile had the presentation translated into Spanish to educate their growing population of Internet users.

"The program can be accessed from anywhere in the world, and the manuals and guides are there to educate the parent more than the child," Sullivan said.

The decision to form the Internet Crimes Unit came in 1994 after the police department was asked to assist the FBI on a major case involving a Naperville resident. The investigation resulted in the arrests of more than 60 people nationwide for trading and selling child pornography over the Internet.

Because of his technical knowledge, Sullivan was chosen to work with the federal agents in their investigation. "We went in, searched the residence, and seized the computer," Sullivan said. From the computer, the investigators extracted evidence incriminating the suspect.

Shortly after that, Naperville Police Chief David Dial decided to create a unit to investigate computer crimes in Naperville, and selected Sullivan to head it. Initially, Sullivan was the only member of the unit, but as the number of cases quickly grew, other investigators were recruited.

Four of the seven investigators who work with the Naperville Internet Crimes Unit are certified computer crimes investigators, having completed a 40-hour course at the Suburban Law Enforcement Academy at the College of DuPage.

The unit's investigations are either reactive or proactive. A reactive investigation deals with a complaint that has been made by someone, such as a parent or child, who came in contact with objectionable material. A proactive investigation is when the detectives, posing as children, go on line in an attempt to identify predators attempting to solicit and seduce children.

In a recent reactive investigation, Sullivan helped bring charges against a Joliet resident who was having a dispute with a neighbor and allegedly retaliated by posting on the Internet that the neighbor's 9-year-old daughter provided sexual services. The neighbor's home phone number and address were listed on a Web site created by the suspect. The man recently pleaded guilty to disorderly conduct and harassment by phone, and received a $750 fine and 18 months probation.

Reactive investigations also include cases where companies are hit by computer hackers or viruses.

Statewide task force

The Naperville Internet Crimes Unit is part of the multi-agency Internet Child Exploitation Task Force, which is coordinated by the Illinois Attorney General's Internet Criminal Activity Unit. The task force coordinates the efforts of local, state, and federal authorities throughout Illinois in fighting child exploitation through the Internet.

The expertise in computer crime gained by members of the strike force also has helped smaller departments with fewer resources. One such case involved a 14-year-old Batavia girl and a Texas man she met on line. The man came to Illinois to meet the girl and then assaulted her at a motel in Rochelle in Ogle County. When the case came to the attention of local authorities, the Ogle County Sheriff's Department contacted the Illinois Attorney General's Office for assistance. The Naperville Internet Crimes Unit was asked to assist with the investigation.

"Rochelle realized they were in way over their heads with this case Internet-wise, and they (Ogle County) knew there was someone else they could contact," said Fabbri. The man who pursued the girl using the Internet was convicted of sexual assault and sentenced to three years in the Illinois Department of Corrections.

Focus on education

Fabbri and Sullivan have traveled to schools, colleges, and businesses in Ohio, Indiana, Minnesota, Missouri, Georgia, and throughout Illinois as part of the public education approach of the unit.

When talking about child victims through the Internet, Sullivan uses an analogy of a predator finding an unsupervised child in a park. In the past, a predator might find a child at a public place and use toys or candy to entice them, he said. Now they can simply use the title of a chat room to discover the child's interest and pull them into an on-line conversation. Predators also can create their own chat rooms that children can visit through the Internet. Many Web sites and chat rooms are used strictly for sexual purposes, and thousands of chat rooms are unmonitored and uncensored.

Recognizing the vulnerability of children using the Internet, Sullivan contacted Microsoft in 1997 with the idea of creating a Web site where children and parents could access information that would protect them from on-line predators. Working with Microsoft and the Illinois Attorney General's Office, the Naperville Police Department created an interactive educational program on the Microsoft Web site.

Often, the computer crimes unit has discovered that parents are technologically ignorant when it comes to the Internet, and are oblivious to its dangers. Parents also are usually not aware of inexpensive and simple computer software programs that can safeguard a child's computer.

Among these programs are the Cyber Sentinel and Net Nanny. These are child predator protection libraries and most can be purchased for a one-time fee. These precautionary programs block phrases, words, and personal information from being accessed and document every screen. The programs also can prohibit credit card purchases, as well as log the location and description of anyone who sends an e-mail message.

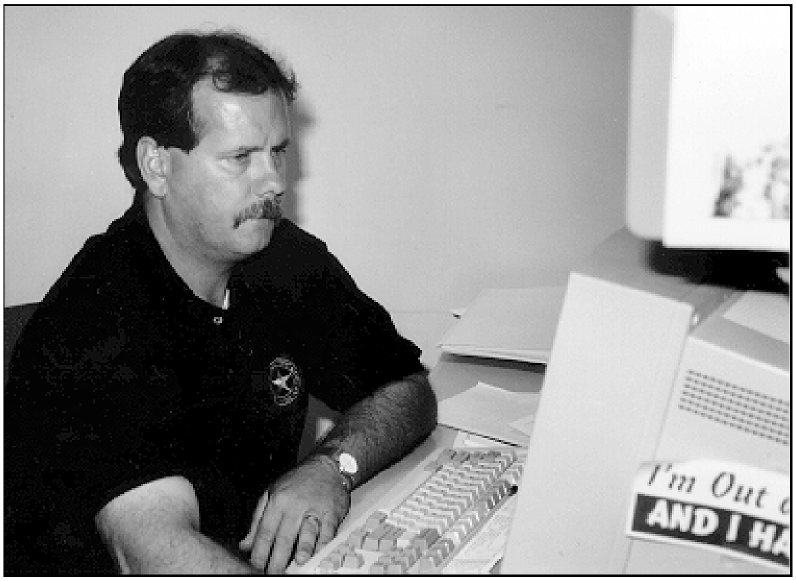
Fabbri

Because many children are more technically advanced than their parents, some of these programs are "childproof," to the extent that they cannot be manipulated without being detected. Parents are notified by e-mail if alterations are made to the program.

Fabbri said she was astonished by how knowledgeable children are about technology at such an early age. On-line safety presentations were first centered on fifth and sixth graders. They found, however, that children at that level already were aware of child exploitation over the Internet, and many previously had been approached. Now, the presentations are given to fourth graders, Fabbri said.

Affluent communities like Naperville often are the most susceptible to computer crime because of the preponderance of computers in the homes. Naperville is an upper-middle class city where many children have unsupervised on-line access, said Sullivan. This fact keeps the Internet Crimes Unit busy, he said.

Sullivan said he expects the focus of computer crime to be shifted to on-line theft in the next few years. Electronic commerce through the Internet, he said, will facilitate theft. "Thieves can steal more with a pen than with a gun, but even more with a computer," Sullivan said.



Photos by Aurora Aguilar

Detective Mike Sullivan of the Naperville Police Department Internet Crime Unit operates in chat rooms looking for sexual predators.

Patrolling the information superhighway

By Sal Perri

Like so many other endeavors on the Internet, criminal activity is flourishing. Though originally conceived to serve educational, research, and communications purposes, the Internet has now become an avenue for criminals to scam, abuse, harass, and exploit people. There is no question that the Internet presents a vast opportunity for criminals who want to exploit it.

Internet expansion

A recent study by Nielsen Media Research estimated that 70.5 million Americans, or about a third of the nation's population, are on line. Nearly half of those between ages of 16 and 34 are using the Internet. Mediamark Research, Inc. has reported that 37 percent of the U.S. population 18 and over has access to the Internet. In local figures, Yahoo! Internet Life magazine cited a study that showed about 18 percent of Chicago's population is using the Internet. All of these users are potential victims of Internet scam artists.

Cyber scams

According to Internet Fraud Watch, some of the most common on-line scams, many of which were popular before the Internet, but have now found a new medium, include:

- Web auctions that misrepresent products that are sold: Inflated competing bids act as an incentive because it drives up bids by 50 percent or more. Some auction firms, such as Ebay.com, use a customer rating system to warn of past unfavorable activity.
- Fraudulent merchandise sales: Goods are never delivered or are not as advertised.
- Misleading Internet service sales: A person may be charged for services advertised as free, or the service advertised is something other than delivered.
- Pyramids and multi-level marketing schemes: Schemers make money by recruiting others to sell products or services and then charge their recruits training or work fees.
- Business opportunities that seem too good to be true: They promise big profits with little or no work. Usually, these schemes involve "investing" in a business package.
- Shady work-at-home plans: Victims pay fees to receive material to work at home but are never sent business.
- Duplicitous advance-fee loans: Loans are secured by a fee, but the money is never disbursed.
- False credit repair: Companies promise to clean up your credit reports, but don't.
- Deceptive credit cards: Companies commit to giving credit lines to people with bad or no credit if they pay an initial fee, but the victims never receive the credit cards.

Crimes against children

Because computers are popular educational tools for children across the country, many parents and law enforcement officials are concerned that children will become the most vulnerable targets of cyber crime. The Internet presents an unmonitored medium of unlimited potential for children to access objectionable material.

Impact of computer crime

Federal law enforcement officials have warned that the impact of computer crime goes well beyond the potential loss to an individual victim. While individual accounts of losses are staggering, computer crime affects the national economy and security.

- North America represents 27 percent of worldwide losses to software piracy, or \$3.1 billion. The U.S. accounted for \$2.7 billion of the North American losses, up from \$2.3 billion in 1996. Overall, revenue losses to the worldwide software industry due to piracy were estimated at \$11.4 billion.[1]
- 208,000 laptop computers were stolen in 1995, up 39 percent from the year before. As many as one in every 14 laptop computers sold in the United States was stolen last year.[2]
- For the third straight year, financial losses due to computer security breaches amounted to more than \$100 million. The most serious financial losses occurred through theft of proprietary information for a total of \$42.5 million and financial fraud for a total of \$39.7 million. [3]

Sal Perri is a research analyst with the Authority's Research and Analysis Unit.

- The actual losses to victimized individuals and institutions of financial crimes involving identity fraud totaled $442 million in 1995, $450 million in 1996, and $745 million in 1997. Moreover, officials from various federal law enforcement agencies said that identity fraud can be an element of various financial crimes and that Internet growth increases opportunities for criminal activity. [4]

- The direct cost of high-theft crime is $250 million which includes the theft of computers, peripherals, and cell phones each year from their manufacturers, mainly while the goods are being shipped. Indirect costs (such as lost sales and expensive theft-reduction strategies) and industry losses could push total losses past $5 billion. [5]

Policing efforts

Cyber crime is receiving much attention from law enforcement agencies and prosecutors. A number of entities have teamed up to combat these crimes.

Illinois Attorney General Jim Ryan established the statewide Internet Criminal Activity Unit (ICAU), which also coordinates the efforts of the statewide Internet Child Exploitation Task Force. The multi-jurisdictional effort includes representatives from the Illinois State Police (ISP); Naperville, Des Plaines, and Arlington Heights police departments; DuPage County Sheriff's Police; DuPage, Will, and Cook County state's attorneys' offices; and the United States Postal Inspection Service. The task force also has consulted with several local state's attorneys' offices (Cook, DuPage, Gallatin, Grundy, Kane, Kankakee, Lake, Livingston, McHenry, and Will counties) in litigation strategy and the drafting and execution of computer search warrants.

Task force members monitor the Internet for child sexual exploitation and targets offenders who use computers to find their victims and distribute child pornography. The task force and ICAU also investigate and prosecute other criminal matters involving the Internet, such as harassment, indecent solicitation of adults, computer tampering, and theft.

Other law enforcement agencies are fighting the battle against Internet crime as well. The Illinois State Police established an Internet task force for proactive and reactive case investigation and prosecution. Six investigators are assigned to the task force. Two-member teams have been established in northern, central and southern Illinois. Each unit has an investigator for on-line crimes and a computer evidence recovery specialist. The Division of Internal Investigations' computer recovery unit hired new employees to provide training that includes technical assistance and guidance to the task force. A legal advisor from the ISP provides consultation and training in technology law. In addition, the task force developed a cooperative investigative agreement with the attorney general, the FBI "Innocent Image" program, and other federal agencies and local prosecutors.

The Illinois Attorney General's Office and the Illinois Law Enforcement Training and Standards Board developed the Illinois Computer Crime Institute (ICCI), which is guided by a multi-agency advisory board. ICCI was created to provide computer crime training to investigators and also to develop a Web site to facilitate communication between the investigating agencies.

The National Center for Missing and Exploited Children (NCMEC) also strives to prevent Internet crime. NCMEC helps locate and recover missing children and raises public awareness on preventing child abduction, molestation, and sexual exploitation. NCMEC, a private, nonprofit organization established in 1984, operates under a congressional mandate and works in conjunction with the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention. As the nation's resource center for child protection, the NCMEC provides police officers with case assistance.

The U.S. Department of Justice has developed the National Cybercrime Training Partnership (NCTP) to work with state, local, federal, and international law enforcement agencies. The NCTP coordinates a wide spectrum of resources. NCTP will work with all levels of law enforcement to develop and promote a long-range strategy for high-tech police work in the 21st century, including interagency and interjurisdictional cooperation, and information networking and technical training.

The Federal Trade Commission's Project Safebid Steering Committee conducts investigations of fraudulent Internet auction activity. The FTC is especially interested in forging ties with local criminal law enforcement agencies to stop scam artists. The commission provides much of the evidence necessary to bring criminal cases against Internet auction con artists.

Notes:

1. BSA/SPA 1997 Global Piracy Report, May 1998 - A Study conducted by International Planning and Research Corporation for the Business Software Alliance and Software Publishers (http://www.spa.org or http://www.bsa.org).

2. Wanted: Your Laptop, by Michael Meyer, Newsweek: U.S. Edition July 15, 1996, Page 42.

3. Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey, by The Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation (FBI) Computer Intrusion Squad, March 5, 1999.

4. Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited, Government Accounting Office (GAO): Briefing Report to Congressional Requesters, May 1998 (GAO/GGD-98-100BR).

5. The Economic Costs and Implications of High-Technology Hardware Theft, By: J.N. Dertouzos, E.V. Larson, P.A. Ebener , A Rand Corporation Report 1999 (MR-1070-AEA) (http://www.rand.org/publications/MR/MR1070/).■

A parent's guide to internet safety

(Reprinted with permission from the FBI Web site: **www.fbi.gov**. This information also is available as a pamphlet from FBI field offices. This guide was prepared in conjunction with the National Center for Missing and Exploited Children: **www.missingkids.com** 1-800-843-5678.)

Dear Parent: Our children are our Nation's most valuable asset. They represent the bright future of our country and hold our hopes for a better nation. Our children are also the most vulnerable members of society. Protecting our children against the fear of crime and from becoming victims of crime must be a national priority. Unfortunately the same advances in computer and telecommunication technology that allow our children to reach out to new sources of knowledge and cultural experiences are also leaving them vulnerable to exploitation and harm by computer-sex offenders. I hope that this pamphlet helps you to begin to understand the complexities of on-line child exploitation. For further information, please contact your local FBI office or the National Center for Missing and Exploited Children at 1-800-843-5678.
Louis J. Freeh, Director
Federal Bureau of Investigation

While on-line computer exploration opens a world of possibilities for children, expanding their horizons and exposing them to different cultures and ways of life, they can be exposed to dangers as they hit the road exploring the information highway. There are individuals who attempt to sexually exploit children through the use of on-line services and the Internet. Some of these individuals gradually seduce their targets through the use of attention, affection, kindness, and even gifts. These individuals are often willing to devote considerable amounts of time, money, and energy in this process. They listen to and empathize with the problems of children. They will be aware of the latest music, hobbies, and interests of children. These individuals attempt to gradually lower children's inhibitions by slowly introducing sexual context and content into their conversations.

There are other individuals, however, who immediately engage in sexually explicit conversation with children. Some offenders primarily collect and trade child-pornographic images, while others seek face-to-face meetings with children via on-line contacts. It is important for parents to understand that children can be indirectly victimized through conversation, i.e. "chat," as well as the transfer of sexually explicit information and material. Computer-sex offenders may also be evaluating children they come in contact with on-line for future face-to-face contact and direct victimization. Parents and children should remember that a computer-sex offender can be any age or sex. The person does not have to fit the caricature of a dirty, unkempt, older man wearing a raincoat to be someone who could harm a child.

Children, especially adolescents, are sometimes interested in and curious about sexuality and sexually explicit material. They may be moving away from the total control of parents and seeking to establish new relationships outside their family. Because they may be curious, children/adolescents sometimes use their on-line access to actively seek out such materials and individuals. Sex offenders targeting children will use and exploit these characteristics and needs. Some adolescent children may also be attracted to and lured by on-line offenders closer to their age who, although not technically child molesters, may be dangerous. Nevertheless, they have been seduced and manipulated by a clever offender and do not fully understand or recognize the potential danger of these contacts.

This guide was prepared from actual investigations involving child victims, as well as investigations where law enforcement officers posed as children. Further information on protecting your child on line may be found in the National Center for Missing and Exploited Children's *Child Safety on the Information Highway* and *Teen Safety on the Information Highway* pamphlets.

What are signs that your child might be at risk on line?

Your child spends large amounts of time on line, especially at night.

Most children that fall victim to computer-sex offenders spend large amounts of time on line, particularly in chat rooms. They may go on line after dinner and on the weekends. They may be latchkey kids whose parents have told them to stay at home after school. They go on line to chat with friends, make new friends, pass time, and sometimes look for sexually explicit information. While much of the knowledge and experience gained may be valuable, parents should consider monitoring the amount of time spent on line.

Children on line are at the greatest risk during the evening hours. While offenders are on line around the clock, most work during the day and spend their evenings on line trying to locate and lure children or seeking pornography.

You find pornography on your child's computer.

Pornography is often used in the sexual victimization of children. Sex offenders often supply their potential victims with pornography as a means of opening sexual discussions and for seduction. Child pornography may be used to show the child victim that sex between children and adults is "normal." Parents should be conscious of the fact that a child may hide the pornographic files on diskettes from them. This may be especially true if the computer is used by other family members.

Your child receives phone calls from men you don't know or is making calls, sometimes long distance, to numbers you don't recognize.

While talking to a child victim on line is a thrill for a computer-sex offender, it can be very cumbersome. Most want to talk to the children on the telephone. They often engage in "phone sex" with the children and often seek to set up an actual meeting for real sex. While a child may be hesitant to give out his/her home phone number, the computer-sex offenders will give out theirs. With Caller ID, they can readily find out the child's phone number. Some computer-sex offenders have even obtained toll-free 800 numbers, so that their potential victims can call them without their parents finding out. Others will tell the child to call collect. Both of these methods result in the computer-sex offender being able to find out the child's phone number.

Your child receives mail, gifts, or packages from someone you don't know.

As part of the seduction process, it is common for offenders to send letters, photographs, and all manner of gifts to their potential victims. Computer-sex offenders have even sent plane tickets in order for the child to travel across the country to meet them.

Your child turns the computer monitor off or quickly changes the screen on the monitor when you come into the room.

A child looking at pornographic images or having sexually explicit conversations does not want you to see it on the screen.

Your child becomes withdrawn from the family.

Computer-sex offenders will work very hard at driving a wedge between children and their families, or at exploiting their relationship. They will accentuate any minor problems at home that a child might have. Children may also become withdrawn after sexual victimization.

Your child is using an on-line account belonging to someone else.

Even if you don't subscribe to an on-line service or Internet service, your child may meet an offender while on line at a friend's house or the library. Most computers come preloaded with on-line and/or Internet software. Computer-sex offenders will sometimes provide potential victims with a computer account for communications with them.

What should you do if you suspect your child is communicating with a sexual predator on line?

1. Consider talking openly with your child about your suspicions. Tell them about the dangers of computer-sex offenders.

2. Review what is on your child's computer. If you don't know how, ask a friend, coworker, relative, or other knowledgeable person. Pornography or any kind of sexual communication can be a warning sign.

3. Use the Caller ID service to determine who is calling your child. Most telephone companies that offer Caller ID also offer a service that allows you to block your number from appearing on someone else's Caller ID. Telephone companies also offer an additional service feature that rejects incoming calls that you block. This rejection feature prevents computer-sex offenders or anyone else from calling your home anonymously.

4. Devices can be purchased that show telephone numbers that have been dialed from your home phone. Additionally, the last number called from your home phone can be retrieved provided that the telephone is equipped with a redial feature. You will also need a telephone pager to complete this retrieval.

5. This is done using a numeric-display pager and another phone that is on the same line as the first phone with the redial feature. Using the two phones and the pager, a call is placed from the second phone to the pager. When the paging terminal beeps for you to enter a telephone number, you press the redial button on the first (or suspect) phone. The last number called from that phone will then be displayed on the pager.

6. Monitor your child's access to all types of live electronic communications (i.e., chat rooms, instant messages,

Internet Relay Chat, etc.), and monitor your child's e-mail. Computer-sex offenders almost always meet potential victims via chat rooms. After meeting a child online, they will continue to communicate electronically often via e-mail.

7. Should any of the following situations arise in your household, via the Internet or on-line service, you should immediately contact your local or state law enforcement agency, the FBI, and the National Center for Missing and Exploited Children:

- Your child or anyone in the household has received child pornography;

- Your child has been sexually solicited by someone who knows that your child is under 18 years of age;

- Your child has received sexually explicit images from someone that knows your child is under the age of 18.

If one of these scenarios occurs, keep the computer turned off in order to preserve any evidence for future law enforcement use. Unless directed to do so by the law enforcement agency, you should not attempt to copy any of the images and/or text found on the computer.

What can you do to minimize the chances of an on-line exploiter victimizing your child?

1. Communicate, and talk to your child about sexual victimization and potential on-line danger.

2. Spend time with your children online. Have them teach you about their favorite on-line destinations.

3. Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for a computer-sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.

4. Utilize parental controls provided by your service provider and/or blocking software. While electronic chat can be a great place for children to make new friends and discuss various topics of interest, it is also prowled by computer-sex offenders. Use of chat rooms, in particular, should be heavily monitored. While parents should utilize these mechanisms, they should not totally rely on them.

5. Always maintain access to your child's on-line account and randomly check his/her e-mail. Be aware that your child could be contacted through the U.S. Mail. Be up front with your child about your access and reasons why.

6. Teach your child the responsible use of the resources on line. There is much more to the on-line experience than chat rooms.

7. Find out what computer safeguards are utilized by your child's school, the public library, and at the homes of your child's friends. These are all places, outside your normal supervision, where your child could encounter an on-line predator.

8. Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions.

9. Instruct your children:

- to never arrange a face-to-face meeting with someone they met on line;

- to never upload (post) pictures of themselves onto the Internet or on-line service to people they do not personally know;

- to never give out identifying information such as their name, home address, school name, or telephone number;

- to never download pictures from an unknown source, as there is a good chance there could be sexually explicit images;

- to never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing;

- that whatever they are told on line may or may not be true.

Frequently asked questions:

My child has received an e-mail advertising for a pornographic Web site, what should I do?

Generally, advertising for an adult, pornographic website that is sent to an e-mail address does not violate federal law or the current laws of most states. In some states it may be a violation of law if the sender knows the recipient is under the age of 18. Such advertising can be reported to your service provider and, if known, the service provider of the originator. It can also be reported to your state and federal legislators, so they can be made aware of the extent of the problem.

Is any service safer than the others?

Sex offenders have contacted children via most of the major on-line services and the Internet. The most important factors in keeping your child safe on line are the utilization of appropriate blocking software and/or parental controls, along with open, honest discussions with your child, monitoring his/her on-line activity, and following the tips in this pamphlet.

Should I just forbid my child from going on line?

There are dangers in every part of our society. By educating your children to these dangers and taking appropriate steps to protect them, they can benefit from the wealth of information now available on line.

Helpful definitions:

Internet - An immense, global network that connects computers via telephone lines and/or fiber networks to storehouses of electronic information. With only a computer, a modem, a telephone line and a service provider, people from all over the world can communicate and share information with little more than a few keystrokes.

Bulletin Board Systems (BBSs) - Electronic networks of computers that are connected by a central computer setup and operated by a system administrator or operator and are distinguishable from the Internet by their "dial-up" accessibility. BBS users link their individual computers to the central BBS computer by a modem which allows them to post messages, read messages left by others, trade information, or hold direct conversations. Access to a BBS can, and often is, privileged and limited to those users who have access privileges granted by the systems operator.

Commercial On-line Service (COS) - Examples of COSs are America Online, Prodigy, CompuServe and Microsoft Network, which provide access to their service for a fee. COSs generally offer limited access to the Internet as part of their total service package.

Internet Service Provider (ISP) - Examples of ISPs are Erols, Concentric and Netcom. These services offer direct, full access to the Internet at a flat, monthly rate and often provide electronic mail service for their customers. ISPs often provide space on their servers for their customers to maintain World Wide Web sites. Not all ISPs are commercial enterprises. Educational, governmental, and nonprofit organizations also provide Internet access to their members.

Public Chat Rooms - Created, maintained, listed, and monitored by the COS and other public domain systems such as Internet Relay Chat. A number of customers can be in the public chat rooms at any given time, which are monitored for illegal activity and even appropriate language by systems operators (SYSOP). Some public chat rooms are monitored more frequently than others, depending on the COS and the type of chat room. Violators can be reported to the administrators of the system which can revoke user privileges. The public chat rooms usually cover a broad range of topics such as entertainment, sports, game rooms, children only, etc.

Electronic Mail (E-mail) - A function of BBSs, COSs and ISPs which provides for the transmission of messages and files between computers over a communications network similar to mailing a letter via the postal service. E-mail is stored on a server, where it will remain until the addressee retrieves it. Anonymity can be maintained by the sender by predetermining what the receiver will see as the "from" address. Another way to conceal one's identity is to use an "anonymous remailer," which is a service that allows the user to send an e-mail message repackaged under the remailer's own header, stripping off the originator's name completely.

Chat - Real-time text conversation between users in a chat room with no expectation of privacy. All chat conversation is accessible by all individuals in the chat room while the conversation is taking place.

Instant Messages - Private, real-time text conversation between two users in a chat room.

Internet Relay Chat (IRC) - Real-time text conversation similar to public and/or private chat rooms on COS.

Usenet (Newsgroups) - Like a giant, cork bulletin board where users post messages and information. Each posting is like an open letter and is capable of having attachments, such as graphic image files (GIFs). Anyone accessing the newsgroup can read the postings, take copies of posted items, or post responses. Each newsgroup can hold thousands of postings. Currently, there are over 29,000 public newsgroups and that number is growing daily. Newsgroups are both public and private. There is no listing of private newsgroups. A user of private newsgroups has to be invited into the newsgroup and be provided with the newsgroup's address.

For more information:

Federal Bureau of Investigation
Office of Crimes Against Children
935 Pennsylvania Avenue, NW
Room 4127
Washington, D.C. 20535
http://www.fbi.gov
(202) 324-3666

National Center for Missing and Exploited Children
http://www.missingkids.com/
1-800-843-5678. ■

LEADS upgrade, digital wireless network will soon be serving agencies in Illinois

Two major projects in information systems technology are under way in Illinois that will help criminal justice agencies meet the communications challenges of the 21st Century.

The initial phases of a major upgrade to the Law Enforcement Agency Data System (LEADS) have been completed, and testing for the first phase of the Illinois Wireless Information Network (IWIN) is under way.

The process of upgrading LEADS, the statewide system for tracking arrest warrants and providing other information and services to criminal justice agencies in Illinois, has already made the current LEADS network and applications year 2000 compliant.

NCIC 2000 link

The next stages of the upgrade will establish a link with the FBI's NCIC 2000, the national system for sharing criminal justice information that has recently been upgraded, and bring up to date the technological platform upon which the 30-year-old LEADS system was based.

Among the advancements with NCIC 2000 will be an improved name search capability. The new system will have broader parameters for matching names and birth dates, which will result in more "hits" for inquiries made by LEADS users.

Another feature of NCIC 2000 will be duplicate vehicle notification. Under the current NCIC system if multiple agencies list a vehicle as stolen and the vehicle is recovered, only one of the entries is canceled, resulting in a record "left hanging." Under the new system, NCIC 2000 will automatically notify all agencies that have entered the same vehicle whenever a change is made to the records.

As part of the LEADS upgrade, the new Illinois Criminal History Record Information (CHRI) application became operational in early June. The new application is fully year 2000 compliant.

Upgraded fingerprint system

Also, the Illinois State Police (ISP) is moving this summer to the new Automated Fingerprint Identification System, AFIS-21. Under this upgraded system, fingerprints submitted electronically using livescan or cardscan technology will be processed, on the average, in approximately two hours.

The FBI's new Integrated AFIS, known as I-AFIS, will also become operational this summer, and Illinois' system will be connected to I-AFIS. At that point, agencies in Illinois will no longer be required to complete the FBI fingerprint card; only the state fingerprint card will be required.

When operational, the Illinois AFIS-21 will forward the fingerprint images and demographic data electronically to the FBI I-AFIS. A response will be returned to Illinois within two hours. Agencies in Illinois using livescan or cardscan technology to submit electronic fingerprints to ISP can expect to receive both a state and federal response within two to four hours in most cases.

Among the other developments that will be part of the LEADS upgrade is a juvenile justice tracking database. This application was not included in the original design but was added after legislation mandating its creation was passed by the General Assembly last year. The application will be available for use around Jan. 1, 2000.

A digital wireless network

IWIN is statewide wireless data network that will be available to state and local agencies.

IWIN uses cellular digital packet data technology (CDPD) to provide real-time, bi-directional mobile connectivity to its users. The system is being developed and implemented through a partnership of the State of Illinois, Ameritech, and Software Corporation of America (SCA).

IWIN is being introduced in four phases based on geographical region. Phase I includes Cook and the collar counties, as well as numerous Downstate counties. Phase I is expected to be operational this fall and Phase IV should be completed by the end of 2000.

IWIN does not replace the Authority's ALERTS mobile data terminal system, which is used by more than 300 agencies in the state. ISP and the Authority are continuing to work together in deploying wireless mobile data technology. IWIN will provide local and state governments with optional wireless data solutions in areas where both networks have coverage. ALERTS users will continue to have the opportunity to access LEADS via the ALERTS network.■

Information in this article was abstracted from materials prepared by the Illinois State Police.

Gov. signs law extending Council's term

By Robert P. Boehmer

On July 9, Gov. George H. Ryan signed into law Public Act 91-85, which extends the expiration date of the Illinois Motor Vehicle Theft Prevention Act from Jan. 1, 2000 to Jan. 1, 2004. The Illinois Motor Vehicle Theft Prevention Council is now gathering information to develop a four-year Statewide Motor Vehicle Theft Prevention Strategy.

Extension of the sunset clause

The Illinois Motor Vehicle Theft Prevention Act was established in 1991. The Act requires insurance companies to pay into a special trust fund an amount equal to $1 for each private passenger automobile insured for physical damage coverage. This amount, collected and administered by the Council, totals about $5.4 million each year. Funds are primarily designated for law enforcement programs that increase the investigation and prosecution of vehicle theft-related crimes. The Act also created the Illinois Motor Vehicle Theft Prevention Council, an 11-member coalition comprised of law enforcement and insurance industry officials to oversee the program. The Act originally was scheduled to expire in 1996, and the expiration date was extended to Jan. 1, 2000. With Public Act 91-85, the Council will continue to operate through 2003.

Adoption of strategy

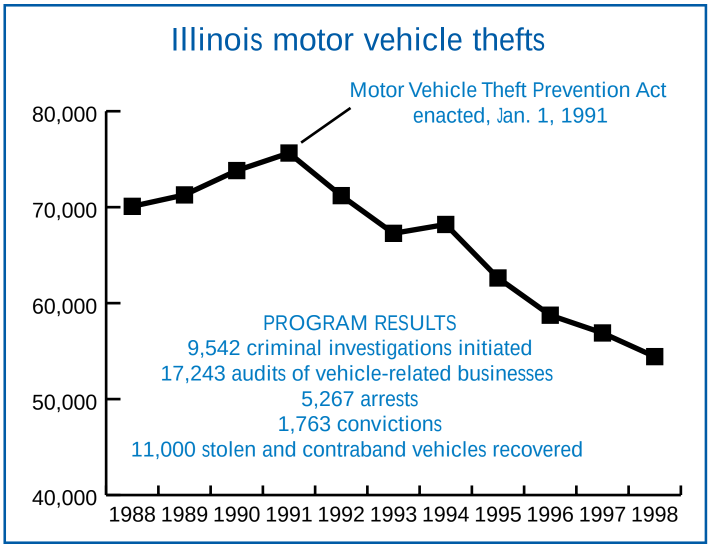
In the past, the Council has annually developed and adopted *The Statewide Motor Vehicle Theft Prevention Strategy*. The strategy included an overview of motor vehicle theft in Illinois; discussion of the nature and extent of the problem, and current efforts to address the problem; resource needs; areas of greatest need within the state; and a description of a strategy for addressing motor vehicle theft, including the identification of eligible program areas.

Consistent with the statewide strategy, the Council then solicited and negotiated program proposals from eligible recipients, and ultimately decided which programs to fund. The strategy, then, is the foundation upon which the Council's support of efforts to combat motor vehicle theft is built.

The Council's strategy has been successful. Between 1991 and 1998, vehicle theft declined by 28 percent. More than 21,000 fewer vehicles were stolen during 1998 than in 1991.

In light of the enactment of Public Act 91-85, the Council has begun the process of adopting a new strategy. This year, the Council decided to adopt a four-year, rather than an annual strategy, to allow for long-range planning by the Council and its grantees. This is particularly important since funding for the Council is not expected to increase significantly, while personnel costs are rising.

Robert P. Boehmer is general counsel of the Authority and secretary to the Motor Vehicle Theft Prevention Council.



The strategy will set the framework for the funding of grant programs until 2003. In order to adopt the strategy this summer, the Council:

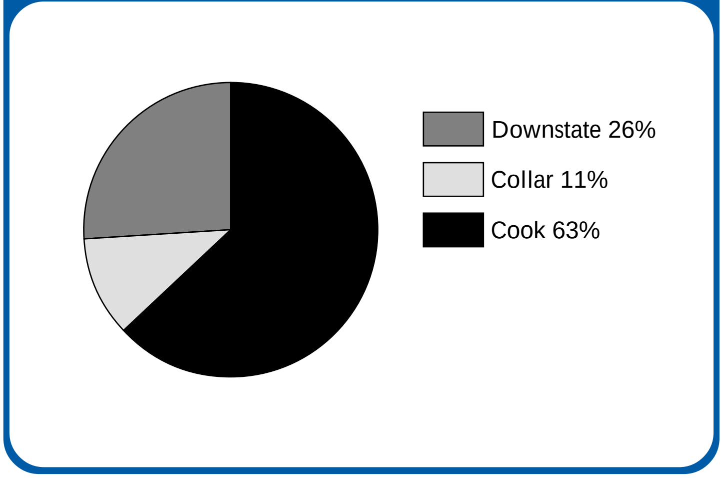
(1) has solicited written input first to help identify issues, problem areas, and effective strategies regarding motor vehicle theft in Illinois; and

(2) will host public hearings, organized around specific aspects of the strategy, and based upon the written input received. The hearings will involve brief panel presentations and discussions organized to provide input on the Council's strategy. A one-hour period at the end of each hearing will be reserved for comments from interested witnesses. Panels might cover such topics as: the nature and extent of motor vehicle theft in Illinois; law enforcement strategies; vehicle-related business involvement; insurance fraud strategies; and community-based approaches.

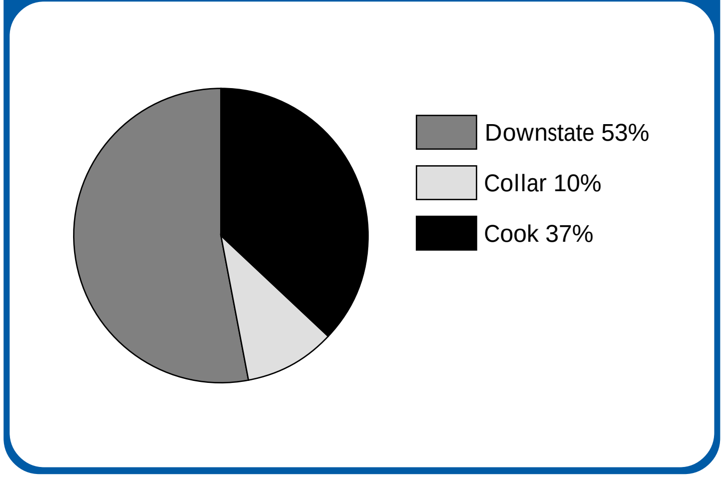
This approach should help the Council ensure that a broad range of issues and topics are dealt with and that all facets of the statewide strategy are considered. The new strategy will be designed to continue the Council's successes in contributing to the decline in auto thefts, saving consumers and the insurance industry millions of dollars.■

Trends

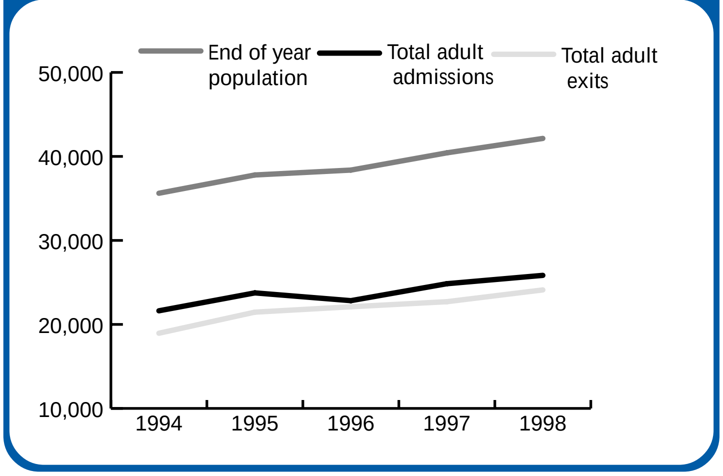
Illinois Department of Corrections
1998 adult admissions



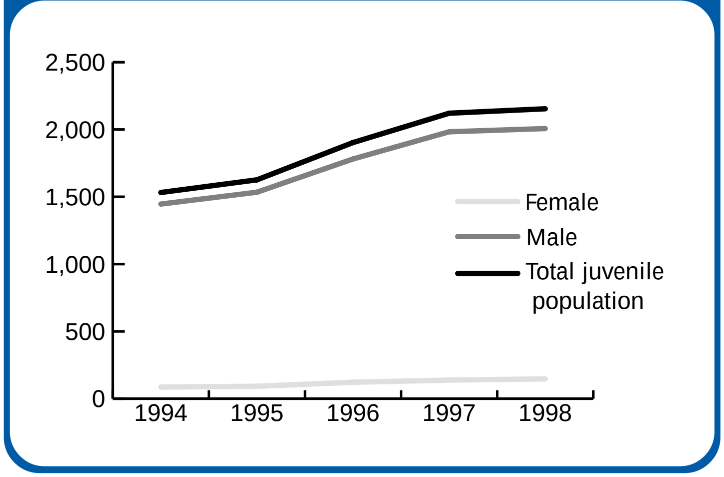
Illinois Department of Corrections
1998 juvenile admissions



Illinois Department of Corrections
1998 adult population



Illinois Department of Corrections
1998 juvenile population



Source: Illinois Department of Corrections

ILLINOIS
Criminal Justice Information Authority

120 S. Riverside Plaza, Suite 1016
Chicago, Illinois 60606
312-793-8550, TDD: 312-793-4170, Fax: 312-793-8422
www.icjia.state.il.us

For address corrections, additions, or deletions, write the information below and return this portion of the page to the Authority’s Office of Public Information. Please include your telephone number. Thank you.

____

____

____