

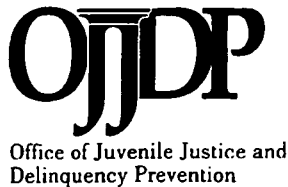
185232

Protecting Children Online Unit Commander/Policy Training

UNITED STATES DEPARTMENT OF JUSTICE
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC)

Performed Under Contract
Fox Valley Technical College
Criminal Justice Department
Appleton, Wisconsin

1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960



**OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION,
NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN,
AND
FOX VALLEY TECHNICAL COLLEGE**

PRESENT:

**PROTECTING CHILDREN ONLINE
UNIT COMMANDER/POLICY TRAINING

August 30-September 1, 1998**

Time	Event
------	-------

Sunday, August 30

8:00 a.m. - 8:30 a.m. **Welcome & Overview of Course
Student Introductions**

8:30 a.m. - 10:30 a.m. **Computer Crimes Against Children**
Lieutenant Bill Walsh

This module of instruction will provide students with information regarding the nature of the growing problem of computer crimes against children. The presentation will provide an overview of how sex offenders use personal computers and the Internet to assist them in their sexual abuse and exploitation of children. Case examples will be used to illustrate how computers are used to store, manufacture, and distribute child pornography; and to solicit children for sexual contact. Participants will be provided with information regarding the dynamics of the sexual abuse of children, as they relate to the victim-offender relationship, the level of force involved, the degree of sexual activity, the impact on the victim, and the impact on society. This will be followed by a discussion on how the use of computer technology by sexual offenders has impacted these areas.

10:30 a.m. - 10:40 a.m. **Break**



Time	Event
------	-------

Sunday, August 30 (continued)

10:40 a.m. - 12:00 noon

Introduction to Computer Technology
Robert Kreisa

This module will provide unit commanders with an understanding of how computer technology has changed how some crimes are committed and investigated. A goal of this course is to teach unit commanders the basics of computer technology so they can be conversant with investigators regarding investigations and evidence. Computer equipment commonly used to create and distribute child pornography will be available for inspection.

12:00 noon - 12:45 p.m.

Lunch Break

12:45 p.m. - 2:30 p.m.

Overview of Online Communications
Robert Kreisa

This module will familiarize unit commanders with the concept of computer networks and online communications. The Internet and how it works will be described, with particular attention to how the Internet is used to exploit children.

2:30 p.m. - 2:40 p.m.

Break

2:40 p.m. - 4:30 p.m.

Unit Commander Responsibilities
Commander Bradley Russ

This module will provide organizational and management concepts for the creation and oversight of programs designed to protect children online. Case management principals are examined and students receive information regarding their responsibilities in managing specialized units and programs. Interagency collaboration and the supervision of multi-jurisdictional cases as well as collaboration with state, local, and federal agencies is discussed. Written material, computer programs and informational videotapes are reviewed as part of the unit commander's responsibilities to educate the community and develop partnerships with neighborhood, business, and civic organizations.

Monday, August 31

8:00 a.m. - 12:00 noon

Coordinating and Conducting the Investigation
Sergeant James Doyle

This module will provide an overview of investigative techniques, methods, and actual case scenarios that will assist a unit commander in managing a complex, technical child exploitation investigation. This type of investigation is fairly new in law enforcement training regimes and require a thorough understanding of the legal and technical pitfalls that can derail a successful criminal investigation.



Time	Event
------	-------

Monday, August 31 (continued)

12:00 noon -12:45 p.m. **Lunch Break**

12:45 p.m. - 4:30 p.m. **Legal Issues**
Daniel Armagh

This module is designed to provide students with a comprehensive overview of privacy issues, search and seizure issues, and legal exposure attendant with the investigation and prosecution of computer assisted sexual exploitation of children. Students will be instructed on the most recent court rulings in relevant cases and what the legal analysis means for the investigation protocol for law enforcement. Classic and evolving defenses will be examined and instruction on how to rebut these defenses in and out of court will be discussed. Jurisdiction and partnering will be addressed to empower local and state law enforcement to successfully investigate and prosecute computer exploitation cases.

Tuesday, September 1

8:00 a.m. -11:30 a.m. **Resources**

This module will identify and explain the many resources that can be utilized in the successful investigation of computer crimes against children, including the National Center for Missing and Exploited Children's Exploitation Child Unit, the FBI, U.S. Postal, and U.S. Customs.

Tour of the National Center for Missing and Exploited Children

11:30 a.m. - **Evaluations and Closing**



Acknowledgments

The *Protecting Children Online-Unit Commander/Policy* training program was jointly developed by the United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention, the National Center for Missing and Exploited Children and Fox Valley Technical College, Appleton, Wisconsin.

Contributors

Daniel Armagh
Director
American Prosecutors Research
Institute's National Center for
Prosecution of Child Abuse
99 Canal Center Drive, Suite 510
Alexandria, VA 22314
703-519-1681
daniel.armagh@ndaa-apri.org

Peter Banks
Director of Training and Outreach
National Center for Missing and
Exploited Children
2101 Wilson Blvd., Suite 550
Arlington, VA 22201-3052
703-516-6109
pbanks@ncmec.org

Philip Condu
OJJDP Program Coordinator
Fox Valley Technical College
Criminal Justice Department
1825 North Bluemound Drive
Appleton, WI 54914
800-648-4966
condu@foxvalley.tec.wi.us

Sergeant James Doyle
New York City Police Department
Computer Investigations &
Technology Unit
One Police Plaza, Room 1110D
New York, NY 10038
212-374-4247
jrdoyle@ix.netcom.com

Detective Robert Farley
Cook County Sheriff's Police
Department
Child Exploitation Unit
1401 S. Maybrook Drive
Maywood, IL 60153
708-865-4875
rfarley@wwa.com

J. Patrick Finley
OJJDP Program Manager
Fox Valley Technical College
Criminal Justice Department
1825 North Bluemound Drive
Appleton, WI 54914
800-648-4966
76065.463@compuserve.com



Kathy Free
Project Manager
Exploited Child Unit
National Center for Missing and
Exploited Children
2101 Wilson Blvd, Suite 550
Arlington, VA 22201-3052
703-516-7187
kfree@ncmec.org

Detective Sergeant Michael
Geraghty
New Jersey State Police
High Technology Crimes Unit
Building 14, River Road
West Trenton, NJ 08628
609-882-2000 x2555
michael_geraghty@ibm.net

Michelle Jezycki
Internet Crimes Against Children
Coordinator
National Center for Missing and
Exploited Children
2101 Wilson Blvd, Suite 550
Arlington, VA 22201
703-516-6147
mjezycki@ncmec.org

Robert Kreisa
President
Criminal Justice Associates
3180 Dans Drive
Stevens Point, WI 54481
715-342-4872
cja@coredcs.com

Ronald Laney
Director
Missing and Exploited Children's
Program
Office of Juvenile Justice and
Delinquency Prevention
810 7th Street NW
Washington, DC 20531
202-616-3637
laney@ojp.usdoj.gov

Senior Special Agent John
MacKinnon
United States Customs Service
Child Pornography Enforcement
Program
45365 Vintage Park, Suite 250
Sterling, VA 20166
703-709-6934
jpmac33@ibm.net

Michael Medaris
Program Manager
Missing and Exploited Children's
Program
Office of Juvenile Justice and
Delinquency Prevention
810 7th Street NW
Washington, DC 20531
202-616-3637
medarism@ojp.usdoj.gov

Sergeant Gary O'Connor
Lower Gwynedd Township Police
Department
1130 North Bethlehem Pike
Spring House, PA 19477
215-646-5303



Detective Wayne Promisel
Fairfax County Police
10600 Page Avenue
Fairfax, VA 22030
703-246-7813

John Rabun
Vice President and Chief Operating
Officer
National Center for Missing and
Exploited Children
2101 Wilson Blvd, Suite 550
Arlington, VA 22201-3052
703-516-6116
jrabun@ncmec.org

Ruben Rodriguez
Director
Exploited Child Unit
National Center for Missing and
Exploited Children
2101 Wilson Blvd, Suite 550
Arlington, VA 22201-3052
703-235-3900
rrodriguez@ncmec.org

Commander Bradley Russ
Portsmouth Police Department
Bureau of Investigative Services
3 Junkins Avenue
Portsmouth, NH 03801
603-427-1500
bruss@pd.cityofportsmouth.com

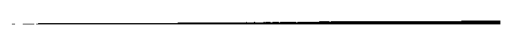
Lieutenant Bill Walsh
Dallas Police Department
Youth & Family Crimes Division
106 S. Harwood Street, Room 225
Dallas, TX 75201
214-670-5936
bcwalsh@gte.net



**PROTECTING CHILDREN ONLINE
UNIT COMMANDER/POLICY TRAINING**

Table of Contents

1. Computer Crimes Against Children
2. Introduction to Computer Technology
Overview of Online Communications
3. Unit Commander Responsibilities
4. Coordinating and Conducting the Investigation
5. Legal Issues
6. Resources
7. Appendix



**PROTECTING CHILDREN ONLINE
UNIT COMMANDER/POLICY TRAINING**

Mission Statement

The purpose of this training program is to provide law enforcement unit commanders with an understanding of the key management issues for the effective investigation, prosecution, intervention, and prevention of computer crimes against children.




Computer Crimes Against Children



**COMPUTER CRIMES
AGAINST CHILDREN**

*UNIT COMMANDERS' TRAINING
PROTECTING CHILDREN ON-LINE*


Presented by
Lt. Bill Walsh
Dallas Police Department



10-CCAC-1

LT. BILL WALSH

Youth & Family Crimes Division
Dallas Police Department
106 S. Harwood St. Rm. 225
Dallas, Texas 75201
214-670-7075
214-670-3759 Fax
bcwalsh@gte.net



10-CCAC-2

Child Sexual Abuse



10-CCAC-3

Child Sexual Abuse

- ◆ 61% of all rape victims are under 18 yrs. old
- ◆ Girls 12-15 are victims of violent crime at a rate 84 % higher than the general public
- ◆ While victimization can occur at any age, the ages between 7 and 13 years represent the peak period of vulnerability
- ◆ 40% of imprisoned sex offenders reported that their victims were less than 12 yrs. old.



WCCCA

Unique Problems with Child Sexual Abuse Investigations

- ◆ Child victims
- ◆ Dynamics of sexual abuse
- ◆ Disclosure process
- ◆ Forensic interviews of children

WCCCA

Child Victims

- ◆ Children are "perfect victims"
- ◆ They are often too trusting
- ◆ They often desire attention and affection
- ◆ They often desire material things
- ◆ They are often curious about sex
- ◆ They often defy their parents
- ◆ They are often not viewed as credible witnesses

WCCCA

Dynamics of Sexual Abuse

- ◆ Almost always occurs in private
- ◆ In the majority of cases, there is no medical evidence
- ◆ In most cases, child “knows” the offender
- ◆ Child may not want the offender punished

IC-CCAC-7

Disclosure Process

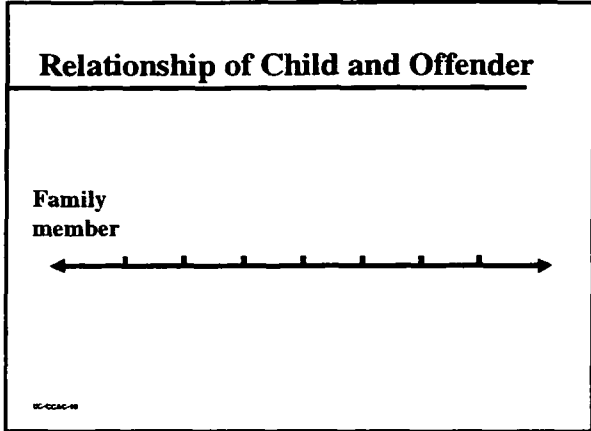
- ◆ Some children tell promptly
- ◆ Some children delay disclosing
- ◆ Some children give partial and/or progressive disclosures
- ◆ Some children never tell
- ◆ Some disclosures occur accidentally
- ◆ Some disclosures are initiated by others

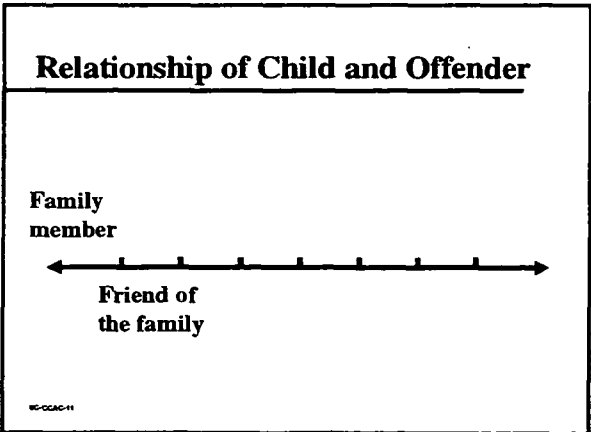
IC-CCAC-8

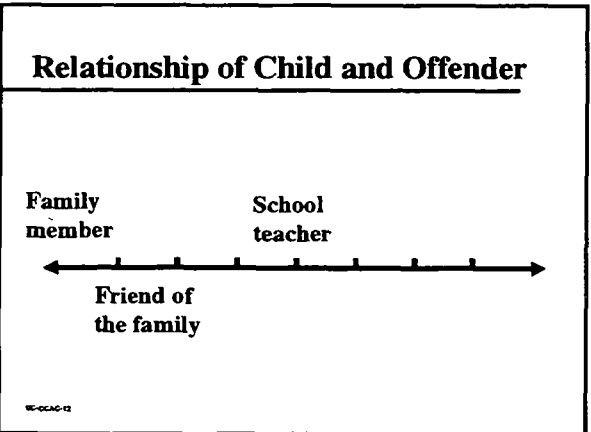
Forensic Interviews

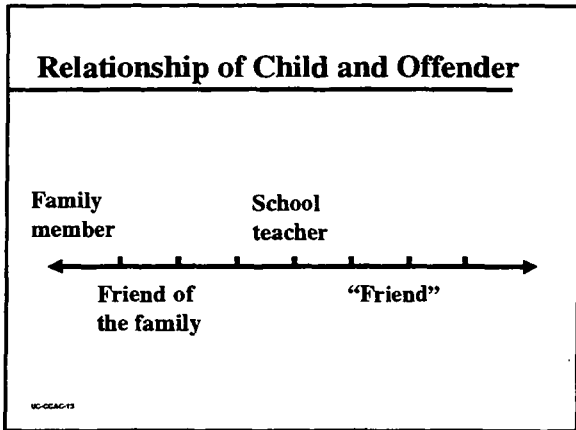
- ◆ Quality investigative interviews are critical to the investigation
- ◆ Require special training
- ◆ Must be legally defensible
- ◆ Must be developmentally appropriate

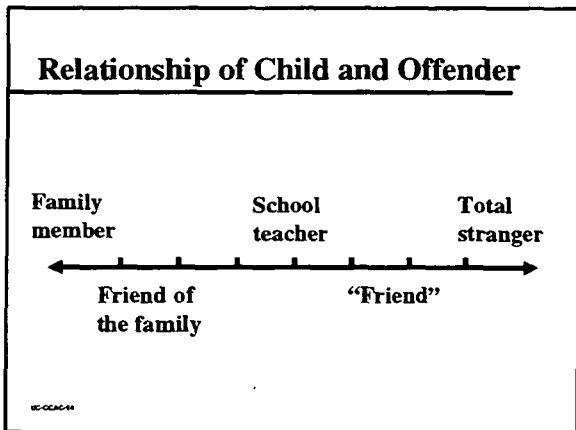
IC-CCAC-9

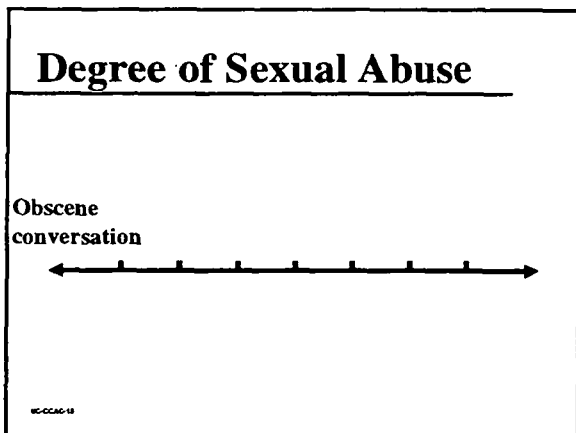


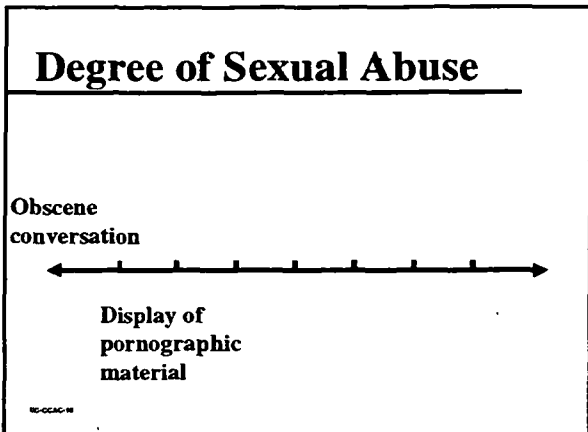


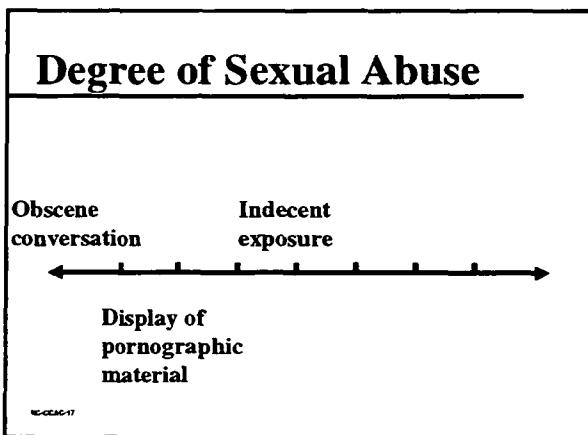


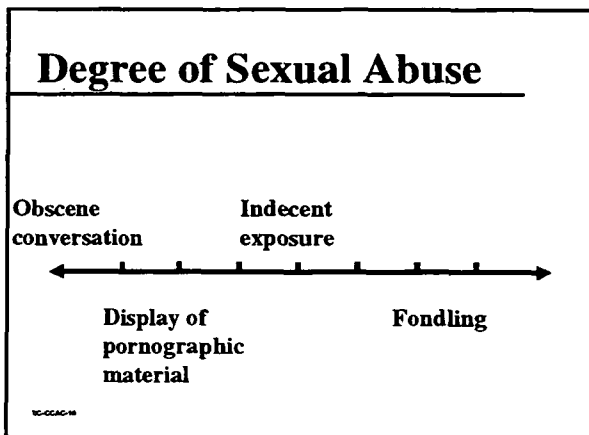


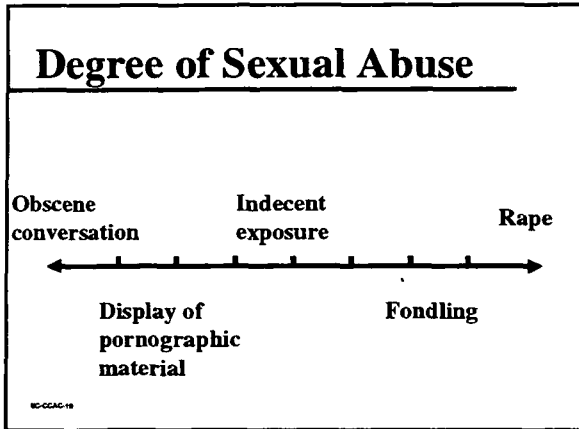


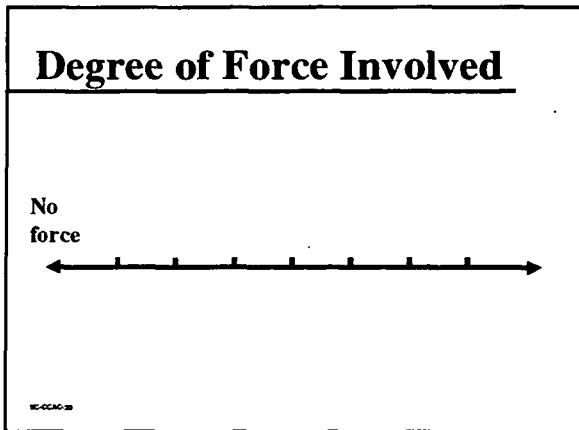


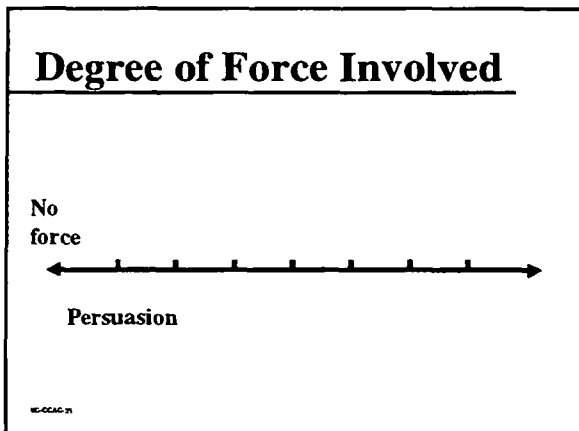


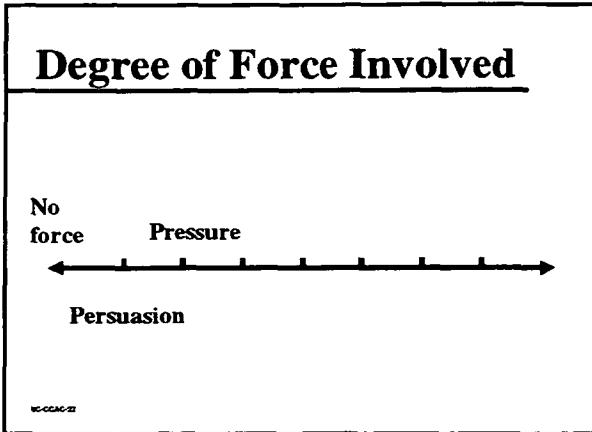


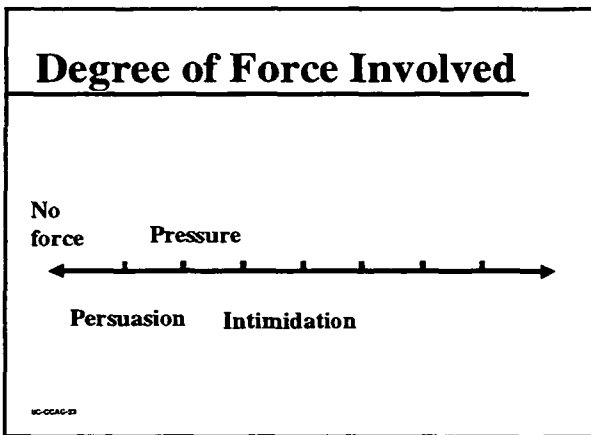


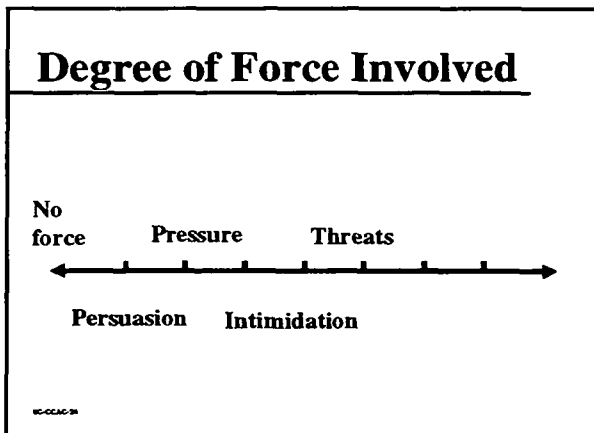


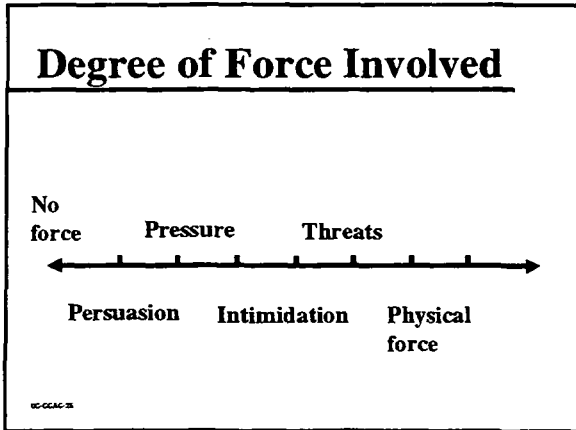


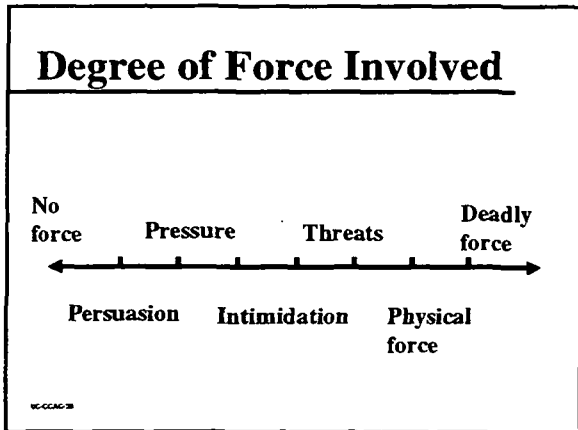


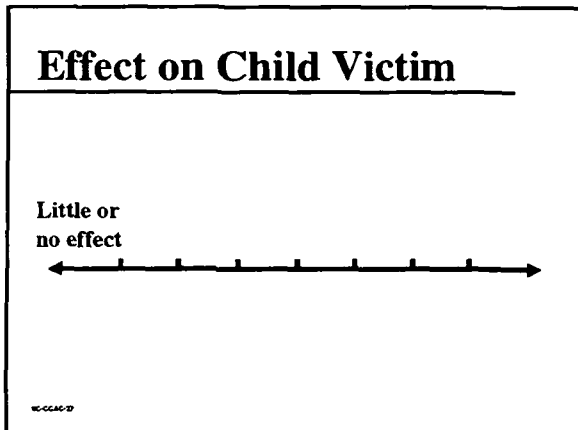












Effect on Child Victim

Little or no effect

Physical and Emotional problems

CC-CAC-2

Effect on Child Victim

Little or no effect

Substance abuse

Physical and Emotional problems

CC-CAC-2

Effect on Child Victim

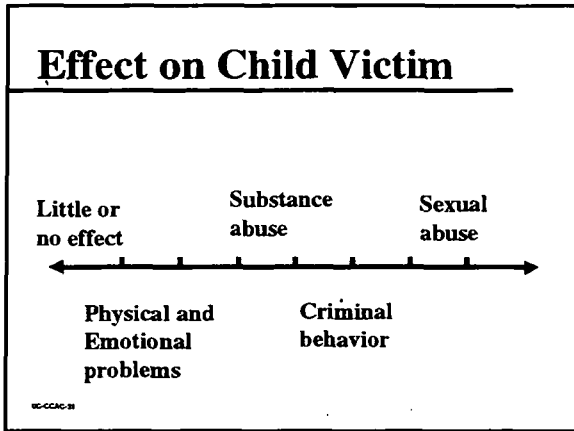
Little or no effect

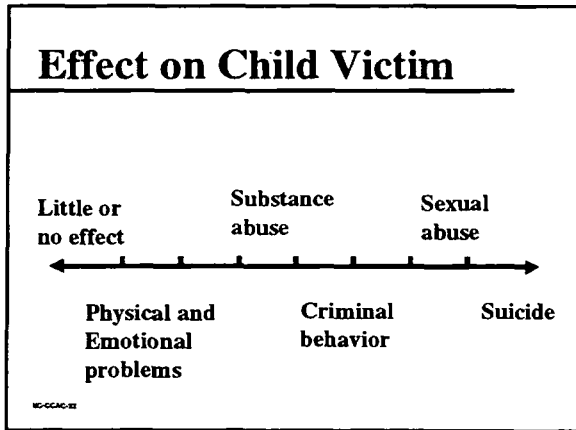
Substance abuse

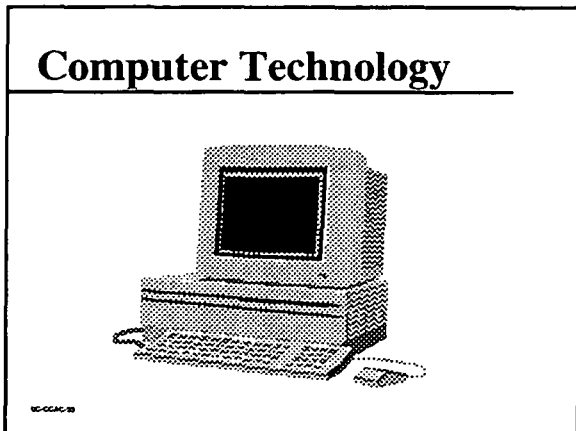
Physical and Emotional problems

Criminal behavior

CC-CAC-2







**Impact of Computer Technology
on the Sexual Abuse of Children**

Advancements in computer technology
Offender's sexual interest in children
+ Children's increased use of computers

= Increased use of computers by sex
offenders in the sexual abuse and
exploitation of children

10-00000-04

Relationship of Child and Offender

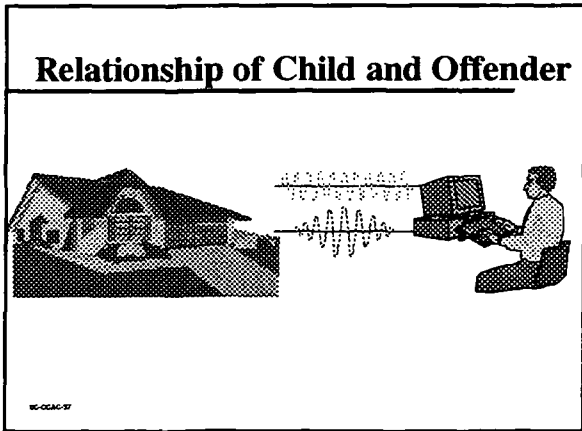


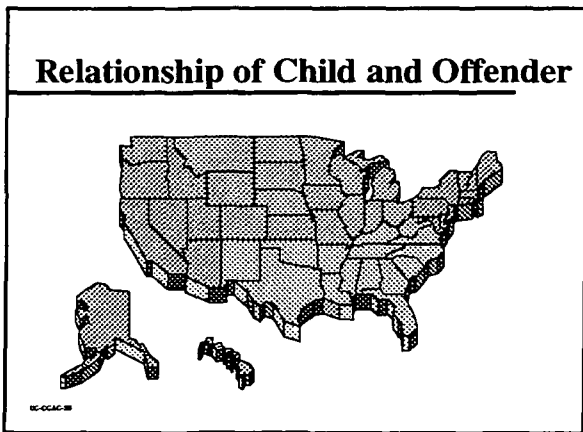
10-00000-04

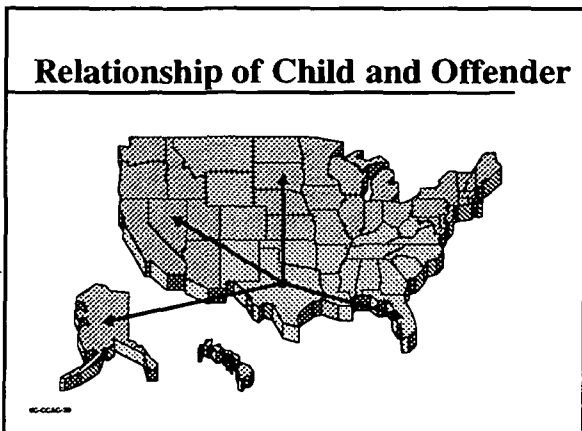
Relationship of Child and Offender




10-00000-04








Relationship of Child and Offender



16-CCAC-8

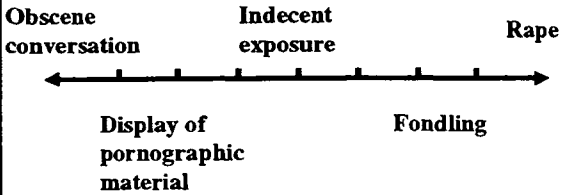
Relationship of Child and Offender



16-CCAC-8

Degree of Sexual Abuse

All types of sexual abuse are facilitated by the offender's use of computers



Obscene conversation Indecent exposure Rape

Display of pornographic material Fondling

16-CCAC-12

Computers as Tools used for the Sexual Abuse of Children



10-0000-0

Computers Appeal to Offenders

- ◆ Privacy
- ◆ Anonymity
- ◆ Instant gratification
- ◆ Expands their reach
- ◆ Facilitates their "interest" in children
- ◆ Accessibility
- ◆ Security

10-0000-0

Uses of Computers in the Sexual Abuse and Exploitation of Children

- ◆ Storage devices
 - child pornography
 - child erotica
 - diaries, letters
 - information on potential and actual victims

10-0000-0

Uses of Computers in the Sexual Abuse and Exploitation of Children

- ◆ **Medium for real time communication using Chat Rooms and E-mail**
 - with children
 - with other offenders

IC-CCAC-6

Uses of Computers in the Sexual Abuse and Exploitation of Children

- ◆ **Manufacture and distribution of child pornography**
 - homemade
 - commercial
 - morphed
- ◆ **Obscene display of adult pornography**

IC-CCAC-7

Uses of Computers in the Sexual Abuse and Exploitation of Children

- ◆ **On-line solicitation of children for meetings and subsequent sexual activity**

IC-CCAC-8

Uses of Computers in the Sexual Abuse and Exploitation of Children

- ◆ On-line solicitation of children for meetings and subsequent sexual activity
 - FBI's "Innocent Images" Investigation
 - » May 1993 disappearance of 10 yr. old boy
 - » 2 suspects arrested, multiple victims, over 25 yrs
 - » Computer used for transfer of child pornography and to lure minors into sexual activity
 - » To date:
328 search warrants 162 indictments
161 arrests 184 convictions

WCCAC-8

Computer Crimes Against Children

- ◆ New challenge to law enforcement in :
 - its ability to learn the latest computer technology and related laws
 - its ability to obtain the necessary equipment, personnel and training
 - its ability to protect children from sexual abuse and exploitation
 - and its ability to investigate it thoroughly when it happens

WCCAC-8

Effect on Society

- ◆ Need for New Legislation
- ◆ Increase in Computer Related Litigation
- ◆ Increased Funding for Criminal Justice Agencies
 - Law Enforcement
 - Prosecution
 - Probation and Parole
- ◆ Need for On-Line and Internet Oversight

WCCAC-8

1998 Justice Appropriations Act

- ◆ \$10 M to FBI to enhance "Innocent Images"
 - 40 new positions
 - Creation of a second "Innocent Images" Squad
- ◆ \$2.4 M to Office of Justice Programs & NCMEC
 - Plan for 8 regional internet crimes against children task forces

10-CCAC-02



Child Pornography on the Internet and the Sexual Exploitation of Children

Statement of Louis J. Freeh, Director
Federal Bureau of Investigation

Before the Senate Appropriations Subcommittee
for the Departments of Commerce, Justice, and State,
the Judiciary, and related Agencies

*Washington, D. C.
March 10, 1998*

Good morning, Chairman Gregg, Senator Hollings, and members of the Subcommittee. I am very pleased to appear before you today to discuss the problems of child pornography on the Internet and the sexual exploitation of children.

I would like to acknowledge the strong support of the Subcommittee for the FBI and other federal, state, and local law enforcement organizations and agencies working to protect children from computer sex offenders. Last April, this Subcommittee convened the first Congressional hearing during my tenure as Director that focused solely on this important issue. As I told the Subcommittee at that time, our children are our nation's most valuable resource. They represent the bright future of our country and hold our hopes for a better Nation. They are also among the most vulnerable members of society.

Your hearing last year was instrumental in raising public awareness to the seriousness of the problem of child pornography on the Internet. Your hearing also raised the recognition of this problem among law enforcement officers and prosecutors. Most importantly, you followed up your concern and commitment with action.

As a result of your efforts through the 1998 Justice Appropriations Act, the FBI, our state and local partners, and the National Center for Missing and Exploited Children, and others are taking positive actions to make our children's safety and future more secure by reducing their vulnerability to sexual predators using the Internet and commercial on-line services. Through your recognition of this issue, funding is available this year to improve the FBI's efforts to combat child pornography on the Internet, to enhance training and other related programs at the National Center for Missing and Exploited children, and to establish state and local law enforcement child sexual exploitation cyber-squads. This Subcommittee is making a significant difference in providing law enforcement with the tools and capabilities they need to respond to this problem. On behalf of law enforcement, I thank you.

Yesterday, I had the honor to join Senators Gregg and Hollings and Ernie Allen, the President of the National Center, at the dedication of the Cyber TipLine. The Cyber TipLine is one example of the type of joint public-private sector partnerships that are mutually beneficial to law enforcement and the public, especially to our children. I hope that yesterday's events will bring to the public's attention the

availability of the TipLine and that its use will assist in preventing innocent and unsuspecting children from being exploited and harmed.

IMPLEMENTATION OF 1998 FBI ENHANCEMENTS

I would like to start by bringing the Subcommittee up to date on how the FBI is using the additional staffing and funding provided for child pornography investigations that was included in the 1998 Justice Appropriations Act. The Act provided \$10.0 million for enhancing our ongoing "Innocent Images" initiative which is a nationwide investigation coordinated in the FBI's Baltimore, Maryland, field office. This funding allows for 60 new positions, including 25 agents. As we allocated these additional resources, we considered and balanced the full range of requirements needed for the "Innocent Images" initiative, including additional investigators for Baltimore and other key locations, analysts, laboratory examiners and services, training and outreach, and case management automation. I believe the plan that we are implementing allows us to have the most impact with the additional resources the subcommittee provided us.

Baltimore. Most of the new positions -- 40 total, including 13 agents and 12 Intelligence Research Analysts -- are being assigned to our Baltimore Field Office. At Baltimore, we are creating a second "Innocent Images" squad to expand the scope of our current on-line undercover operation. Baltimore will also be able to provide 24-hour support to "Innocent Images" cases that involve suspects located in other FBI field offices. Currently, 95 percent of the "Innocent Images" cases generated by the Baltimore Field Office involve suspects who live in states other than Maryland.

The "Innocent Images" agents assigned to Baltimore will also use their expertise to provide training programs for state and local law enforcement and prosecutors, including those trained through the National Center for Missing and Exploited Children. Two special agents from the Baltimore Division's "Innocent Images" staff will be assigned as instructors to teach law enforcement officers on-line child pornography/child sexual exploitation investigations. Since last April, FBI "Innocent Images" staff have made 54 presentations to approximately 2,100 state and local law enforcement officers and prosecutors.

We are also improving the "Innocent Images" case management system that supports on-line sessions conducted by undercover agents and which stores case and federal grand jury subpoena information. With the additional cases that will be generated by the increased number of agents added to the "Innocent Images" squads, an updated system is needed.

Los Angeles. The FBI's Los Angeles Field Office plays a significant role in support of the "Innocent Images" initiative, including the conducting of on-line undercover sessions. We are placing 4 agents and 1 intelligence research specialist in the Los Angeles Field Office where they will be dedicated to supporting the "Innocent Images" initiative. These agents will allow the Los Angeles Field Office to provide more timely follow up investigations regarding suspects identified and referred by the Baltimore Field Office, as well as initiate new Internet and on-line service child pornography investigations. Investigations by the Los Angeles Field Office are being fully coordinated with the national "Innocent Images" task force in Baltimore.

Forensic services. Child pornography investigations and prosecutions depend upon the identification and timely analysis of evidence from seized computers and media used to produce, store, and transmit illegal images and pictures. Individuals involved in the distribution and exchange of on-line child pornography and the recruitment of children for illicit sexual purposes are among the most sophisticated computer users the FBI is encountering. The additional cases that will be generated by the new squad being established in Baltimore will also increase the forensic workload of the FBI Laboratory. Consequently, improving FBI Laboratory capabilities to respond to the growing number of these cases is a high priority.

We are adding 6 positions, including 5 agents, to the FBI Laboratory to increase the number of examiners performing forensic examinations of computer-related evidence from "Innocent Images" cases. These agents will also travel to other field offices to assist in the execution of search warrants generated from cases developed by the "Innocent Images" squads.

Pocatello Information Technology Center. We are also adding 2 intelligence research specialists to the FBI Information Technology Center (ITC) located in Pocatello, Idaho. The Pocatello ITC provides a variety of overall case support services for "Innocent Images" investigations, including searches of commercial databases to locate and trace suspects and fugitives. During a court authorized wire interception in an on-line child pornography investigation, the very first of its kind, analysts at the Pocatello ITC directly assisted our investigators in the administration of this electronic surveillance.

Child Abduction and Serial Killer Unit. The FBI's Child Abduction and Serial Killer Unit provides critical behavioral profiling to FBI field offices, other federal agencies, and state and local law enforcement agencies working missing children cases and serial crimes, including cases involving sexual predators. Beginning in September 1997, the FBI began distribution of a "Child Abduction Response Plan" to over 17,000 federal, state, and local agencies to provide suggestions and guidance, based upon our experience, on dealing with these types of tragic incidents. This plan was prepared by the Child Abduction and Serial Killer Unit.

We are adding 2 additional agents and 1 Intelligence Research Specialist to ensure this Unit continues to provide timely and effective response to requests from law enforcement for assistance in missing children and child exploitation cases, especially those in which sexual predators use the Internet or on-line services to entice children to meet for illicit sexual purposes.

Liaison with the National Center for Missing and Exploited Children. The FBI is in the process of assigning a Special Agent full-time to the National Center for Missing and Exploited Children to improve our liaison with the Center and to facilitate the timely referral of child sexual exploitation and missing children complaints and tips to FBI field offices.

Training. Just one and one half weeks ago, the FBI conducted the first of five regional On-line Child Pornography/Child Sexual Exploitation conferences in Atlanta, Georgia. Attending that conference were 30 FBI agents and 200 state and local law enforcement officers and officials from 7 Southeastern states: Georgia, Florida, South Carolina, North Carolina, Tennessee, Alabama, and Mississippi. Other regional conferences will be held this year in Dallas, Texas; Los Angeles, California; Chicago, Illinois; and Newark, New Jersey. These conferences are possible due to the additional funding provided in 1998.

Later this year, we are planning to convene a national-level symposium on Internet and on-line child pornography and child exploitation for all FBI field offices. Through this symposium, we hope to bring together FBI Special Agents who work on-line child pornography/child sexual exploitation investigations, prosecutors, Internet and on-line service providers, and others to exchange ideas and to build bridges between the various groups that will have a positive impact on reducing the vulnerability of children to these types of crimes.

Training law enforcement, prosecutors, and others is an important element of our effort to combat child pornography and child sexual exploitation on the Internet. We will continue our training efforts in 1999.

Increasing Public Awareness. One of the most effective ways to prevent children from becoming victims of on-line sexual predators is to educate them and their parents to follow safe Internet and on-line practices. Too often, unsuspecting children believe they are talking to a peer with similar interests and hobbies when, in fact, they are being recruited by a sexual predator who is exploiting the anonymity allowed by the Internet to hide his true intentions.

Thanks to your suggestion, Mr. Chairman, and that of Senator Hollings, we are incorporating Child Awareness of On-line Child Exploitation into the FBI Headquarters tour. Annually, more than 500,000 people take the FBI tour with the majority being school age children.

Among the ideas we are considering are short videos highlighting the issues of child abduction and child safety on the Internet that could be shown on televisions installed in the general waiting areas for tours. We are also considering locating two or three kiosks containing interactive computers along the tour route that would offer two different information programs, one for adults and one for children, relating

to child safety on the Internet. Finally, we are considering a Crimes Against Children display that would be constructed and located outside the Firearms Range waiting area. The National Center for Missing and Exploited Children is working with us in developing these ideas and content.

"INNOCENT IMAGES"

The FBI initiated its "Innocent Images" investigation in 1995 as an outgrowth of the investigation into the disappearance of ten-year-old George Stanley Burdynski, Jr., in Prince George's County, Maryland. Investigation into the activities of two suspects determined that adults were routinely using computers to transmit images of minors showing frontal nudity or sexually explicit conduct, and to lure minors into illicit sexual activities.

"Innocent Images" focuses on individuals who indicate a willingness to travel for the purposes of engaging in sexual activity with a child; individuals who produce and/or distribute child pornography through the Internet and on-line services; and, individuals who post illegal images onto the Internet and on-line services. The FBI has investigated more than 70 cases involving pedophiles traveling interstate to meet minors for the purposes of engaging in illicit sexual relationships.

FBI Agents and other federal, state, and local investigators participating on the "Innocent Images" task force go on-line in an undercover capacity, posing as either young children or as sexual predators, to identify those individuals who are victimizing children. The coordinated effort has generated significant results: since 1995, the "Innocent Images" investigation has generated 328 search warrants, 62 consent searches, 162 indictments, 69 informations, 161 arrests, and 184 convictions.

I am particularly pleased to report that since March of 1997, the number of search warrants executed increased 62 percent; the number of indictments obtained increased 50 percent; the number of arrests increased 57 percent; and the number of convictions increased 45 percent.

As I mentioned earlier, we have started on-line "Innocent Images" investigations in our Los Angeles field office. We are also considering the need for on-line "Innocent Images" efforts in other field offices based upon workload and the identification of specialized user populations involved in on-line child pornography and related sexual offenses. All of these efforts will be coordinated with and through our Baltimore Field Office.

The "Innocent Images" initiative has expanded its investigative scope to include investigations involving news groups, Internet Relay Chat (IRC) and file servers (also known as fserver).

CHALLENGES FOR COMBATING CHILD EXPLOITATION

I would like to comment briefly on several challenges that face not only the FBI, but all of law enforcement, as we move ahead in our efforts to combat Internet and on-line child pornography and sexual exploitation.

Encryption. When I testified last week before the Subcommittee on the FBI's 1999 budget request, I outlined for the Subcommittee a number of challenges facing the FBI as it moves toward the 21st century. One of these challenges is the growing use of encryption by criminals to conceal their illegal activities. The "Innocent Images" initiative has uncovered sexual predators who use encryption in their communication with each other and in the storage of their child pornography computer files. This encryption is extremely difficult, and often impossible, to defeat.

It is essential that law enforcement agencies at all levels of government maintain the ability, through court order, to access encrypted communications and data relating to illegal activity.

National Coordination. The FBI has designated its Baltimore Field Office as the national coordinator for its "Innocent Images" initiative. Investigations of "Innocent Images" referrals conducted by other FBI Field Offices are coordinated through Baltimore.

Numerous other federal, state, and local law enforcement agencies are initiating on-line undercover child exploitation investigations, some as part of task forces and others on an individual agency basis. As more law enforcement agencies begin to use this investigative technique, the likelihood that one agency will begin investigating another agency's undercover operation will increase. This is an obvious waste of very finite resources. On-line child exploitation investigations often cross jurisdictional lines and, in some instances, even national boundaries. Investigations that begin in one area may branch off to involve locations throughout the country and have links to other ongoing investigations. These types of cases must be coordinated among the various law enforcement agencies having jurisdiction. I believe the FBI is in a position to provide valuable and effective leadership to spearhead this national effort.

The 1998 Justice Appropriations Act provides \$2.4 million to the Office of Justice Programs for grants to establish state and local law enforcement cyber-squads. This subcommittee also instructed that these cyber-squads follow the investigative protocols developed by the Department of Justice in the "Innocent Images" investigation. The Office of Juvenile Justice and Delinquency Prevention, the Child Exploitation and Obscenity Section of the Criminal Division, the FBI, and the National Center for Missing and Exploited Children are working closely together to develop a plan for the formation of eight regional state and local task forces using these funds.

I would like to see our "Innocent Images" initiative serve as a national clearinghouse, with links to a network of regional task forces staffed by federal, state, and local investigators. Such a clearinghouse and network would enhance support for, and coordination of, on-line child exploitation investigations and facilitate the sharing of intelligence information gathered through undercover sessions and cases.

DNA Profiles. Sexual predators have predictable behavior traits. Clinical research studies have found that the average child molester will have more than 70 victims throughout his lifetime. DNA profiles are one law enforcement tool that can be effective in quickly identifying suspects.

The FBI continues to work with states to establish the Combined DNA Information System (CODIS) that will allow state and local crime laboratories to exchange and compare DNA profiles electronically, thereby linking serial violent crimes and to identify suspects by matching DNA evidence to offender profiles. CODIS is operational in 86 crime laboratories in 36 states and the District of Columbia.

Currently, 48 of 50 states and all territories and possessions have enacted laws allowing the collection of DNA samples from convicted sex offenders and others convicted of violent crimes. We are working with the two states that do not have laws and expect those states to enact appropriate laws this year. At this time, there is no comparable effort to collect and maintain DNA samples from individuals convicted federally for sex crimes and other violent offenses. As a result of the "Innocent Images" initiative and other cases, more and more individuals are being convicted in Federal Court for sex offenses involving minors.

Steps need to be taken to close the gap between state and federal DNA profiling efforts so that a true nationwide database of DNA profiles for all convicted sex offenders is available.

Sex Offender Registry. The permanent national sex offender registry is scheduled to be implemented in July 1999 when the National Crime Information Center (NCIC) 2000 system becomes operational. This file will have the capability to retain an offender's current and previous registered addresses, dates of registration and conviction(s), photograph and fingerprints. Currently, an interim National Sex Offender Registry is operational which utilizes the FBI's Interstate Identification Index and the National Law Enforcement Telecommunications System. The initiative became operational in February 1997. As of February 12, 1998, 23 states are participating in the Registry with 30,778 records flagged as sex offenders.

Industry Actions and Assistance. Over the past year, we have seen positive steps by the software and Internet Service Provider industries to reduce the availability of pornography to minors. Some Internet Service Providers are exploring different methods for protecting our children; to include blocking access to chat rooms and Internet news groups -- the places where Sexual Predators target and recruit minors.

Some site providers are using proof of age and similar shielding systems to keep underage children from accessing sites containing adult-oriented materials.

Yet, more can and should be done to keep sexual predators from being able to reach our children through the Internet and commercial services. I urge the manufacturers of software products, those used for connecting to the Internet and also used in modems and computers, to include with their products a copy of the Internet safety publications prepared by either the FBI, the National Center for Missing and Exploited Children, the Department of Education or a pamphlet of their own design. This simple action would help raise the awareness of parents and provide children with safety tips and practices to use while enjoying the Internet.

Another problem we encounter is access to subscriber information. When we identify an individual's screen name -- not their subscriber name -- through an on-line session, we must secure a Federal Grand Jury subpoena and then go to the Internet Service Provider to obtain subscriber and account information for that particular screen name. Oftentimes, sexual predators and others use multiple screen names or change screen names on a daily basis. Some Internet Service Providers retain screen name identifiers for such short periods of time -- in some instances less than two days -- that when law enforcement presents a subpoena, the Internet Service Provider is not able to retrieve from its archives the requested subscriber and account information.

The telephone industry is required by Federal Communications Commission regulation to maintain subscriber and call information for a fixed period of time. It would be beneficial for law enforcement if Internet Service Providers adopt a similar approach for retaining subscriber information and records for screen names and associated Internet Working Protocol numbers, or "IP addresses." Such information, when provided to law enforcement upon service of a subpoena, is critical to the timely identification of persons sending child pornography or trying to recruit a child for illicit sexual purposes.

Where possible, it would be beneficial for Internet service providers to capture and retain Caller ID data on persons accessing ISP lines. The capturing of Caller ID data will greatly assist law enforcement in child pornography/child sexual exploitation investigations.

CRIMES AGAINST CHILDREN

Our efforts to combat child pornography on the Internet and commercial service providers is one element of the FBI's comprehensive Crimes Against Children Initiative. The FBI's overall goal for its Crimes Against Children initiative is to provide a quick and effective response to all reported incidents. Through a timely response, we believe the FBI can, in conjunction with its law enforcement partners, increase the number of incidents in which the victimization of children is stopped and increase the likelihood that abducted or missing children are safely recovered.

In each of our field offices, we are reaching out to our state and local law enforcement partners to encourage them to notify the FBI within that critical first hour of a reported child abduction or missing child. Once notified, our goal is to rapidly deploy those resources necessary to support or conduct an investigation.

I directed that two things be done to help ensure a timely notification is made in these cases. On February 2, 1997, the FBI added a new dimension to the National Crime Information Center (NCIC) that allows law enforcement agencies to "flag" entries when there is a reasonable indication that a child is missing under suspicious circumstances or that the child is believed to be in a life-threatening situation. NCIC then notifies the National Center For Missing and Exploited Children and the FBI's Child Abduction and Serial Killer Unit. Special thanks go to Senator McConnell for his pioneering work that led to this new program.

Shortly after last year's hearing, in May 1997, I instructed each Special Agent in Charge to designate two FBI Agents to serve as Crimes Against Children Coordinators within their field office territories and to serve as field office points of contact for notifications.

No single law enforcement agency is equipped to handle the broad spectrum of issues that accompanies crimes against children. Working together, we can leverage our individual capabilities and expertise into an effective and comprehensive resource team. I have instructed each FBI field office to begin establishing multi-agency, multi-disciplinary resource teams consisting of federal, state and local law enforcement, prosecutors, victim/witness specialists, and health and social service professionals. These resource teams will facilitate interagency sharing of intelligence and information and enable effective investigation and prosecution of cases that transcend jurisdictional and geographical boundaries.

The FBI's 1999 budget includes a request for 81 positions, including 30 agents and 31 victim/witness coordinators, and \$8,009,000 to improve the delivery of law enforcement services to Indian Country. Between 1994 and 1997, 83 percent of the crimes on Indian reservations cases opened by the FBI involved either crimes of violence (47 percent) or the sexual or physical abuse of a minor child (36 percent). I urge your support for these additional resources that will allow us to investigate crimes against children living in Indian Country.

CONCLUSION

Mr. Chairman, I would like to again express my gratitude for the Subcommittee's strong support and confidence in the FBI. Both you and Senator Hollings can take pride in the leadership exerted by the Subcommittee in the area of protecting our children from sexual offenders and pedophiles. I believe your approach of balancing targeted increases in FBI investigative resources and capabilities in select areas with an emphasis on training for state and local law enforcement encourages partnerships and cooperation that are the keys to an effective response to the problem of Internet and on-line child pornography and child exploitation by sexual offenders and pedophiles.

This concludes my prepared remarks. I would like to respond to any questions that you may have.



[Congressional Affairs](#)



[FBI Home Page](#)



Introduction to Computer Technology

Overview of Online Communications



Protecting Children On-line
Unit Commander Course

**Introduction to Computer Technology
and Online Communications**



Today's Topics

- **Computers and crime**
- **How computers work**
- **Computer hardware and software**
- **Computer networks**
- **The Internet**



**What is Driving the Rapid
Pace of Change in Society?**



Here is a Hint!



Old Crimes



- New techniques and tools
- New types of evidence

Cybercops Face Net Crime Wave

Interactive Week Magazine, June 1996

In a bank robbery , we know to put up yellow tape around the scene, watch the video, and dust for prints. But on the Internet, you cannot seal off the area and get out of the way.

Scott Charney, U.S. Department of Justice

Futurists Predict



- Technology and policing tactics will eliminate much conventional crime
- Technology and computer crime will take the place of conventional criminal acts

“By the year 2000, there will be so much computer related crime, law enforcement will be reduced to taking reports because we will not know how to investigate it.”

**Dr. William Tafoya
1988 and 1997**



Attorney General Janet Reno



- 10/26/96 IACP General Assembly
- Identified computer crime as one of her top three priorities
 - Computers used to commit crimes
 - Computers that were victims of crime
 - Computers used to store data of a criminal enterprise

Pornography

- Rule in cyberspace is anything goes
- Sex flourishes on the Internet
- Gigabytes of graphic material that is easily downloaded
- Virginia security firm says there is some form of pornography in one of four corporate computers

--

Sexual Predators



- Find victims on the Internet
- Pose as other children
- Find kids in chat rooms, newsgroups
- Transmit and exchange child pornography
- Send unsolicited pornography
- Market in kiddy porn
- Other techniques will be discussed

--

Our Aim

- To understand how computer technology is changing the nature of criminal investigations and evidence
- To understand computers and the on-line world and be conversant with investigators in technology matters
- To reinforce the importance of competent and thorough investigations



--

How Do Computer's Work?

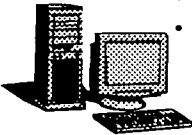
- They manipulate and store bits and bytes of digital information
- 1's and 0's
- Requires a combination of hardware and software to work



...

Hardware

- Processing devices
- Input / output devices
- Storage devices and media
- Communications devices



...

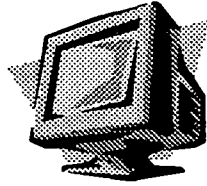
System or Base Unit

- Contains mother board, CPU, hard drive, power supply
- Floppy drive is generally installed
- Higher capacity storage devices may be installed, such as zip or tape drives

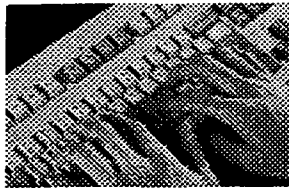


...

Monitor or CRT

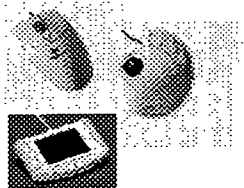


Keyboard



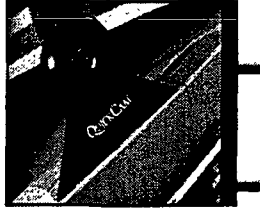
Pointing Devices

- Mouse
- Trackball
- Touch pads
- Touch screens



Video and Audio Devices

- Speakers, microphones and headsets for online voice communications
- Video cameras for online video applications



LC 18

Peripherals Commonly Used

- Scanners
- Digital Cameras



LC 20

Storage Devices and Magnetic Media

- Used to store digital information
- May be part of the computers system unit or a separate peripheral
- Consists of a device to read and write the data and a magnetic media to store the data on.
- Capacity measured in the amount of bytes of information they will store

LC 21

Some Examples

- Floppy disks 1.44 MB
- Zip Drives 100 MB



INTERNAL ZIP DRIVES

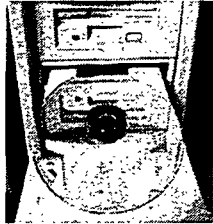


PORTABLE ZIP DRIVES

UC 22

CD-Roms

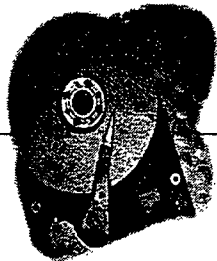
- 650 MB Capacity (read and write)



UC 23

Hard Drive

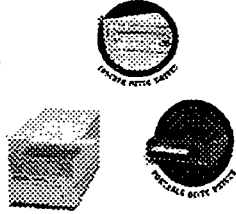
- Generally installed in system unit
- Up to 8 GB capacity on consumer computers



UC 24

Tape Drives

- Back up tape drives store up to 10 GB
- 8 mm tapes (DAT) up to 20 GB



...



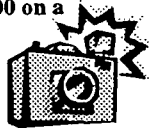
What can you fit into a 4 inch square? 1 GB Capacity



...

With an average picture size of 50,000 bytes

- You could store 20,000 images on one jaz drive
- You could store 400,000 on a DAT tape



...

Modem



- Modulator/demodulator
- Turns digital computer data--bits and bytes--into analog information
- Allows computer data to be transmitted over conventional phone lines
- Capabilities are rapidly changing

--

The Evolution of Computer Power

- The growth of computer capabilities in several areas has made today's applications and communications possible
 - Processing speed
 - Communications speed
 - RAM (random access memory)
 - Storage



--

Processor Speed

- Early computers had clock speed of less than 1 MHz
- Today you can affordably buy a computer that runs at 333 MHz



--

Communication Speed

- Earliest consumer modems communicated at 120 BPS
- Today you can purchase one that is capable of 56,000 BPS over conventional phone lines
- 1.5 million BPS in near future



...

Random Access Memory

- Early consumer PC's had 1000 to 4000 bytes
- Today this laptop has 32 million bytes, and could easily have more



...



Storage

- Early floppy disks held 120,000 bytes of data
- Early hard drives held 10 million bytes
- Today you can store a gigabyte (billion) of data on a small cartridge
- Hard drives in consumer machines hold up to 8 gigabytes and more

...

This Power Enables

- **Great strides in productivity in many areas**
- **Easier means to store, share and manipulate images, such as child pornography**
- **Real time audio and video communications via computer networks**



--

Computer Power is Rapidly Increasing



It is safe to predict that computers in the year 2047 will be at least one hundred thousand times more powerful than those of today

Gordon Bell and James Gray of Microsoft

--

Computing Power in the Future will Create More Benefit, but will also Create More Opportunity to Exploit the Technology for Criminal Purposes



--

Software

- Operating systems
- Application software
- Data files



--

Operating Systems

- DOS
- Windows 95
- Windows NT
- Unix
- Many others



--

Applications Software

- Word and Word Perfect
- Excel
- Database packages
- Thousands of others, both commercial or developed for specific users



--

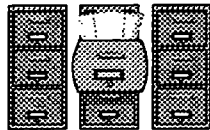
Applications Used in Child Pornography

- Photo editing software
- Graphics viewers and converters
- Scanning software
- CU-See Me and other video applications



Data Files

- Data files from specific application
- Text
- Sound
- Graphics



Picture Formats

- Pictures on computers come in hundreds of formats
- The most common formats on the Internet are GIF (graphics information format) and JPEG (photographic experts group format)
- These two formats compress pictures into small file sizes
- Files will appear as filename.gif or filename.jpg



Connectivity and Computer Networks



...

Networks



- Interconnected computers that can share data
- May be in one room or around the world
- Usually a client/server architecture
- May be as small as a two machine peer to peer network
- May be as big as Hewlett Packard's intranet consisting of 90,000 PC's, 23,000 workstations, 4000 servers, and 800 mini-computers



...

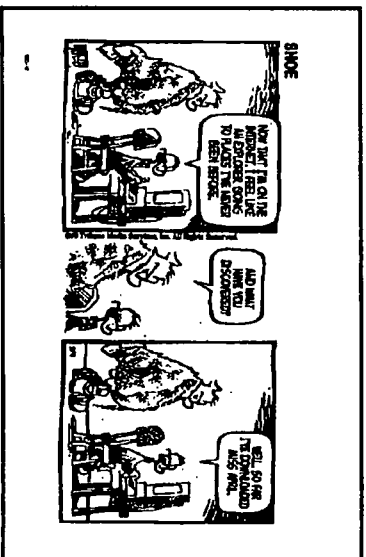
But the World's Biggest Network is the Internet

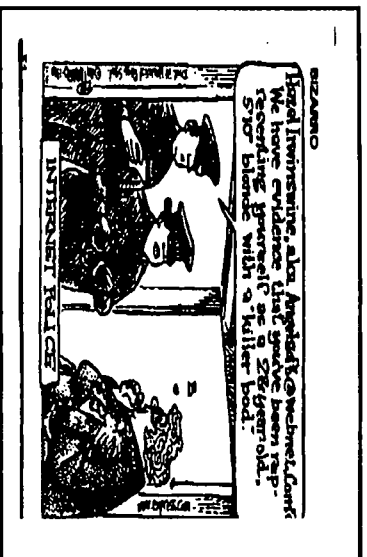


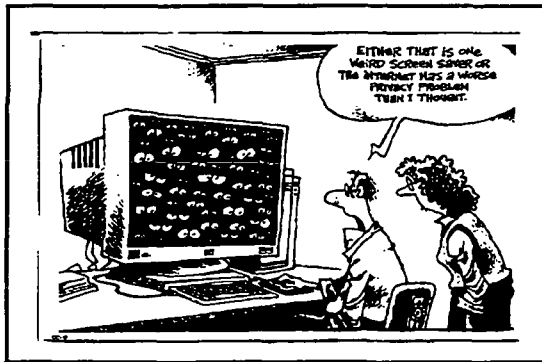
A Network of Networks

...











"Everyone has a different Internet."

- Bruce Sterling, science fiction writer and Internet philosopher



Why was the Internet Created?



- Why was the Internet created?
 - Defense Dept. Strategy
 - Share information
 - Communication

Internet Timeline



- 1957 – the USSR launched Sputnik, the first artificial earth satellite. In response, the US Department of Defense formed the Advanced Research Projects Agency (ARPA) to establish the US as a leader in military technology and science.
- 1969 – ARPANET commissioned by DoD for research into national networking in the event of a nuclear disaster. First nodes: UCLA, Stanford, UCSB, and U of Utah.
- 1979 – USENET established between Duke and UNC.

--



- 1986 – NSFNET created, linking the United States into one large network, hundreds of universities come online.
- 1988 – First foreign countries connect into NSFNET and –IRC (Internet Relay Chat) developed.
- 1992 – World-Wide Web is released.
- 1993 – Business and media begin to take notice of the Internet. Mosaic takes the Internet by storm, WWW proliferates at a 341,634% annual growth rate.

--



- 1996 – The Internet is the dominant theme throughout the computer industry.
- And Beyond – Personal and private use of the net grows exponentially, and will continue to do so

--

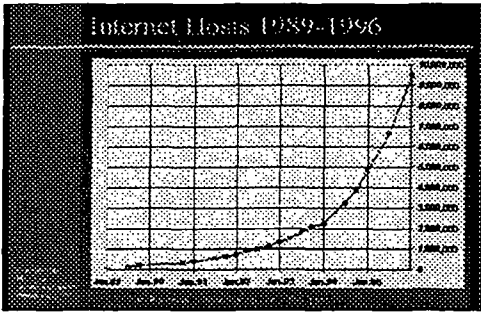
The Internet



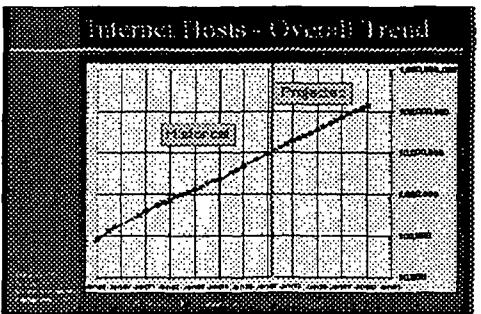
It is not far-fetched to expect that the net will gradually reorganize how, what, where and when we produce and consume

Riel Miller, The Internet in Twenty Years: Cyberspace, the Next Frontier?, 1997

Internet Hosts 1989-1996



Internet Hosts - Overall Trend



Internet Time

Three Months Equals One Year



-Paul Wormeli, PSI International

Connecting to the Internet

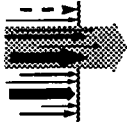


Getting On-Line

- **Hardware**
 - Modem
 - Computer
 - Telephone Line
- **Software**
 - Web browser
 - Other applications
- **Internet Account**



Four Basic Ways to Access the Internet



- Shell Account access
- PPP Dial-Up access
- Commercial Service access
- Leased-line access

--

Shell Account Access

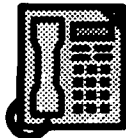
- Low end connection
- Computer acts as dumb terminal
- No graphics
- BBS or FreeNet
- Unix Connection



--

PPP Dial-Up Access

- PPP = Point to Point Protocol
- High end connection
- Local Service Provider
- Low cost
- Allows for greater flexibility - software stored on your computer



--

Commercial Service Access

- Prodigy
- CompuServe
- America Online
- Delphi
- MSN



Leased Line Access



- Most expensive access
- High speed, digital transmission
- Direct line-always on
- 5 to 10 times faster than regular modem
- Government agencies, corporations and research institutions



So What's Out There?



- Text files
- Graphics files
 - Pictures
 - Movies
 - Streaming Video
- Sound files
 - Internet Telephony

Some Internet Clients/Applications

- E-Mail
- Mailing Lists
- Newsgroups
- FTP
- Telnet
- Gopher
- World Wide Web



E-Mail

- ◆ Most popular Internet application
- ◆ Easy way to send /receive messages and files
- ◆ No long distance charges, fast, cost-effective
- ◆ Global communication and data exchange
- ◆ Ability to send mail to a group
- ◆ Permanent log of correspondence



Names and Addresses

- E-mail users will have an e-mail address
- An e-mail address will resemble the following:

cja@coredcs.com

cja= username
coredcs= internet service provider
com= domain



Common Address Domains

- Domestic US Domains
 - .COM -- Commercial Institutions
 - .EDU -- Academic Institutions
 - .GOV -- US Government
 - .MIL -- Military
 - .NET -- Network Institutions
 - .ORG -- Non-profit Organizations
- International Domains
 - .AU - Australia
 - .CH - Switzerland
 - .UK - United Kingdom
 - .CA - Canada
 - .NL - Netherlands



Newsgroups/Usenet

- Subject specific discussion forums
- Delivered via a universal feeder network called Usenet
- Messages kept on news servers, which carry various newsgroups
- Messages are not delivered to your mailbox, you must visit a Newsgroup
- 18,000+ Newsgroups exist



Newsgroup Basics

- All newsgroups are divided into categories or hierarchies, which try to define a broad commonality.
- Newsgroup names start with a very broad hierarchy area, followed by more specifics on the topic of discussion.



Newsgroup Hierarchies

Hierarchy:	Category:
bionet	Biology Research
bit.listserv	LISTSERVs
biz	Business
comp	Computers
misc.	Stuff that doesn't fit elsewhere
news	News about USENET
rec	Hobbies, games and recreation
sci	Science other than biology
soc	Social groups, ethnic groups
talk	Politics and related topics
alt	Controversial or unusual topics

--

Sample Newsgroups

- alt.abuse-recovery -- Helping victims of abuse recover
- alt.barney.dinosaur.die.die.die -- Barney haters unite!
- bionet.jobs -- Biology job listings
- bit.listserv.xerox-1 -- Xerox products
- biz.books.technical -- Selling and buying books
- clari.biz.top -- Top business news
- comp.cog-eng -- Cognitive engineering



--

Newsgroups Are Used Extensively by Sexual Predators

- Largest single area of pornography and child pornography
- Meetings are set up in newsgroups and child pornography and communications can be exchanged using a private application
- No controls over newsgroups except by ISP's who may decide not to carry some

--

Some Examples

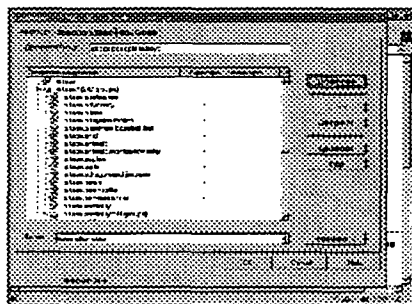


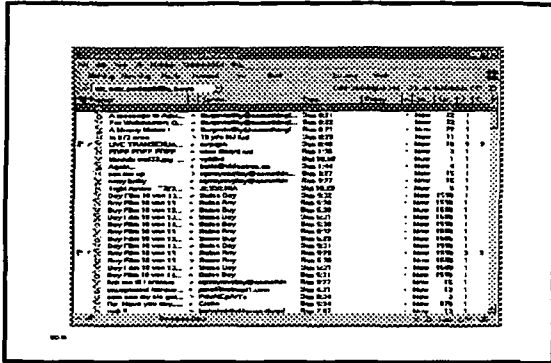
- alt.binaries.pictures.erotica.child.female
- alt.binaries.pictures.erotica.child.male
- alt.binaries.pictures.erotica.children
- alt.binaries.pictures.erotica.pre-teen
- alt.binaries.pictures.erotica.teen
- alt.binaries.pictures.erotica.teen.d
- alt.binaries.pictures.erotica.teen.female
- alt.binaries.pictures.erotica.teen.male
- alt.binaries.pictures.erotica.female.teen
- alt.binaries.pictures.nudism

And More....



- alt.sex.boys
- alt.sex.children
- alt.sex.preteens
- alt.sex.pedophilia
- alt.sex.pedophilia.boys
- alt.sex.pedophilia.girls
- alt.sex.pedophilia.pictures
- alt.sex.pedophilia.swaps





File Transfer Protocol (FTP)

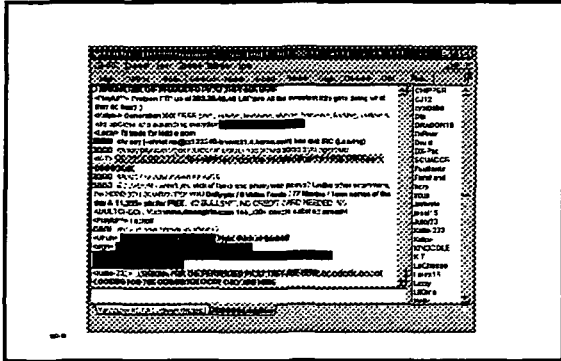
- **FTP** stands for *file transfer protocol*. It allows a user to move or transfer files from one Internet-connected computer to another
- A way for users to transfer files to and from a server or other user
- Allows the transfer of pictures to others or web server in a matter of seconds




IRC

- Internet relay chat
- Huge multi-user chat facility
- Number of major IRC servers around the world that are linked to each other
- Anyone can create a "channel" and anything typed on that channel is seen by everyone else on the channel
- Private channels can be created

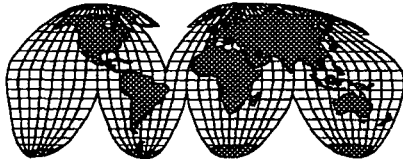




 **Chat Rooms**

- Similar to IRC
- Provided by commercial services, such as AOL
- Buddy lists and user profiles can be used to stalk children

World Wide Web



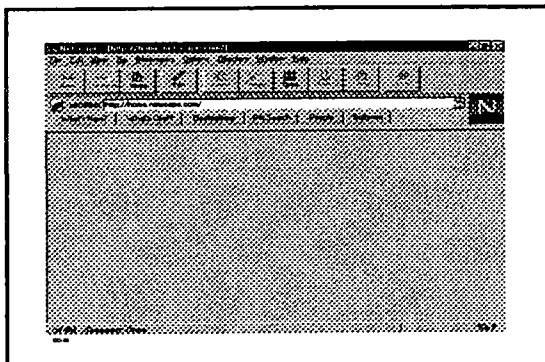
What is the World Wide Web?



The World Wide Web (WWW) is a global interactive, dynamic, cross platform, graphical hypertext information system that runs on the Internet.

What is a Web Browser?

- A Web Browser is special software such as Netscape Communicator or Internet Explorer which allows a user to view pages delivered from a Web Site situated at a particular URL on the World Wide Web.



What is a URL?

A URL or Uniform Resource Locator is a unique address for the location of any type of Internet resource. A typical World Wide Web URL looks like this:

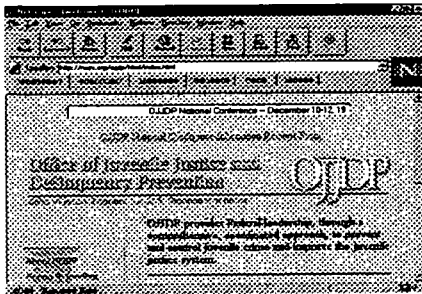
<http://www.ibm.com>

--

What is a Web Page?

A Web Page is a single document written in HTML (Hyper Text Mark-up Language) that includes the text of the document, its structure, any links to other documents and graphic images and other media.

--



--

What Is Available on the Web?

- Every type of organization, business, and enterprise has a web presence
- Many individuals have their own web sites
- Every digital resource imaginable is available
- There is too much information for anyone to comprehend

--

And on the Darkside

- Hundreds of thousands of sites dedicated to questionable or illegal activities
- Sex sites flourish
- It is simple and inexpensive for anyone to set up a web site in minutes and post child pornography
- WWW sites are advertised in Newgroups and IRC

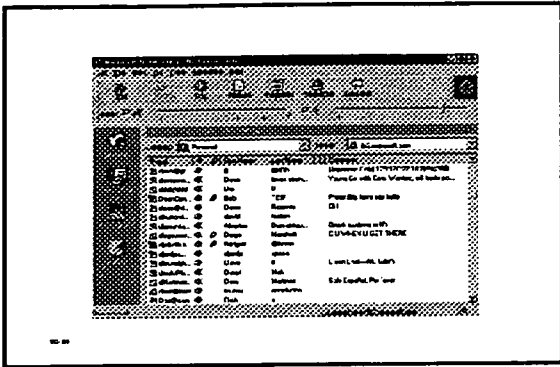
--

Growing Use of Internet Telephony and Video

- Netscape Conference
- Microsoft NetMeeting
- CU-See Me



--



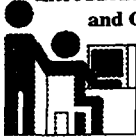


Summary

- Computer crime is a growth industry
- Computer hardware allows computers to process, input, display, store, and communicate data
- Computer software consists of operating systems, applications, and data files
- Networks are interconnected computers
- The Internet is the world's largest computer network
- Different Internet applications are used to exploit children

Protecting Children On-line
Unit Commander Course

**Introduction to Computer Technology
and Online Communications**





Unit Commander Responsibilities



**PROTECTING CHILDREN
ON-LINE
UNIT COMMANDER
RESPONSIBILITIES**

OJJDP/FVTC
Commander Bradley J. Russ

CC-Law 041, Slide 1

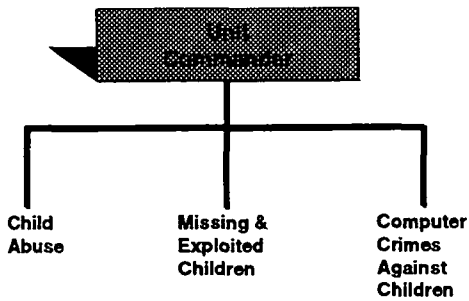
I. INTRODUCTION

In this class we will review:

- *Case Management and Supervision*
- *Program Management and Special Units*
- *Managing Multi-jurisdictional Investigations*
- *Providing Investigative Resources*
- *Community Education and Outreach Activities*

CC-Law 041, Slide 2

II. Organizational Structure



CC-Law 041, Slide 3

STATE POLICE

- Special Units and Agency Mission
- Does it enhance the existing philosophy?
- Purpose defined at outset of program
- Program vs. Special Unit mentality

RELATIONSHIP TO DEPARTMENT'S OVERALL MISSION

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

STATE POLICE

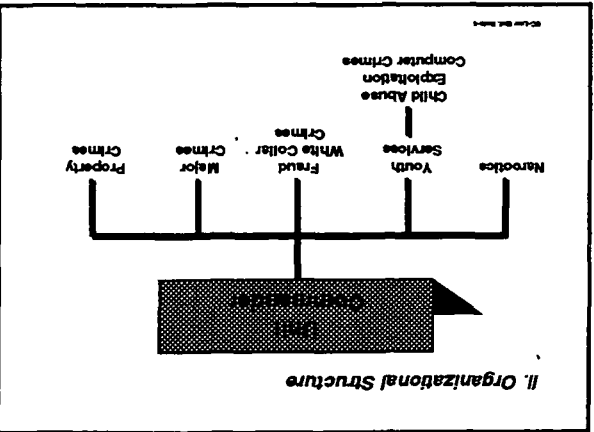
Statement of the Michigan State Department of Police

The Michigan State Department of Police is a public law enforcement agency, established by the Michigan State Police Act of 1961. The Department is responsible for the investigation and prosecution of crimes against the State of Michigan. The Department is also responsible for the training and supervision of police officers and the maintenance of law and order throughout the State.

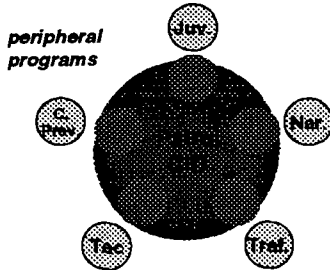
The Department is organized into several divisions, each with its own specific responsibilities. These divisions include the Criminal Division, the Traffic Division, the Community Relations Division, and the Training Division. Each division is headed by a division chief who reports to the Chief of Police.

The Department is also responsible for the coordination of law enforcement activities with other agencies, including the Michigan State Police, the Michigan State Sheriff's Department, and the Michigan State Police Reserve. The Department is also responsible for the coordination of law enforcement activities with local law enforcement agencies, including police departments and sheriff's offices.

The Department is committed to providing the highest quality of law enforcement services to the people of Michigan. We are dedicated to the protection of life, property, and the general welfare of the State. We are also committed to the promotion of community relations and the maintenance of law and order throughout the State.



SPECIAL UNIT STYLE OF POLICING



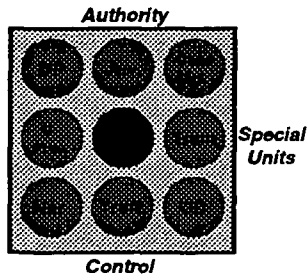
© Law 84, 84-12

SPECIAL UNIT STYLE OF POLICING (con't)

- *Functions pulled-out of the mainframe of the organization to receive special attention and visibility*
- *Special units or assignments are staffed by handpicked persons*
- *Special unit staff develop special access to top executives which produces problems in the chain of command*
- *Productivity and competency drop in the main body of the organization*
- *Special units begin to deliver the key services for the police agency, thus shielding its lack of effectiveness*
- *Special units are the first to go in cutback management—and the competency of the organization goes with them*

© Law 84, 84-12

PROGRAM MANAGEMENT STYLE OF POLICING



© Law 84, 84-12

PROGRAM MANAGEMENT STYLE OF POLICING (con't)

- *Departmentwide programs are established formally by general order*
- *Program management units are retained in the service delivery system*
- *The job of the program management unit is to coordinate program activities **horizontally** across the sub-divisions of the law enforcement organization*
- *The program management system is a means of balancing the need for **vertical** authority and control with the need for a **horizontal** coordination of programs across unit lines*


IC-Law 04L 0409-20

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS


INTEGRATION TO DIVISION'S GOALS & OBJECTIVES

- *Internal and External Needs Assessment*
- *Establish Priorities*
- *Where do you want to go?*
- *How are you going to get there?*
- *Who is responsible and by when?*

IC-Law 04L 0409-4



TEAM ACTION PLAN



Jurisdiction: _____
 Squad # _____

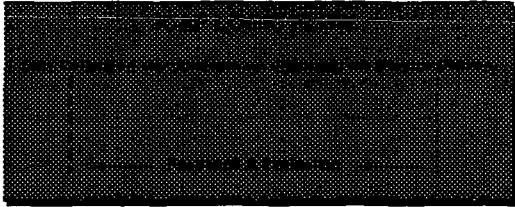
DATE	NAME	ASSIGNED	STATUS	COMPLETED	BY WHOM
	<ul style="list-style-type: none"> • Where are we going? • How are we going to get there? • Who is responsible? • By when? 				

Page 1 of 1

IC-Law 04L 0409-23

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

DEVELOPMENT OF PLANS & STRATEGIES FOR UNIT



IC-Law 04, 04b-7

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

- *Formalize through Policy & Procedure*
- *Integrate throughout Dept. Operations*
- *Oversight and the Control Process*
- *Manager vs. Investigator*
- *Intra-agency Coordination & Communication*
- *MOSS Units*

IC-Law 04, 04b-8

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

ESTABLISHMENT OF STANDARDS

- *System & Process of Controlling*
- *Establishment of Standards*
- *Performance Measures*
- *Correct Deviations*

IC-Law 04, 04b-9

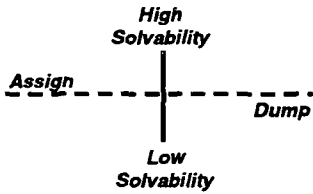
III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

CASE MANAGEMENT

● *Resolvability vs. Solvability*

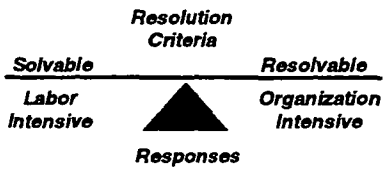
ICLAP 001 000-16

**CASE ASSIGNMENT
(Vertical Perspective)**



ICLAP 001 000-17

**CASE ASSIGNMENT
(Horizontal Perspective)**



ICLAP 001 000-18

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

CASE MANAGEMENT

- *Resolvability vs. Solvability*
- *Case Screening*
- *Case Assignment*
- *Monitoring Activities & Accountability*
- *Monkey Theory*

IC-Law 04, 828-8

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

CASE MANAGEMENT (con't)

- *Inter-agency Coordination*
- *Managing Multi-Jurisdictional Investigations*
- *Outside Assistance & Case Referral*
- *Case Closure & Quality Control*
- *Services to Victims*

IC-Law 04, 828-11

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

LIABILITY ISSUES

- *Seizure of Equipment*
- *Damage to Property*
- *Business Interruption*
- *Media Coverage/Damage to Reputation*
- *Training*

IC-Law 04, 828-12

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

BEST PRACTICES

- *Model Programs*
- *Model Policies & Procedures*
- *Investigative Protocols*
- *Student Examples*


IC-Law 04-000-01

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

COMMUNITY EDUCATION & OUTREACH

- *Public Service Announcements*
- *Community Relations & Crime Prevention*
- *PTO's & Civic Organizations*
- *High School & College Computer Classes*
- *Filters & Protective Software*
- *Resources (NCMEC, AOL, etc.)*

IC-Law 04-000-01




THE CYBER TIPLINE
FOR CHILDREN'S PROTECTION

For more information, visit our website at www.fbi.gov/ncmeclaw or call 1-800-843-5678.

The Cyber Tipline hotline is a free, 24-hour service for reporting the sexual exploitation of children.

- Child sexual abuse or exploitation
- Child pornography
- Child prostitution
- Child sex trafficking
- Child sex tourism

CLICK HERE

REPORT ONLINE

NCMEC, in partnership with the Federal Bureau of Investigation, U.S. Customs Service, and the U.S. Postal Inspection Service, serves as the national Cyber Tipline and is the national Child Pornography Tipline. 1-800-843-5678. Please contact us if you have information that helps us investigate child sexual exploitation.

The U.S. Congress has funded these resources for reporting child sexual exploitation.

IC-Law 04-000-01

Child Participation: School to Adult as well as at the Workplace

The Importance of Good Work: Self-Expression of Child Participation

Child participation has been defined as the child's active involvement in a range of activities that are relevant to their lives. This includes the child's own activities, as well as those of the community in which they live. The child's own activities are those that are directly related to their own interests and needs, while those of the community are those that are related to the child's role as a member of the community.

The Young Entrepreneurs of Children for Social Action

The growth of the Internet in recent years has created a new arena for children to express their views and opinions. There are many examples of children's websites, many of which have been developed by children. These websites provide a way for children to express their views on a wide range of issues, including social and environmental issues. This is a very important way for children to be heard, and it is also a way for them to learn about the world around them.

Child Participation

Child participation is a way of involving children in decisions that affect their lives. It is a way of giving children a voice in the decisions that are made about them. This is important because children are often affected by decisions that are made about them without their views being taken into account. Child participation is a way of ensuring that children's views are taken into account, and it is a way of giving children a sense of control over their own lives.

© Law Ltd, 2003

Child Site: Learning

The Internet is a very powerful learning tool. It provides a wide range of resources that can be used to support learning. This includes text, audio, video, and interactive resources. The Internet also provides a way for children to learn from each other. This is done through online discussion groups and chat rooms. The Internet is a very important tool for learning, and it is important that children are given the opportunity to use it.

Child Social: Education, Not to the World

The Internet is a very powerful learning tool. It provides a wide range of resources that can be used to support learning. This includes text, audio, video, and interactive resources. The Internet also provides a way for children to learn from each other. This is done through online discussion groups and chat rooms. The Internet is a very important tool for learning, and it is important that children are given the opportunity to use it.

© Law Ltd, 2003

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

BUSINESS PARTNERSHIPS

- **Equipment Donations**
- **Technology Assistance & Training**
- **Partnerships with Computer Stores**
- **College Campus Labs**

© Law Ltd, 2003

III. MANAGEMENT AND OVERSIGHT OF SPECIAL UNITS

MODEL LEGISLATION

- *New Mexico*
- *Florida*
- *Alabama*
- *Illinois*
- *Indiana*
- *New Hampshire*
- *North Carolina*
- *Oklahoma*
- *New Jersey*
- *Tennessee*

IC-Law Div. 8/84-94

January, 1993

Portsmouth Police Department

Mission

The Mission of the Portsmouth Police Department is to prevent crime, preserve order, and to protect the rights, lives and property of all people. We will work in partnership with our Community to identify and effectively respond to the diverse, ever-changing social and neighborhood problems and needs. We will do this with respect, fairness and compassion.

Beliefs

To accomplish our Mission, we are committed to the following Beliefs.

We believe...

- In fair, equitable, and impartial treatment for all.
- Our Community must be a part of the law enforcement and crime prevention process, and that with its active involvement, we will achieve our goals.
- The Police and the Community are accountable to each other.
- All people in our Community have a right to live in a safe, crime free environment.
- A harmonious and healthy work environment improves the quality of our services to the Community.
- Employee involvement in the creation of Department policy, procedures and objectives is essential to the attainment of our mutual goals, and the delivery of effective police services.
- Open and honest communication within our Department will promote an atmosphere of trust, cooperation and respect.
- Self-improvement is an individual responsibility.
- The Department must continuously provide for the development of personnel.
- That, in order to maintain the public's trust and support, we must hold ourselves to the highest ethical and professional standards.

William T. Burke
Chief of Police

MaryAnn N. Blanchard
Police Commissioner
January 1992 - December 1997

TEAM ACTION PLAN

Jurisdiction: _____

Goal # _____

TASK #	TASKS	AGENCY	BEGIN DATE	COMPLET. DATE	ISSUE #
	<ul style="list-style-type: none"> • Were are we going? • How are we going to get there? • Who is responsible? • By when? 				

The Law Enforcement Guide to OnLine Crime

- Types of On-Line Crime
- Where On-Line Crime Occurs
- How On-Line Crimes are Committed
- Key Questions to Ask
- Clues to Look For
- How to Follow Up

**Written by
John Spiropoulos**

Table of Contents

Section	Page
1. Tour of Cyberspace.....	1
2. The World Wide Web.....	2
3. UseNet Newsgroups.....	3
4. Internet Relay Chat.....	4
5. OnLine Service Providers.....	6
6. The Scenes of the Crime.....	7
7. The Chase Through Cyberspace.....	9
8. The Stolen Cyberspace Getaway Car.....	11
9. E-Mail Disguises.....	14
10. Information Available from Internet Service Providers.....	16
11. The Search Warrant Request.....	17
12. Seizing the Computer.....	18
13. Key Contacts & Phone Numbers.....	21
14. Glossary of Terms.....	22

Acknowledgements

I am a writer and former TV news reporter. (I went straight many years ago.) For the last four years I've done law enforcement training on technology issues. In order to put together a booklet that you would find truly useful in your everyday police work, I interviewed people who do this work everyday in local, state, and federal law enforcement agencies. Their names are listed below and I can't thank them enough for their contributions to this project.

Some people deserve special mention for assistance above and beyond the call of duty: Sgt. Toby Tyler, Detective Mike DeMitteo, Detective Mike Menz, and Investigator Mike McCartney. Finally, special thanks to Special Agent John MacKinnon.

Sgt. Toby Tyler, Crimes Against Children Detail, San Bernardino Sheriff's Office, San Bernardino, CA
Mike DiMatteo, Detective, San Bernardino Sheriff's Office.
Mike Menz, Detective, Sacramento, CA Hi-Tech Crimes Task Force
Don Hoyek, U.S. Customs Service
John MacKinnon, U.S. Customs Special Agent
Claude Davenport, U.S. Customs Service
Dennis Vaccro, Attorney General, State of New York
Eric Wenger, Assistant Attorney General, New York State
Mike McCartney, Internet Investigator, New York State Attorney General's Office
Peter Banks, Training Director, National Center for Missing and Exploited Children.
John Ryan, Assistant General Counsel, America OnLine
Don Calcoloug, Security Director, America-OnLine

Introduction

Criminals are more efficient than ever. They operate in the world of on-line computer communications — sometimes called cyberspace. More criminals now commit their crimes electronically — by going on line with a computer. It's quick. It's often easy. And they figure the police don't know enough to catch them. It's true that the crooks have a head start. But this booklet will help you catch up.

Chasing a crook through cyberspace isn't anything like the classic chase in the movie "The French Connection." That was all action. This is all details. You don't have to be a techno-nerd to catch a cyber-crook. You just have to do what you do every day:

- Ask the right questions.
- Understand what clues, leads, and evidence to look for.
- Collect and preserve the evidence.

With cyber-crime, you have new questions to ask, new clues to look for, and new rules about the collection and preservation of evidence. All are included in this booklet. With each type of cyber-crime discussed, there is a list of cyber-questions for you to ask the victim or complainant.

This is new material for many of you. So, there are new terms to learn. Each time a new word is introduced, we include a definition. In addition, all underlined words have a definition in the glossary at the back of the booklet.

Now for a legal disclaimer. This booklet is intended as an educational resource. It is not intended and should not be relied on for legal advice. Your actions should comply with the laws of your jurisdiction as well as your department's policies, procedures, and legal guidance.

In addition, this booklet is designed to raise your awareness, knowledge, and ability to effectively react to and follow up on an on-line crime. The lessons learned will make you a better, more effective, and more successful law enforcement officer.

But this booklet does not do several things. It does not make you a computer expert. It does not make you a computer forensics specialist. It does not prepare you to work proactively in the on-line world where undercover officers patrol the internet looking for criminals. Those lines of work require specialized training. If you're interested, go for it. That's where the future of law enforcement lays. That future is now. And right now, there's a shortage of law enforcement officers who have the skills to do the job.

1. A Tour of Cyberspace

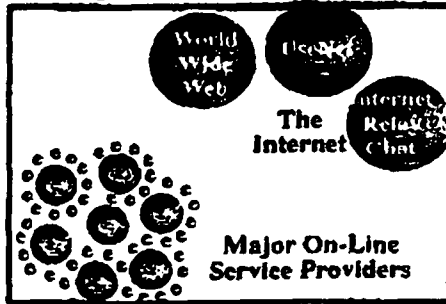
There are tens of thousands of places to visit in Cyberspace — just as there are in a city. You need a map to find your way around a city and you need a map in Cyberspace too. The map below depicts the major "planets" or "neighborhoods" in Cyberspace. Crime may occur in any one of them.

Neighborhoods of Cyberspace

The Internet is the largest neighborhood in Cyberspace.

It has three distinct subdivisions.

Each part of the Internet performs a specific function.



World Wide Web

The World Wide Web consists of thousands of "electronic storefronts" set up by businesses, organizations, government agencies and individuals. The "Web" is a source for news and information as well as a marketplace where you can purchase goods and services.

UseNet (Newsgroups)

Newsgroups are similar to a bulletin board at an office where you can read what's been posted and post something yourself. There are thousands of UseNet newsgroups devoted to a wide variety of subject.

Internet Relay Chat

Internet Relay Chat consists of thousands of electronic chatrooms where you can "talk" to another person or to a group by typing on your keyboard.

Internet-Only Connections

Most people connect to the Internet through an Internet Service Provider (ISP). Some ISPs merely link you to the Internet. You connect to the ISP which then connects you to the Internet.

Internet Connections Plus Other On-Line Services

Some ISPs are also "On-Line Service Providers." They offer a connection to the Internet as well as other on-line services available to their members only. These additional on-line services are similar to what is available on the Internet. They include news and information, on-line shopping, bulletin or message boards, and chatrooms.

Major On-Line Service Providers

- America OnLine
- AT&T WorldNet
- CompuServe
- Microsoft
- Netcom
- Prodigy

2. The World Wide Web

The World Wide Web is where organizations set up Web sites — think of them as electronic storefronts in cyberspace. The "Web" is a place where you can get the latest news or buy a wide variety of products and services. You can also tap into a vast library of information stored on millions of computers around the world.

Web sites may be a combination of graphics, still pictures, videos, and sounds. The web site for the U.S. Customs Service is shown below. Each web site has an internet address. It's called a Uniform Resource Locator (URL). The web site address is listed here.

See closeup view
of the URL.



Address: <http://www.oustoms.ustreas.gov/>

Criminal Use: Web Site Scams

Sometimes Web sites vanish overnight. Here's what happens. Criminals set up a web site, collect money or identification information, and then "erase" the web site. It can disappear at a moment's notice. Here's how consumers get ripped off:

- A con artist sets up a web site to sell products at very low prices — prices too good to be true. The consumer may pay \$200 for an item that usually sells for much more. However, what the consumer receives is an item worth as little as \$20.
- Criminals also set up web sites to collect credit card numbers and other personal information from customers who believe they're buying a product or service. In reality, nothing is ever delivered. The criminal then sells the stolen information to other criminals or uses it for his own illegal purposes.

Cyber Questions to Ask In Web Site Crimes

You have a variety of questions to ask at any crime scene. When you have a case involving a web site, here are the additional cyber-questions to ask:

- What is the address of the Web site? A Web site address is called the Uniform Resource Locator or URL. It may read www.crimesrus.com or it could be just a series of numbers: 207.262.64.8.
- When did the complainant contact the web site?

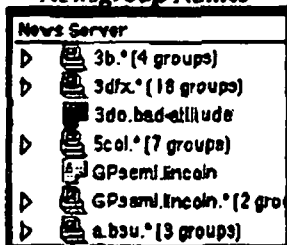
3. UseNet (Newsgroups)

Another major subdivision of the Internet is called Usenet. It's made up of Newsgroups. Think of newsgroups as bulletin boards like the one at your precinct or office. You drop by, read what's on it, and maybe add your own comments or articles.

In Cyberspace, there are thousands of newsgroups with postings on just about any activity you can imagine, some of it illegal. If you want to keep a copy of something, you download it to your computer. If you have an article or comment you want to post, you upload it to the newsgroup.

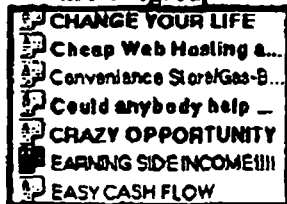
List of Newsgroup Names

The box to the right shows how a list of newsgroups appears on my computer screen. This is just a few of the thousands of newsgroups I can "read." The newsgroup's name often gives you an idea of the subject matter. However, many names are mysterious. I "clicked" on one titled: 3do.bad-attitude.



Postings in Newsgroup

What appeared next was a list of the titles of dozens of postings, some of which appear in the box to the right. When I "clicked" on Earning Side Income, I discovered it was nothing more than the usual chain letter scam.



Criminal Use

- There are newsgroups dedicated to the collection and dissemination of child pornography.
- Thieves also use Newsgroups to advertise stolen products for sale.
- Some newsgroups are collections of traditional consumer scams such as Ponzi schemes and chain letters.

Cyber Questions to Ask in Newsgroup Crimes

You have a variety of questions to ask at any crime scene. When you have a case involving a Newsgroup, here are the additional cyber-questions to ask:

- What is the name of the newsgroup?
- What is the title of the posting?
- Who sent the posting?
- What is their E-mail address
- What is the message ID on the posting?

4. Internet Relay Chat

Internet Relay Chat (IRC) is another major part of the Internet. This is where people "chat" — not by speaking — but by typing the words on the keyboard. Here are the basics:

These chats take place via a server. A server is a computer which "serves" up information, just as a waiter serves up food. There are dozens of IRC servers offering thousands of channels of chat. Let's look at the one that's highlighted.

IRC Server Listings

```
washington-1.dc.us.undernet.org
washington-r.dc.us.undernet.org
Chicago.IL.US.Undernet.org
Chicago-R.IL.US.Undernet.org
lowell.ma.us.undernet.org
Baltimore.MD.US.Undernet.org
```

Channel Listings

When you select a server, you then get a choice of channels. A few are shown to the right. Let's click on bbw, whose full title is Big Beautiful Women.

```
184 #gaysexefr
185 #bbw
186 #winnuke
187 #scabs
188 #canada
```

When you enter a chat channel, different "windows" on your computer screen provide information. One window shows the "Chat Dialogue." (See Chat Dialogue box below) Another window contains the the "Users List" with all of the nicknames of the people on the channel. (See Users List box below)

Chat Dialogue

```
softly: hello
softly: :)))))))))
Rhapsody : softly!!!! *hugs*
LdyCharle looks at snuggly, better not leave
bruise or my husband might suspect something ;)
softly: Rhapsody hi:)))
LdyCharle: hi softly
Snuggler: bruise? me... never...
LADYmte: hehehe
LdyCharle: *piggie*
```

The Chat Dialogue window shows Softly, Rhapsody, Ldy Charle and Snuggler "chatting" to the whole group. In a chat-room you can choose to talk to everyone or have a private chat with just one person. You can identify who is in the chatroom by looking at the Users List which shows who is in the room at that moment. Here is a sample of the information provided.

Users List

```
silktongu      silktongu@slip129-87-208-48.ch.
Snuggler      kaici@pm3bky1-66-88.intrepid.net
softly        leaf@d0-0-236.ann-arbor-avis.dia
ster69        user@host100.209-113-209.gis.ne
```

The Users List shows the person's nickname on the left and their Internet Protocol Address on the right. Both are key pieces of information that are needed to trace anyone in Internet Relay Chat. Internet Protocol Addresses and traces are discussed on Pages _____

Key Information to Collect: Example

There are thousands of IRC-channels discussing specific subjects — music, sports, politics, sex, you name it. If a crime occurs, it's going to be very difficult to investigate the case unless you collect specific information. Let's assume a citizen reports a crime occurred in the chat channel discussed on the previous page. Here are the key questions and answers that investigators would need to work the case.

Q. What is the name of the channel?

A. bbw

Q. What server is the channel on?

A. Baltimore.MD.US.Undernet.Org

Q. What was the nickname used by the offender?

A. Snuggler

Q. What is his Internet Protocol Address?

A. kaici@pm3bky1-66-88.intrepid.net

Q. What time of day did the communication occur?

A. 3:45pm central standard time

Q. How do you know that for sure?

A. The time is listed on my computer screen.

Criminal Use

- Pedophiles meet in some chatrooms to discuss their sexual exploits.
- Pedophiles often trade child pornography pictures via E-mail with an attached file.
- Pedophiles and other sexual predators also visit chatrooms catering to children and teenagers. They start communicating with them. After engaging children and teenagers in conversation — sometimes over a period of days, weeks, or months — they'll try to lure them into a real world sexual relationship — off line.
- Fraudsters work in chatrooms developing relationships, looking for someone who will fall for their get-rich-quick schemes and phony business "opportunities."
- Criminals sometimes hold their "meetings" with co-conspirators on IRC channels where they can communicate person to person. No one else "sees" what they say to one another. It's a method of communication which avoids wiretaps.

Cyber Questions to Ask

You have a variety of questions to ask at any crime scene. When you have a case involving Internet Relay Chat, here are the additional cyber-questions to ask:

- What is the name of the channel?
- What server is the channel on?
- If the complaint is about a specific person, what "nickname" or "screen name" did that person use?
- Did you note the person's Internet Protocol Address next to their name?
- Did you save a copy of what was said on the screen?
- Do you have a printout of what was said?
- Do you know exactly what time the communication occurred?

5. On Line Service Providers

Internet Service Providers connect most people to the Internet. Some ISPs, known as "Online Service Providers," offer more than just a connection to the Internet. They offer their members a variety of added on-line services which are similar to what is available on the Internet.

Major On-Line Service Providers

- America OnLine
- AT&T WorldNet
- CompuServe
- Microsoft
- Netcom
- Prodigy

Services Available from On-Line Service Providers

- On-line shopping
- News and Information
- Research
- Message boards (Similar to Internet Newsgroups)
- Chatrooms (Similar to Internet Relay Chat Channels)

Criminal Use

- Pedophiles and sexual predators sometimes lurk in chatrooms to identify and communicate with children and teenagers with the purpose of luring them off-line.
- Con artists use message boards to promote get-rich-quick schemes and other fraudulent activities.
- Criminals sometimes market their fraudulent scams through electronic mail. This unsolicited "junk" E-mail mail is called SPAM. And the technique of sending E-mail messages to thousands of consumers is called Spammimg.

Cyber-Questions to Ask: E-Mail

- What is the name of the Internet Service Provider?
- If the complaint involves E-mail, does the complainant's computer still contain the E-mail?
- What is the offender's screen name?
- What is the offender's E-mail address?

Cyber-Questions to Ask: Message Boards

- What is the name of the message board?
Note: There are tens of thousands of message boards. An Internet Service Provider needs to know more than the name of the message board to locate it.
- Does the complainant know the path he or she took to get to that message board?
- If not, can he or she try to go through the steps that brought them to that message board?

Cyber-Questions to Ask: Chatrooms

- What is the name of the chatroom?
- Where is it located within the ISP's services?
- Does the complainant know the path he or she took to get to that chatroom?
- If not, can he or she try to go through the steps that brought them to that message board?

6. The Scenes of the Crime

Since online crime is committed via computer, there are two scenes of the crime: both the victim's computer as well as the criminal's computer. So, there may be evidence in each computer. In addition, there's a trail of evidence between the two computers. That trail of evidence is kept in the records of the Internet Service Provider — the victim's ISP, the criminal's ISP, or both. The availability of ISP records and the legal procedures required to get it are discussed on page _____.

Location of the Evidence

- The Victim's Computer or Storage Device(s)
- The Victim's Internet Service Provider Records
- The Criminal's Internet Service Provider Records
- The Criminal's Computer or Storage Device(s)

Ask the Right Questions

Many types of crime have an online connection, but it's not always obvious. So, ask, Does the victim have a computer? Does he or she go online? This is critically important when you have a missing person — whether it's a child, teen, or adult.

Get Expert Help Fast

If someone's personal safety may be in danger, quickly call a computer specialist for assistance.

Why You Need Help

Key clues and leads may be in the computer. (See case example in box to the right) A computer forensics specialist can ensure that critical evidence isn't inadvertently destroyed.

Warning:

An everyday working knowledge of computers doesn't qualify anyone to tamper with a computer at a crime scene — except under extreme circumstances. The retrieval and preservation of evidence is a specialized skill.

Solving the Case of the Missing 15-Year Old Girl

A 15-year old California girl runs away from home, leaving her parents a message that she's run away with Paul. The parents don't know who he is. They call the police.

The police respond and one of their questions is, "Does she talk on the Internet?" The parents say she talks on the Internet every night. So they call the daughter's best friend who says, "Oh, yeah, Paul is someone she met on the Internet. Knowing that, the officer calls in the Sacramento Hi-Tech Crimes Task Force.

A computer specialist from the task force looks through the computer files. He finds no clues as to who Paul is or where he lives. Then he uses a special computer program to retrieve files which the girl had deleted. Within minutes he finds a message from Paul. The message includes his full name and address. And within 24-hours, by tracing Paul's license plate, they find the girl and Paul, a 26-year old man.

Cyber Fact-Finding at the Scene of the Crime

You know how to respond to a crime scene based on your training and experience. So you know the questions to ask when it comes to identifying a victim, a perpetrator, and the importance of preserving evidence at the scene of the crime. Because computers are often now involved in crimes, here are additional cyber-questions to consider.

- Is a computer involved?
- Is there an on-line connection?
- Get a computer specialist involved as soon as possible, if someone's physical safety is in jeopardy.
- Who is the victim's Internet Service Provider?

Location of the Crime

When a complainant says the crime "happened on the Internet, that's like telling a New York City policeman that the crime occurred somewhere in New York. Which part of New York? Do you have an intersection? Do you have a street address? Below you'll find a similar line of "location questions" involving on-line crimes. Also listed are the page numbers for the specific cyber-questions for different parts of cyberspace which were covered in earlier sections.

- Where in Cyberspace did the on-line crime occur?
- Did it occur on the Internet or at an on-line service provider like America OnLine, AT&T Worldnet, Microsoft, and others.
- If the Internet was involved, which part of the Internet?
 - ✓ World Wide Web site? See page _ for web site questions.
 - ✓ Internet Newsgroup? See page _ for newsgroup questions.
 - ✓ Internet Relay Chat? See page _ for IRC questions.
- If the crime involves a service offered by an on-line service provider, what is the name of the On-Line Service Provider?
- What on-line service is involved?
 - ✓ A Message Board? See page _ for message board questions.
 - ✓ Chat Room? See page _ for chat room questions.

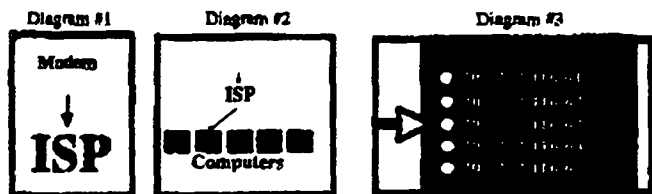
Other Questions to Ask and Clues to Look For

- Are there any printouts of E-mail messages?
- Are there any computer files of E-mail messages?
- Are there saved computer files or printed copies of chatroom conversations?
- Are there saved computer files or printed copies of materials downloaded from a newsgroup or web site?
- Is an unfamiliar E-mail address been discovered in the case of a missing person?

7. The Chase Through Cyberspace

If a crook uses his real E-mail address, it's easy to trace a crime to a specific account. Frequently, crooks spoof (falsify) their E-mail address. Then you try to find them through the Internet Protocol Address (IP address) that was used. The IP address looks like gobbledygook — numbers, letters and other keyboard characters. Not to worry. It's not your job to analyze it. *Just collect it accurately and get it to the Internet Service Provider.* The ISP will analyze it and do the trace (when issued a subpoena). Here's how the system works. In order for you to go on line:

- Your modem has to dial into a phone number at an Internet Service Provider. Diagram #1.
- When the call reaches the ISP, it is assigned to one of the ISP's computers. Diagram #2
- The call is then assigned to a specific port of entry on that computer. Diagram #3.
- Each port has a number. (Diagram #3) That number is the Internet Protocol Address for all activity that occurs on the account during that one specific "call" or, on-line session



- An IP address is contained in each Internet communication.
- Each Internet Service Provider is assigned a specific set of Internet Protocol Addresses.
- Only one customer account can use a specific IP address at any given date and time.
- The ISP has a minute-to-minute record of each IP address and which customer account used it.
- When provided with the Internet Protocol Address as well as the date and time of the communication, the ISP can identify the specific account which was used to commit the crime.

Example:

In the diagrams above, someone went on line and was assigned to IP address #295.252.116.63. While on line, that person was involved in fraudulent activity.

The citizen who was bilked reported the crime and showed investigators the scheme as it appeared on his computer. The communication he received from the crook shows it was sent at 3:55pm EST on March 1, 1998. The Internet Protocol Address was #295.252.116.63.

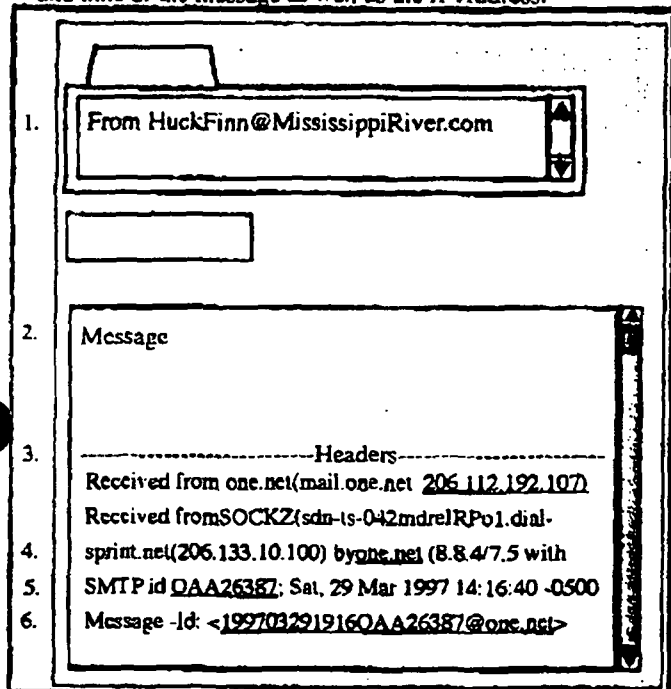
Investigators provide a copy of the communication to the Internet Service Provider who will, when issued a subpoena, identify which customer account was used to commit the crime.

Note: Each time a computer user connects to an ISP, the user may be assigned a different IP address. So, you could be investigating four frauds, involving four IP addresses, but when the ISP traces all of them, they lead to the same account.

The IP Address on an E-Mail Document

Someone commits a crime using the E-mail address of: HuckFinn@MississippiRiver.com. Obviously, it's a phony E-mail address. So we'll take a closer look at the E-mail.

- Item #1 shows the E-mail address
- Item #2 shows where the message goes.
- Item #3 in the "Headers." Though they are called "headers," they are not at the head of the document, they are at the bottom. The headers identify the specific internet computers that the message was routed through. The computer found at the top of the list (206.112.192.107) is the last computer the message passed through before reaching the recipient. Work your way down the list. The computer at the bottom of the list is the one that originated the message.
- Item #4 shows the name of the Internet Service Provider of the originating computer (see underline)
- Item #5 shows The Internet Protocol Address (see underline) of the originating computer.
- Item #6 shows the Message Id which includes both the date and time of the message as well as the IP Address.



Your job is to get all the header information and supply it to the ISP in order to do the trace. When the ISP identifies the account, does that mean the account-holder committed the crime? No. As we'll explain in the next section, the customer's account may have been stolen and used to commit the crime.

8. The Stolen Cyberspace Getaway Car

On the street, criminals use stolen cars to commit crimes and make their getaway. In Cyberspace, criminals use an online version of a getaway car. Here's how. When I go online, I enter a secret password known to me and my internet service provider. But sometimes passwords are stolen. If a criminal steals my password, he goes online using my account to commit his crime. It's a way to avoid being traced. In fact, the evidence points to my account. But I'm innocent. There are three ways criminals can get a Cyberspace getaway car.

Getaway #1: The Stolen Password (Trojan Horse)

A crook E-mails you something enticing. In one case it was an offer of a miracle weight reduction plan. The E-mail says "Just click the line below." When you do, the E-mail secretly infiltrates your computer and installs a secret computer program on it. Later, that program steals your password and E-mails it back to the crook. This technique is called a Trojan Horse — based on Greek Mythology. It's the legend of a huge wooden horse. It was presented as a gift to an enemy but was secretly filled with soldiers who later infiltrated the enemy city.

Getaway #2: The Password Scam (Password Solicitation)

A criminal sends you an E-mail claiming he's from your Internet Service Provider's billing department. The E-mail reads, "We've had a computer problem Send us your screen name and password as soon as possible or you won't be able to access your account." With that information, the criminal now has the opportunity to access your account and commit crimes with your account.

Getaway #3: Identity Theft

A criminal sends you E-mail asking for name, address, and credit card number. He may claim he's from the billing department at your Internet Service Provider. The E-mail looks like it's from the ISP. In one case, it even had the company president's picture on it. Once a criminal has the information he applies for and gets on-line accounts with several Internet Service Providers. He uses those accounts to commit crimes. When law enforcement traces the crime, the IP address and the E-mail mail point to an innocent person, not the criminal.

Leading You in the Wrong Direction

When criminals use any of the "Getaways" they're trying to lead you in the wrong direction. Much, if not all, of the cyber-evidence (the E-mail addresses and IP addresses used) will lead you to an innocent person. That's why simply identifying which account was used to commit a crime does not provide you with probable cause to get a search or arrest warrant for the name and address on that account. You'll need to do more investigating to determine if there is a link between the account holder (or other members of the household) with the criminal activity that was committed with that account.

Continuing Your Investigation

There are several methods to pursue to determine whether anyone in the household may be connected to the criminal activity that occurred with the account.

Where Did Account Sign On?

- When the crime was committed, where did the account sign on to the Internet Service Provider's network? Was it from the account holder's home, place of work, or from another location?

The Internet Service Provider can provide records showing where an account entered its network each time the account logged on.

If an American Online account holder is based in Maryland but records show the account signed on in Chicago, that could indicate unauthorized use of the account.

Or it may indicate the legitimate user was out-of-town when he used it. Or it could simply be a relative using the account.

So while out of town usage may be a clue, still more checks are needed.

- Check how many people live at the account holder's address.
- Check how many vehicles are registered to that address.
- Who is receiving mail at that address?
- In whose name are the utilities registered?
- Actual physical surveillance.
- Check phone records.
- Determine if phone company has records for local calls made. Those records may show that the household dialed into the Internet Service Provider service. They may also show that the household dialed into the ISP at the very times that the crimes were committed on line. That's not proof that someone in the household used the account to commit the crime, but it is an indicator to be weighed with all other information.
- If such local phone records do not exist, get a court order to install a Pen Register on the telephone lines for that address. The Pen register provides you with all of the dialed digits by the phones in the household and the duration of each call. That information allows you to determine whether a call was made to an Internet Service Provider.
- Make pre-text calls to the household of the suspect account. Some investigators pose as telemarketers to gain valuable information. They sometimes pose as someone doing a survey and ask questions such as:
 - ✓Do you have a computer? What kind?
 - ✓Do you have Internet Service? Which one?
 - ✓Who in your household has access to that service?
 - ✓How often do you go on line?
 - ✓How long do you stay on line?
 - ✓How often do other members of the household go on line?
 - ✓How long do they stay on line?
 - ✓What kinds of computer software do you use?
 - ✓Do you ever use the account while away from home?
 - ✓Do you allow friends, relatives, or associates to use your account?

Reaching a Conclusion

When you complete your investigation, you'll determine whether you have probable cause for search and/or arrest warrants.

- In some cases you will have probable cause to seek warrants for the account holder or another person at the address for the account.
- In some cases, the evidence indicates that the account holder isn't involved. You conclude that someone else committed the crime using the legitimate customer's account as the get-away car. (See box below)
- If the account holder or someone in the household didn't commit the crime, who did? Was an ID stolen? Was the password stolen? Did the account holder give someone else permission to use the account? In cases of fraud where there was the payment of money or the delivery of goods, you may be able to trace them to the criminal. (See Investigating Fraud cases below.)

Example of an Innocent Account Holder

Investigators hot on the trail of an Internet crime, trace it to the name of a prominent person in New York City. At first glance, it looks like a scandal in the making. Closer investigation, however, reveals that all of the suspicious activity is occurring in Texas. Further investigation reveals that the New York city resident had been to Texas and had lost his wallet there. Someone later used his identification to open an account with an Internet Service Provider and then committed crimes with that account.

Investigating Fraud Cases

Criminals who commit fraud may use number of methods to throw you off their trail. Once you've discovered that the legitimate account holder is not involved, there are other paths to

- **Cases Involving the Payment of Funds**
One way or another the money has to be delivered to the crook somewhere, somehow. So, follow the money. It may have been sent to a physical address or a PO Box that's traceable. Or it may have been wired to a bank account which you can subpoena the records for.
- **Cases Involving the Purchase of Goods**
Where you have the purchase of goods with stolen credit cards, trace the shipment. You may find the crook at the receiving end of the delivery.

9. E-Mail Disguises

Criminals try to avoid detection by disguising their true E-mail identity. Sometimes they'll send E-mail anonymously. Often, they'll simply spoof (falsify) their E-mail address.

E-Mail Disguise #1: Sending Mail Anonymously

Anyone can send an E-mail message anonymously by using the services of what's called an "anonymous remailer." Here's how:

- First, the sender E-mails his message to the remailer with instructions on where it should be sent.
- Next, the remailer removes the sender's address and replaces it with its own address.
- Then, the remailer *re-mails* the message to its final destination.

Example

```
From: JNS@anonymousmail.com
To: BCClinton@Whitelouse.Org
```

There are a variety of occasions when it's appropriate to use an anonymous remailer (See box below.) But criminals also use them to hide their identity.

- In some cases, the police have subpoenaed records of an anonymous remailer, learned their true E-mail address, and successfully tracked down a criminal.
- Some remailers don't keep records for very long, if at all. So, it's not always possible to trace the criminal.

Anonymous Remailers

Anonymous remailers have a legitimate purpose. For example, someone who takes part in an Internet support group for drug abuse, alcoholism or some other disease may want to remain anonymous. Law enforcement also may use such anonymous remailers when conducting undercover activity.

E-mail Disguise #2: The Bogus E-Mail address

The E-mail below shows it was sent by lovemoney at AOL.com. If you send a subpoena to AOL to find out who lovemoney is, AOL will tell you it has no such account. As explained on page ____, you can identify the account by looking in the headers for the Internet Service Provider, the Internet Address, and the Message ID.

- The headers show that the message came from an ISP named Erols.
- Send a subpoena and the header information to Erols.
- It will trace the E-mail to a specific account and provide you with the account holder's name, address, and phone number.

```
From: lovemoney@aol.com
```

-----Headers-----

Received from...

Message ID: xxx2942987@erols.com

Once the account is identified, continue your investigation to determine whether the account holder is linked to the criminal activity that took place on the account.

E-Mail Disguise #3.

Sometimes when citizens complain about an E-mail they receive, there is a discrepancy between the actual E-mail address and the address that is reported. This occurs when the letters on the screen aren't what they appear to be. For example:

- What looks like the letter "O" may really be a 0 (zero).
- What looks like an uppercase "I" may really be a lower case letter "l" or the number "1" (one).

Take a look at the suspect E-mail address below.

Actual
E-Mail Address

From: l0vem0ney@aol.com

A citizen reporting the above E-mail crime could easily mis-read it and report that it came from lovemoney at aol.com.

Reported
E-Mail Address

From: lovemoney@aol.com

You send a subpoena to America OnLine for information on that account. AOL says it has no such account. Here's how to avoid a blind alley like this:

- Ask the complainant to take a closer look at the E-mail. Or take a closer look at it yourself.
- Does the address contain letters that can be misinterpreted?
- It may be possible to determine the true address by carefully analyzing what each letter or number is.
- In some cases, it may be necessary to convert the letters to a different typeface (This can be done by using the computer's copy and paste function and a word processing program.)
- The true E-mail address in this case is:

1(one) 0(zero) vem 0(zero) ney@aol.com

Now that the true E-mail address has been deciphered, send AOL a subpoena for information on that account. Then continue your investigation to determine whether the account holder is linked to the criminal activity that took place on the account.

E-Mail Disguise #4

This is a variation of Disguise #3. Here's the E-mail address.

Actual
E-Mail Address

From: l0vem0ney@aol.com

Once again, a citizen mis-reads it and reports that it came from lovemoney at aol.com.

Reported
E-Mail Address

From: lovemoney@aol.com

Here's the problem. In this case AOL has a legitimate account with an e-mail address of "lovemoney." You send a subpoena AOL to get account information for "lovemoney." AOL provides you with the name, address, and phone number. After days or weeks, you'll discover that you're investigating the wrong account. To avoid going down this blind alley, make sure you get the correct E-mail address. To do that, use the steps that were explained above in E-Mail Disguise #3.

10. Information Available from Internet Service Providers

A federal law, the Electronic Communications Privacy Act, ECPA, sets the legal procedures for obtaining information from Internet Service Providers. ECPA governs:

- What information you may get
- What legal document is required

Category of Information	Type of Information Needed	Legal Document Required
Subscriber Information	<ul style="list-style-type: none"> • Name • Address • Phone Number • Billing records 	<i>Subpoena</i>
Transactional Information	<ul style="list-style-type: none"> • Log on & off times/dates • Credit Card Number • Web sites visited • Names of senders and recipients of user's E-mail 	<i>Court Order</i> Under ECPA the court order for transactional records is called an "articulable facts" order
Content Information	<ul style="list-style-type: none"> • Electronic Mail messages sent and received 	<i>Search Warrant</i>

You also need a subpoena have an ISP trace which account used a specific Internet Protocol Address (IP Address) at a specific time and date. IP Address traces are discussed on page

Working with out-of-state Internet Service Providers

Online crime cases pose jurisdictional issues for state and local police when they involve an out-of-state Internet Service Provider. When the ISP is out-of-state, funnel your legal requests through a law enforcement agency in the ISP's jurisdiction. The Internet Service Provider can tell you which local agency to work with.

The Evaporation of Evidence

Internet Service Providers don't keep all records permanently. Much is erased in a matter of days or weeks, depending on the company's policy. So, you must act quickly before potential evidence evaporates. The types of records which are kept temporarily are listed in the box to the right.

ISP Records Which Are Kept on Temporary Basis
<ul style="list-style-type: none"> • Log on and log off times • IP addresses which were used • E-mail sent or received.

11. Search Warrant Request

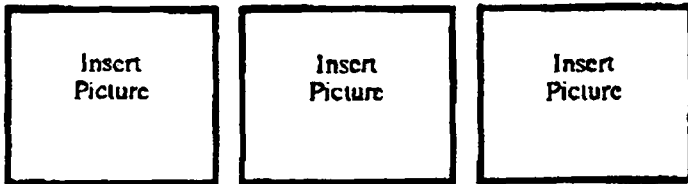
Your search warrant request must comply with the Electronic Communications Privacy Act (ECPA). Your search warrant application request should include the computer as well as all types of media that could record computer evidence. In your affidavit you must articulate probable cause as to specifically what you want to seize and why you want to seize them.

The evidence may be in the computer or it may be electronically stored on a variety of mobile media—disks, cartridges, tapes.

The search warrant authority should also include the seizure of computer manuals. The manuals are helpful if your forensic investigator encounters unfamiliar hardware or software.

Items to Include in Search Warrant Request

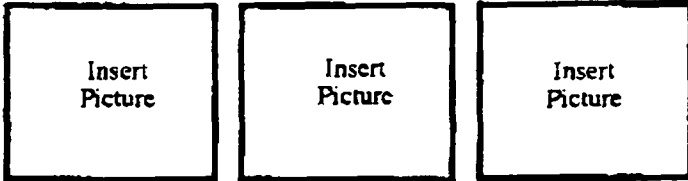
- Computers
- Monitors
- Keyboards,
- External Storage Devices
- Disks, Cartridges, Tapes
- Modem,
- Printer
- Manuals
- Software



Computer and Manuals

Monitor and Keyboard

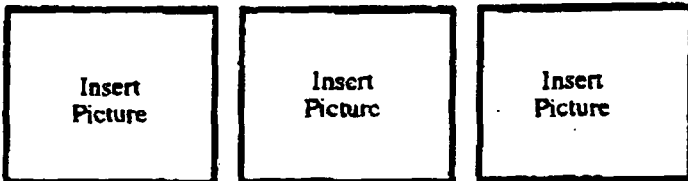
Software and Manuals



Zip Drive and Disks

Jazz Drive and Disks

Tape Drive and Disks



Floppy Disks

Modem

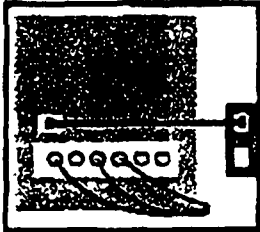
Printer

12. Seizing the Computer

How you seize a computer depends a great deal on whether the computer is connected to other computers. In most home situations, you're dealing with a typical home computer that is a stand-alone — it's not connected to other computers. Businesses, on the other hand, frequently have a number of computers connected to one another in a network. Here's guidance for you to consider, depending on the situation you're facing.

Seizing a Stand-Alone Home Computer in a Residence

- Officer safety is first and foremost. Don't assume the suspect is a passive computer geek. He may be armed, harboring a fugitive, or trafficking in drugs.
- Isolate the computer.
- If the computer is "off," don't turn it on.
- If the computer is "on," don't touch it.
- If the computer is on and someone is at the keyboard, remove them immediately because it's possible, with a few strokes on the keyboard or clicks on the mouse, to quickly alter or destroy evidence in the computer.
- Take a photograph of the screen
- Pull the plug from the back of the computer — *not* from the wall outlet. (see below)



Where to Pull the Plug

The computer system may have an uninterruptible power supply.

If you pull the plug from the wall outlet, the power supply unit thinks the power has been cutoff. It may then start a program that shuts down the computer and possibly destroy evidence or change files.

To avoid this possibility, pull the plug from the back of the computer.

-Claude Davenport,
Computer Forensics Trainer
U.S. Customs Service

- Place an *unformatted* disk into the disk drive. If there is more than one disk drive, put an *unformatted* disk into each one.
- This will prevent the computer from "**booting up**" in case someone inadvertently tries to turn on the computer.
- If someone were to turn on the computer, the booting up process often manipulates files. That could give the defense an argument that law enforcement tampered with the computer after it was seized.

Seizing Networked Computers or Computers at a Business

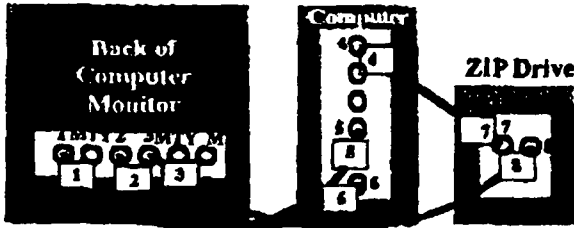
Don't pull the plug on a computer at a business. Instead, try to identify — *in advance of executing a search warrant* — the types of computers and systems involved. Then, when you execute the warrant, bring along a computer forensics specialist who is familiar with those systems and would know how to either get the information needed or know how to turn the system off. Here's why you need extra help with a business situation.

- The computer may be a UNIX system or a computer that is part of a larger network of computers. That network may include computers in other rooms of the building, or other buildings in your area, even computers in other cities. Pulling the plug would, in many cases, severely damage the system.
- The computer contains information that's important to the business. So, seizing it may be inappropriate and may make it impossible for the business to function.

Tagging and Bagging

This is the term often used for the process of seizing a computer and preparing it for storage in the evidence room or wherever seized computers are kept. Proper tagging and bagging is necessary to not only preserve the evidence but to be able to take all the pieces into court, put them together, turn on the system, and show the jury the evidence in the computer. In other words, you'll need to re-create the crime scene just as in any other case.

- Document the back of the computer with a video camera or by taking a series of still photos. This will help you put the computer back together at a later date.
- Make a diagram of the back of the computer
- Label each end of every cable and the the point that it plugs into the computer or any other device.
- If the computer or some other device has a connection point without a cable, then mark it "empty" or with a "zero." Then you know that nothing plugs into those areas.



In the diagram above, note that the far left hand connection point on the computer monitor is labeled "1." The end of the cable that connects to it is also labeled "1." The other end of that same cable is labeled "5" because it plugs into a connection point that's labeled number "5" on the computer box. All connection points which have no cable or other wire connectors are labeled "MTY," signifying that they are empty.

Transporting

- There are several Do's and Don'ts regarding the transporting of computers.
- Put the computer on the floor in the back seat area of the car.
- Don't put the computer on the seat. The seat amplifies the vibrations from the road and can damage the hard drive.
- Don't put the computer in the trunk. The signal from a police radio transmitter in the trunk can damage the hard drive and destroy evidence.

Storing the Computer

- Put the computer in a cool, dry area.
- Do not store near generators or any device which may emit electromagnetic signals.

Key Contacts

Federal Agencies

State Agencies

Law Enforcement Organizations

Internet Service Providers

Glossary of Terms

The Law Enforcement Guide to On-Line Crime
Copyright 1998 Information Video, Inc.
9011 Eton Road Silver Spring, Maryland 20901
Phone 301-587-1984
Fax 301-585-1846
E-Mail spirovideo@aol.com

NEW MEXICO ADVANCE LEGISLATIVE SERVICE
STATENET
Copyright (c) 1998 by Information for Public Affairs, Inc.

NEW MEXICO 43RD LEGISLATURE -- SECOND REGULAR SESSION

CHAPTER 64

SENATE BILL 127

1998 N.M. ALS 64; 1998 N.M. Laws 64; 1998 N.M. Ch. 64; 1998 N.M. SB 127

SYNOPSIS: AN ACT RELATING TO SEXUALLY ORIENTED MATERIAL HARMFUL TO MINORS;
INCLUDING COMPUTER COMMUNICATIONS; CREATING CRIMES; PROVIDING PENALTIES.

----- To view the next section, type .np* TRANSMIT.
To view a specific section, transmit p* and the section number. e.g. p* 1

----- BE IT ENACTED BY THE LEGISLATURE OF
THE STATE OF NEW MEXICO:

[*1] Section 1. A new section of Chapter 30, Article 37 NMSA 1978 is enacted to read:

"DISSEMINATION OF MATERIAL THAT IS HARMFUL TO A MINOR BY COMPUTER--CHILD
LURING.--

A. Dissemination of material that is harmful to a minor by computer consists of the use of a computer communications system that allows the input, output, examination or transfer of computer data or computer programs from one computer to another, to knowingly and intentionally initiate or engage in communication with a person under eighteen years of age when such communication in whole or in part depicts actual or simulated nudity, sexual intercourse or any other sexual conduct. Whoever commits dissemination of material that is harmful to a minor by computer is guilty of a misdemeanor.

B. Child luring consists of a person knowingly and intentionally inducing a child under sixteen years of age, by means of computer, to engage in sexual intercourse, sexual contact or in a sexual or obscene performance, or to engage in any other sexual conduct when the perpetrator is at least three years older than the child. Whoever commits child luring is guilty of a fourth degree felony.

C. In a prosecution for dissemination of material that is harmful to a minor by computer, it is a defense that the defendant has:

(1) in good faith taken reasonable, effective and appropriate actions under the circumstances to restrict or prevent access by minors to indecent materials on computer, including any method that is feasible with available technology;

(2) restricted access to indecent materials by requiring the use of a verified credit card, debit account, adult access code or adult personal identification number; or

(3) in good faith established a mechanism such as labeling, segregation or other means that enables the indecent material to be automatically blocked or screened by software or other capability reasonably available to persons who wish to effect such blocking or screening and the defendant has not otherwise solicited a minor not subject to such screening or blocking capabilities to access the indecent material or to circumvent the screening or blocking.

D. In a prosecution for dissemination of material that is harmful to a minor by computer, a person shall not be held to have violated the provisions of this section solely for providing access or connection to or from a facility, system or network not under the person's control, including transmission, downloading, intermediate storage, access software or

other related capabilities that are incidental to providing access or connection and that do not include the creation of the content of the communication.

E. The limitations provided by Subsection D of this section shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing dissemination of indecent material by computer or who knowingly advertises the availability of indecent material by computer. The limitations provided by Subsection D of this section shall not be applicable to a person who provides access or connection to a facility, system or network that disseminates indecent material by computer that is owned or controlled by him.

F. No employer shall be held liable for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his employment or agency and the employer, having knowledge of such conduct, authorizes or ratifies the conduct or recklessly disregards the conduct."

[*2] Section 2. EFFECTIVE DATE.--The effective date of the provisions of this act is July 1, 1998.

HISTORY: Approved by the Governor March 10, 1998

SPONSOR: Ingle

FLORIDA STATUTES 1997

*** THIS DOCUMENT IS CURRENT THROUGH THE 1997 REGULAR LEGISLATIVE SESSION ***

TITLE XLVI CRIMES
CHAPTER 847 OBSCENE LITERATURE; PROFANITY

Fla. Stat. § 847.0135 (1997)

847.0135 Computer pornography; penalties.

(1) **SHORT TITLE.**--This section shall be known and may be cited as the "Computer Pornography and Child Exploitation Prevention Act of 1986."

(2) **COMPUTER PORNOGRAPHY.**--A person who:

- (a) Knowingly compiles, enters into, or transmits by means of computer;
- (b) Makes, prints, publishes, or reproduces by other computerized means;
- (c) Knowingly causes or allows to be entered into or transmitted by means of computer; or
- (d) Buys, sells, receives, exchanges, or disseminates,

any notice, statement, or advertisement, or any minor's name, telephone number, place of residence, physical characteristics, or other descriptive or identifying information, for purposes of facilitating, encouraging, offering, or soliciting sexual conduct of or with any minor, or the visual depiction of such conduct. The fact that an undercover operative or law enforcement officer was involved in the detection and investigation of an offense under this section shall not constitute a defense to a prosecution under this section. Any person who violates the provisions of this subsection commits a felony of the third degree, punishable as provided for in s. 775.082, s. 775.083, or s. 775.084.

(3) **CERTAIN USES OF COMPUTER SERVICES PROHIBITED.**--Any person who knowingly utilizes a computer on-line service, Internet service, or local bulletin board service to seduce, solicit, lure, or entice, or attempt to seduce, solicit, lure, or entice, a child or another person believed by the person to be a child, to commit any illegal act described in chapter 794, relating to sexual battery; chapter 800, relating to lewdness and indecent exposure; or chapter 827, relating to child abuse, commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(4) **OWNERS OR OPERATORS OF COMPUTER SERVICES LIABLE.**--It is unlawful for any owner or operator of a computer on-line service, Internet service, or local bulletin board service knowingly to permit a subscriber to utilize the service to commit a violation of this section. Any person who violates this section commits a misdemeanor of the first degree, punishable by a fine not exceeding \$2,000.

(5) **STATE CRIMINAL JURISDICTION.**--A person is subject to prosecution in this state pursuant to chapter 910 for any conduct proscribed by this section which the person engages in, while either within or outside this state, if by such conduct the person commits a violation of this section involving a child residing in this state, or another person believed by the person to be a child residing in this state.

HISTORY: s. 11, ch. 86-238; s. 213, ch. 91-224; s. 71, ch. 96-388.

MICHIE'S ALABAMA CODE
Copyright (c) 1997 by Michie,
a division of Reed Elsevier Inc. and Reed Elsevier Properties Inc.
All rights reserved.

*** THIS SECTION IS CURRENT THROUGH THE 1997 SUPPLEMENT ***
*** (1997 REGULAR SESSION) ***

TITLE 13A. CRIMINAL CODE
CHAPTER 6. OFFENSES INVOLVING DANGER TO THE PERSON
ARTICLE 6. SEX OFFENSES BY COMPUTER USE INVOLVING A CHILD

Code of Ala. § 13A-6-110 (1997)

§ 13A-6-110. Child; solicitation by computer

(a) In addition to the provisions of Section 13A-6-69, a person is guilty of solicitation of a child by a computer if the person is 19 years of age or older and the person knowingly, with the intent to commit an unlawful sex act, entices, induces, persuades, seduces, prevails, advises, coerces, or orders, by means of a computer, a child who is less than 16 years of age and at least three years younger than the defendant, to meet with the defendant or any other person for the purpose of engaging in sexual intercourse, sodomy, or to engage in a sexual performance, obscene sexual performance, or sexual conduct for his or her benefit.

(b) For purposes of determining jurisdiction, the offense is committed in this state if the transmission that constitutes the offense either originates in this state or is received in this state.

(c) A person charged under this section shall be tried as an adult, and the record of the proceeding shall not be sealed nor subject to expungement.

(d) Solicitation of a child by computer is a Class B felony.

NOTES: EFFECTIVE DATES. Acts 1997, No. 97-486, effective August 1, 1997.

MICHIE'S ALABAMA CODE
Copyright (c) 1997 by Michie,
a division of Reed Elsevier Inc. and Reed Elsevier Properties Inc.
All rights reserved.

*** THIS SECTION IS CURRENT THROUGH THE 1997 SUPPLEMENT ***
*** (1997 REGULAR SESSION) ***

TITLE 13A. CRIMINAL CODE
CHAPTER 6. OFFENSES INVOLVING DANGER TO THE PERSON
ARTICLE 4. SEXUAL OFFENSES

Code of Ala. § 13A-6-69 (1997)

§ 13A-6-69. Child molestation; enticing, inviting, etc., child to propose sexual acts

It shall be unlawful for any person with lascivious intent to entice, allure, persuade or invite, or attempt to entice, allure, persuade or invite, any child under 16 years of age to enter any vehicle, room, house, office or other place for the purpose of proposing to such child the performance of an act of sexual intercourse or an act which constitutes the offense of sodomy or for the purpose of proposing the fondling or feeling of the sexual or genital parts of such child or the breast of such child, or for the purpose of committing an aggravated assault on such child, or for the purpose of proposing that such child fondle or feel the sexual or genital parts of such person.

Any person violating the provisions of this section shall, for the first violation, be punished by a fine not to exceed \$5,000.00 or by confinement for a term not to exceed five years, or by both fine and imprisonment; and any person who shall be convicted for the second violation of this section shall be punished by confinement in the penitentiary for not less than two nor more than 10 years, and such person shall not be eligible for probation.

NOTES: CROSS REFERENCES. --This law is referred to in: § 15-22-36. Public lewdness, § 13A-12-130.

HOWELL: PRACTICE FORMS. --§ 1-20-11.01.

MADDOX: RULES OF CRIM. PROC. --Rule 27.6; § 27.0.

CASE NOTES

Elements
Evidence /- Sufficient
Included offenses
Instructions
Intent, knowledge
Cited

ELEMENTS.

This section does not require that the proposal be communicated by verbal expression or that the proposal be manifested in any particular form or fashion. *Tedder v. State*, 547 So. 2d 601 (Ala. 1989).

EVIDENCE -- SUFFICIENT.

Defendant's sordid remarks to child riding bicycle on sidewalk and invitation to child to come to defendant's house were sufficient to support a conviction under this section. *Donovan v. State*, 249 So. 2d 635 (Ala. Crim. App. 1971).

Where victim testified that, on each occasion, the appellant would come by on a day when the victim's mother worked, and the victim would tell her mother that the appellant and she were going to play tennis, they would get in the appellant's car and he would drive to his girl friend's house, they would then enter his girl friend's house and walk back to her room, and the appellant would then show the victim dirty magazines and engage in sexual relations with her, this testimony was sufficient to prove the elements of invitation and intent and to submit the case to the jury; the victim's

testimony about the intruder's conduct, once inside the bedroom, was sufficient to prove the intent element. *Williams v. State*, 548 So. 2d 584 (Ala. Crim. App. 1988).

The state presented sufficient evidence to sustain his conviction of enticing, alluring, or persuading the victim to enter house. Although there was no evidence of verbal communication by the appellant to the victim asking him to come into the house, there was an enticement of drugs and alcohol. *Marks v. State*, 581 So. 2d 1182 (Ala. Crim. App. 1990).

INCLUDED OFFENSES.

"Enticing a child to enter a vehicle" is not a lesser included offense of "sexual abuse in the first degree" because it requires an additional element not set out under § 13A-6-66. *Vinson v. State*, 601 So. 2d 196 (Ala. Crim. App. 1992).

INSTRUCTIONS.

Where trial court in its charge to the jury changed wording of indictment, which had charged defendant violated this section by enticing or attempting to entice one named child "and" another named child, the charge constituted a material change in the language of the indictment, which abridged substantial rights of the defendant, because to convict him under the original indictment, the jury had to be convinced he enticed, or attempted to entice, both children, but under the "amended" version, the jury could convict if they were satisfied that he violated this section as to only one of the children but not necessarily both. *Styles v. State*, 474 So. 2d 185 (Ala. Crim. App. 1985).

INTENT, KNOWLEDGE.

Defendant had the required lascivious intent in enticing girls into his studio where the items complained of consisted of sexually explicit materials, including magazines, films and pictures. *Langham v. State*, 494 So. 2d 910 (Ala. Crim. App. 1986).

CITED IN *Merton v. State*, 500 So. 2d 1301 (Ala. Crim. App. 1986); *Tedder v. State*, 547 So. 2d 599 (Ala. Crim. App. 1988); *Tedder v. State*, 547 So. 2d 603 (Ala. Crim. App. 1989); *Goff v. State*, 572 So. 2d 1283 (Ala. Crim. App. 1990); *Jones v. State*, 615 So. 2d 1293 (Ala. Crim. App. 1993); *Ex parte Woodard*, 631 So. 2d 1065 (Ala. Crim. App. 1993), cert. denied, 513 U.S. 869, 115 S. Ct. 190, 130 L. Ed. 2d 123 (1994).

ILLINOIS COMPILED STATUTES ANNOTATED
Copyright (c) 1993 - 1998 by LEXIS Law Publishing,
a division of Reed Elsevier Inc. and Reed Elsevier Properties Inc.
All rights reserved.

*** THIS SECTION IS CURRENT THROUGH PUBLIC ACT 90-573 ***
*** (1997 REGULAR SESSION) ***

CHAPTER 720. CRIMINAL OFFENSES
CRIMINAL CODE
CRIMINAL CODE OF 1961
TITLE III. SPECIFIC OFFENSES
PART B. OFFENSES DIRECTED AGAINST THE PERSON
ARTICLE 11. SEX OFFENSES

720 ILCS 5/11-6 (1997)

[Prior to 1/1/93 cited as: Ill. Rev. Stat., Ch. 38, para. 11-6]

§ 720 ILCS 5/11-6. Indecent solicitation of a child

Sec. 11-6. Indecent solicitation of a child. (a) A person of the age of 17 years and upwards who solicits a child under the age of 13 to do any act, or solicits a person to arrange an act with a child under the age of 13, which if done would be aggravated criminal sexual assault, predatory criminal sexual assault of a child, criminal sexual assault, aggravated criminal sexual abuse or criminal sexual abuse, commits indecent solicitation of a child.

(b) It shall not be a defense to indecent solicitation of a child that the accused reasonably believed the child to be of the age of 13 years and upwards.

(c) Sentence.

Indecent solicitation of a child is:

(1) a Class A misdemeanor when the act, if done, would be criminal sexual abuse;

(2) a Class 4 felony when the act, if done, would be criminal sexual assault, aggravated criminal sexual assault, or aggravated criminal sexual abuse.

(d) For the purposes of this Section, "solicits" includes but is not limited to oral or written communication and communication by telephone, computer, or other electronic means. "Computer" has the meaning ascribed to it in Section 16D-2 of this Code [720 ILCS 5/16D-2].

HISTORY:

Source: P.A. 84-1280; 89-8, § 25-5; 89-203, § 10; 89-428, § 260; 89-462, § 260.

NOTES: NOTE.

This section was Ill.Rev.Stat., Ch. 38, para. 11-6.

CROSS REFERENCES.

For provision requiring the appointment of a guardian ad litem in cases alleging the commission of an offense under this section, see 705 ILCS 405/2-17 and 705 ILCS 405/3-19.

For provision setting forth aggravating factors for purposes of sentencing, see 730 ILCS 5/5-5-3.2.

For provision regarding criminal background investigations, see 105 ILCS 5/10-21.9.

For provision requiring suspension of teaching certificate of any teacher convicted of violating this section, see 105 ILCS 5/21-23a.

EFFECT OF AMENDMENTS.

The 1995 amendment by P.A. 89-8, effective March 21, 1995, in subsection (a), substituted "A" for "Any" and inserted "or solicits a person to arrange an act with a child under the age of 13".

The 1995 amendment by P.A. 89-203, effective July 21, 1995, incorporated the changes by P.A. 89-8; and added subsection (d).

The 1995 amendment by P.A. 89-428, effective December 13, 1995 and the 1996 amendment by P.A. 89-462, effective May 29, 1996, made identical amendments: they each incorporated the amendments by P.A. 89-8 and P.A. 89-203; and in subsection (a) inserted "predatory criminal sexual assault of a child".

CASE NOTES

ANALYSIS

Delinquency

Evidence Held Sufficient

Indictment

--Held Sufficient

Intent

Lesser Included Offenses

--Indecent Liberties with a Child

Prosecutorial Discretion

Sentencing

--Factors

--Sentence Reduced

Separate Offenses

--Shown

DELINQUENCY

Under prior similar provision where the defendant sold an obscene and indecent book to a 16 year old, no one could seriously question that the selling of an obscene and indecent book to a child would tend to corrupt the child's mind and contribute in some measure to indecent and lascivious conduct on his part; thus, such conduct constituted delinquency within the meaning of former section. *People v. Friedrich*, 385 Ill. 175, 52 N.E.2d 120 (1943).

EVIDENCE HELD SUFFICIENT

Evidence was sufficient to support defendant's convictions for indecent liberties with a child (now sexual assault) and indecent solicitation of a child despite the fact that there were inconsistencies as to the details of the offense, where the complainant's testimony established all the elements of the offense. *People v. Leggans*, 80 Ill. App. 3d 51, 35 Ill. Dec. 515, 399 N.E.2d 349 (5 Dist. 1980).

Evidence was sufficient to sustain defendant's conviction of taking immoral, improper, and indecent liberties with a female child under the age of 15 years (now 13 years). *People v. Gilmore*, 320 Ill. 233, 150 N.E. 631 (1926).

INDICTMENT

--HELD SUFFICIENT

Indictment charging defendant with pandering "in that she, for money, knowingly arranged and offered to arrange a situation in which a female, ... may practice prostitution" was not deficient even though it failed to state the name of any person who was the object of the offense and used the term "may" to describe the arranged situation. *People v. Curry*, 56 Ill. 2d 162, 306 N.E.2d 292 (1973).

INTENT

The intent of the prior indecent liberties statute was to protect innocent children from the sexual advances of older persons who have a dangerous propensity to victimize the immature. *People v. Plewka*, 27 Ill. App. 3d 553, 327 N.E.2d 457 (1 Dist. 1975).

LESSER INCLUDED OFFENSES

--INDECENT LIBERTIES WITH A CHILD

Indecent solicitation was not a lesser included offense of indecent liberties with a child (now sexual assault) because the former requires a solicitation, while the latter did not. *People v. Esterline*, 159 Ill. App. 3d 164, 111 Ill. Dec. 242, 512 N.E.2d 358 (1 Dist. 1987).

PROSECUTORIAL DISCRETION

Since the prosecutor has the discretion to decide whether to charge criminal sexual abuse or aggravated criminal sexual abuse, it follows that he has similar discretion when making a decision to file charges under this section. *People v. Nash*, 183 Ill. App. 3d 924, 132 Ill. Dec. 259, 539 N.E.2d 822 (4 Dist. 1989).

SENTENCING

--FACTORS

Defendant's sentence of 25 to 75 years for convictions of indecent liberties with a child and indecent solicitation of a child (now sexual assault) was not excessive in light of the trial court's consideration of the defendant's character, prior record, rehabilitative potential and the nature of the offense. *People v. Leggans*, 80 Ill. App. 3d 51, 35 Ill. Dec. 515, 399 N.E.2d 349 (5 Dist. 1980).

--SENTENCE REDUCED

Where the court disbelieved that the complainant yielded to force, where she was sexually sophisticated, where she was a few months short of 16 and may have looked that age, and where there was no evidence from which it could be inferred that either of the defendants had a tendency to sexually molest children, appellate court concluded that the application of the former indecent liberties statute (see now this section), was inappropriate and the imposition of the minimum penalty of four years exacted by the statute was unduly harsh, and reduced the degree of the offense for which the defendants were convicted from indecent liberties to contributing to the sexual delinquency of a child. *People v. Plewka*, 27 Ill. App. 3d 553, 327 N.E.2d 457 (1 Dist. 1975).

SEPARATE OFFENSES

--SHOWN

Indecent solicitation occurred when a defendant asked a child to perform an act of fellatio, but the former offense of attempted indecent liberties with a child (now sexual assault) occurred when the defendant took a substantial step toward the commission of the offense by unzipping his pants and exposing his penis to the victim; separate acts were committed by the defendant in the commission of each offense. *People v. Brewer*, 118 Ill. App. 3d 189, 73 Ill. Dec. 774, 454 N.E.2d 1023 (3 Dist. 1983), cert. denied, 469 U.S. 930, 105 S. Ct. 324, 83 L. Ed. 2d 261 (1984).

LEGAL PERIODICALS

For case note, "Hewitt v. Hewitt Contract Cohabitation, and 'Equitable Expectations' Relief for Meretricious Spouses," see 12 J. Marshall J. Prac. & Proc. 435 (1979).

For article, "New Class X Sentencing Law: An Analysis," see 66 Ill. B.J. 344 (1978).

For note, "Child Pornography: A New Role for the Obscenity Doctrine," see 1978 U. Ill. L.F. 711.

RESEARCH REFERENCES

Entrapment defense in sex offense prosecutions. 12 ALR4th 413.

Modern status of rule regarding necessity for corroboration of victim's testimony in prosecution for sexual offense. 31 ALR4th 120.

Indecent exposure: What is "person." 63 ALR4th 1040.

Liability of church or religious society for sexual misconduct of clergy. 5 ALR5th 530.

BURNS INDIANA STATUTES ANNOTATED
Copyright (c) 1894-1997 by Michie,
a division of Reed Elsevier Inc. and Reed Elsevier Properties Inc.
All rights reserved.

*** THIS SECTION IS CURRENT THROUGH THE 1997 SUPPLEMENT
*** (1997 SPECIAL SESSION) ***

TITLE 35. CRIMINAL LAW AND PROCEDURE
ARTICLE 42. OFFENSES AGAINST THE PERSON
CHAPTER 4. SEX CRIMES

Burns Ind. Code Ann. § 35-42-4-6 (1997)

§ 35-42-4-6. Child solicitation

A person eighteen (18) years of age or older who knowingly or intentionally solicits a child under fourteen (14) years of age to engage in:

- (1) sexual intercourse;
- (2) deviate sexual conduct; or
- (3) any fondling or touching intended to arouse or satisfy the sexual desires of either the child or the older person;

commits child solicitation, a Class D felony. However, the offense is a Class C felony if it is committed by using a computer network (as defined in IC 35-43-2-3(a)).

HISTORY: P.L.183-1984, § 5; P.L.11-1994, § 16; P.L.79-1994, § 14; P.L.216-1996, § 20.

NOTES: AMENDMENTS. The 1996 amendment added the last sentence of this section.

EFFECTIVE DATES. P.L.216-1996, § 20. July 1, 1996.

NOTES TO DECISIONS

ANALYSIS

Attempted Molesting.

ATTEMPTED MOLESTING.

Child solicitation may constitute attempted child molesting where the solicitation is: (1) substantially in the nature of persuasion; and (2) aimed at immediate commission of the crime. *Ward v. State*, 528 N.E.2d 52 (Ind. 1988).

COLLATERAL REFERENCES. Admissibility of evidence that juvenile prosecuting witness in sex offense case had prior sexual experience for purposes of showing alternative source of child's ability to describe sex acts. 83 A.L.R.4th 685.

Validity, construction, and application of state statutes or ordinances regulating sexual performance by child. 42 A.L.R.5th 291.

BURNS INDIANA STATUTES ANNOTATED
Copyright (c) 1894-1997 by Michie,
a division of Reed Elsevier Inc. and Reed Elsevier Properties Inc.
All rights reserved.

*** THIS SECTION IS CURRENT THROUGH THE 1997 SUPPLEMENT
*** (1997 SPECIAL SESSION) ***

TITLE 35. CRIMINAL LAW AND PROCEDURE
ARTICLE 43. OFFENSES AGAINST PROPERTY
CHAPTER 2. BURGLARY -- TRESPASS

Burns Ind. Code Ann. § 35-43-2-3 (1997)

§ 35-43-2-3. Computer trespass

(a) As used in this section:

"Access" means to:

- (1) Approach;
- (2) Instruct;
- (3) Communicate with;
- (4) Store data in;
- (5) Retrieve data from; or
- (6) Make use of resources of;

a computer, computer system, or computer network.

"Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of two (2) or more interconnected computers.

"Computer system" means a set of related computer equipment, software, or hardware.

(b) A person who knowingly or intentionally accesses:

- (1) A computer system;
- (2) A computer network; or
- (3) Any part of a computer system or computer network;

without the consent of the owner of the computer system or computer network, or the consent of the owner's licensee, commits computer trespass, a Class A misdemeanor.

HISTORY: P.L.35-1986, § 3.

NOTES: CROSS REFERENCES. Computer tampering, IC 35-43-1-4.

COLLATERAL REFERENCES. Criminal liability for theft of, interference with, or unauthorized use of, computer programs, files, or systems. *51 A.L.R. 4th 971*.

What is computer "trade secret" under state law. *53 A.L.R. 4th 1046*.

THE STATE OF NEW HAMPSHIRE
BILL TEXT
STATENET
Copyright (c) 1998 by Information for Public Affairs, Inc.

NEW HAMPSHIRE SECOND YEAR OF THE 155TH SESSION OF THE GENERAL COURT

HOUSE BILL 1561

HB 1561-FN - AS AMENDED BY THE HOUSE
1998 SESSION
HOUSE BILL 1561-FN

1997 NH H.B. 1561

VERSION: Passed First House as Amended

VERSION-DATE: March 5, 1998

SYNOPSIS:

AN ACT preventing computer pornography and child exploitation and increasing penalties for possession under the child pornography laws.

SPONSORS: Rep. Cardin, Hills 32; Rep. Adams, Merr 9; Rep. Knowles, Straf 11; Rep. Micklon, Rock 26; Rep. MacAuslan, Hills 30

COMMITTEE: Criminal Justice and Public Safety

AMENDED ANALYSIS

This bill establishes penalties for child pornography, exploitation, and abuse offenses committed by means of computer. The bill makes owners and operators of computer services criminally liable for knowingly permitting subscribers to utilize their services to commit such offenses.

The bill also increases the penalty for possession offenses under the child pornography laws from a misdemeanor to a class B felony.

STATE OF NEW HAMPSHIRE

In the Year of Our Lord One Thousand Nine Hundred and Ninety-Eight

AN ACT preventing computer pornography and child exploitation and increasing penalties for possession under the child pornography laws.

NOTICE:

[A> UPPERCASE TEXT WITHIN THESE SYMBOLS IS ADDED <A]

[D> Text within these symbols is deleted <D]

TEXT: Be it Enacted by the Senate and House of Representatives in General Court convened:

1 Penalties for Offenses Increased; Misdemeanor to Felony. Amend RSA 649-A:3 to read as follows:

649-A:3 Offenses.

I. A person is guilty of a felony if [D> he <D] [A> SUCH PERSON <A] :

(a) Sells, delivers or provides, or offers or agrees to sell, deliver or provide, any visual representation of a child engaging in sexual activity; or

(b) Presents or directs a visual representation of a child engaging in sexual activity, or participates in that portion of such visual representation which consists of a child engaging in sexual activity; or

(c) Publishes, exhibits or otherwise makes available any visual representation of a child engaging in sexual activity; or

(d) Possesses any visual representation of a child engaging in sexual activity for purposes of sale or other commercial dissemination [D> . <D] [A> ; OR <A]

[A> (E) KNOWINGLY BUYS, PROCURES, POSSESSES, OR CONTROLS ANY VISUAL REPRESENTATION OF A CHILD ENGAGING IN SEXUAL ACTIVITY; OR <A]

[A> (F) KNOWINGLY BRINGS OR CAUSES TO BE BROUGHT INTO THIS STATE ANY VISUAL REPRESENTATION OF A CHILD ENGAGING IN SEXUAL ACTIVITY. <A]

II. An offense under paragraph I shall be:

(a) A class B felony if such person has had no prior convictions in this state or another state for the conduct prohibited by paragraph I;

(b) A class A felony if such person has had one or more prior convictions in this state or another state for the conduct prohibited by paragraph I.

[D> III. A person is guilty of a misdemeanor if he: <D]

[D> (a) Buys, procures, possesses, or controls any visual representation of a child engaging in sexual activity; or <D]

[D> (b) Brings or causes to be brought into this state any visual representation of a child engaging in sexual activity. <D]

2 New Chapter; Computer Pornography and Child Exploitation Prevention. Amend RSA by inserting after chapter 649-A the following new chapter:

CHAPTER 649-B

COMPUTER PORNOGRAPHY AND

CHILD EXPLOITATION PREVENTION

649-B:1 Short Title. This chapter shall be known and may be cited as the 'Computer Pornography and Child Exploitation Prevention Act of 1998.'

649-B:2 Definition. In this chapter, 'child' means any person under the age of 16 years.

649-B:3 Computer Pornography Prohibited.

I. No person shall [A> KNOWINGLY <A] :

(a) Compile, enter into, or transmit by means of computer;

(b) Make, print, publish, or reproduce by other computerized means;

(c) Cause or allow to be entered into or transmitted by means of computer; or

(d) Buy, sell, receive, exchange, or disseminate by means of computer, any notice, statement, or advertisement, or any minor's name, telephone number, place of residence, physical characteristics, or other descriptive or identifying information, for purposes of facilitating, encouraging, offering, or soliciting sexual conduct of or with any child, or the visual depiction of such conduct.

II. The fact that an undercover operative or law enforcement officer was involved in the detection and investigation of an offense under this section shall not constitute a defense to a prosecution under this section.

III. Any person who violates the provisions of this section is guilty of a class B felony.

649-B:4 Certain Uses of Computer Services Prohibited. Any person who knowingly utilizes a computer on-line service, internet service, or local bulletin board service to seduce, solicit, lure, or entice, or attempt to seduce, solicit, lure, or entice, a child or another person believed by the person to be a child, to commit any of the following is guilty of a class B felony:

I. Any offense under RSA 632-A, relative to sexual assault and related offenses.

II. Indecent exposure and lewdness under RSA 645:1; or

III. Endangering a child, as defined in RSA 639:3.

649-B:5 Owners or Operators of Computer Services Liable.

I. It shall be a class A misdemeanor for any owner or operator of a computer on-line service, internet service, or local bulletin board service knowingly to permit a subscriber to utilize the service to commit a violation of this chapter.

II. Any out-of-state computer service company doing business in New Hampshire which receives a subpoena from the state of New Hampshire resulting from an investigation of a violation of this chapter shall respond to such subpoena within 14 days. Failure to respond may result in the suspension or revocation of such company's right to do business in New Hampshire.

649-B:6 State Criminal Jurisdiction. A person is subject to prosecution for engaging in any conduct proscribed by this chapter within this state, or for engaging in such conduct outside this state if by such conduct the person commits a violation of this chapter involving a child or an individual the person believes to be a child, residing within this state.

3 Authorization for Interception of Telecommunications or Oral Communications; Child Pornography Crimes. Amend RSA 570-A:7 to read as follows:

570-A:7 Authorization for Interception of Telecommunications or Oral Communications. The attorney general, deputy attorney general, or a county attorney, upon the written approval of the attorney general or deputy attorney general, may apply to a judge of competent jurisdiction for an order authorizing or approving the interception of telecommunications or oral communications, and such judge may grant, in conformity with RSA 570-A:9, an order authorizing or approving the interception of telecommunications or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offenses as to which the application is made, when such interception may provide, or has provided, evidence of the commission of organized crime, as defined in RSA 570-A:1, XI, or evidence of the commission of the offenses of homicide, kidnapping, gambling, theft as defined in RSA 637, corrupt practices as defined in RSA 640, [A] CHILD PORNOGRAPHY UNDER RSA 649-A, COMPUTER PORNOGRAPHY AND CHILD EXPLOITATION UNDER RSA 649-B, [A] criminal conduct in violation of the securities law, as defined in RSA 421-B:3, 421-B:4, 421-B:5, 421-B:19, and 421-B:24, criminal conduct in violation of

the security takeover disclosure laws, as defined in RSA 421-A:3, 421-A:7, 421-A:8, 421-A:11, and 421-A:13, robbery as defined in RSA 636:1, arson as defined in RSA 634:1, hindering apprehension or prosecution as defined in RSA 642:3, tampering with witnesses and informants as defined in RSA 641:5, aggravated felonious sexual assault as defined in RSA 632-A:2, felonious sexual assault as defined in RSA 632-A:3, escape as defined in RSA 642:6, bail jumping as defined in RSA 642:8, dealing in narcotic drugs, marijuana, or other dangerous drugs, hazardous waste violations under RSA 147-A:4, I, or any conspiracy to commit any of the foregoing offenses.

4 Effective Date. This act shall take effect January 1, 1999.

SPONSOR:

Cardin

LOAD-DATE: March 11, 1998

GENERAL STATUTES OF NORTH CAROLINA
Copyright (c) 1944-1997 by Michie,
a division of Reed Elsevier Inc. and Reed Elsevier Properties Inc.
All rights reserved.

*** THIS SECTION IS CURRENT THROUGH THE 1997 SUPPLEMENT ***

CHAPTER 14. CRIMINAL LAW
SUBCHAPTER VII. OFFENSES AGAINST PUBLIC MORALITY AND DECENCY
ARTICLE 26. OFFENSES AGAINST PUBLIC MORALITY AND DECENCY

N.C. Gen. Stat. § 14-202.3 (1997)

§ 14-202.3. Solicitation of child by computer to commit an unlawful sex act

(a) Offense. -- A person is guilty of solicitation of a child by a computer if the person is 16 years of age or older and the person knowingly, with the intent to commit an unlawful sex act, entices, advises, coerces, orders, or commands, by means of a computer, a child who is less than 16 years of age and at least 3 years younger than the defendant, to meet with the defendant or any other person for the purpose of committing an unlawful sex act.

(b) Jurisdiction. -- The offense is committed in the State for purposes of determining jurisdiction, if the transmission that constitutes the offense either originates in the State or is received in the State.

(c) Punishment. -- A violation of this section is a Class I felony.

HISTORY: 1995 (Reg. Sess., 1996), c. 632, s. 1.

NOTES: EDITOR'S NOTE. --Session Laws 1995 (Reg. Sess., 1996), c. 632, s. 2, made this section effective December 1, 1996, and applicable to acts committed on or after that date.

OKLAHOMA STATUTES

THIS DOCUMENT IS CURRENT THROUGH THE 1997 SUPPLEMENT (1997 FIRST SESSION)

TITLE 21. CRIMES AND PUNISHMENTS
PART IV. CRIMES AGAINST PUBLIC DECENCY AND MORALITY
CHAPTER 39. INDECENT EXPOSURE, OBSCENITY AND DISORDERLY HOUSES

21 Okl. St. § 1040.13a (1997)

§ 1040.13a. Facilitating, encouraging, offering or soliciting sexual conduct with a minor

A person is guilty of violating the provisions of this section *if, for the purposes of facilitating, encouraging, offering or soliciting sexual conduct with any minor, the person knowingly transmits by means of computer, or prints, publishes or reproduces by other computerized means, or buys, sells, receives, exchanges, or disseminates, any notice, statement, or advertisement of any minor's name, telephone number, place of residence, physical characteristics or other descriptive or identifying information.*

Any violation of the provisions of this section shall be a misdemeanor, punishable by the imposition of a fine not to exceed One Thousand Dollars (\$1,000.00), or by imprisonment in the county jail not to exceed one (1) year, or by both such fine and imprisonment.

THE STATE OF NEW JERSEY
BILL TEXT
STATENET
Copyright (c) 1998 by Information for Public Affairs, Inc.

NEW JERSEY 208TH LEGISLATURE

ASSEMBLY BILL 1332

ASSEMBLY, NO. 1332
STATE OF NEW JERSEY
208TH LEGISLATURE
PRE-FILED FOR INTRODUCTION IN THE 1998 SESSION
SPONSORED BY:
ASSEMBLYWOMAN ROSE MARIE HECK
AS INTRODUCED.

1998 NJ A.B. 1332

VERSION: Introduced

VERSION-DATE: January 13, 1998

SYNOPSIS:

An Act concerning protecting children on the Internet, supplementing Title 2C of the New Jersey Statutes and amending P.L.1992, c.7 and N.J.S.2C:24-4.

DIGEST:

STATEMENT

This bill is known as the "Computer Pornography and Child Exploitation Prevention Act of 1998." The bill would establish as a second degree crime the act of communicating with or contacting a child via computer, including on the Internet, in the following circumstances:

-when a person, knowing the character and content of the communication in whole or in part depicts a child engaging in a prohibited sexual act or in the simulation of such an act, does so to initiate or engage in communication or contact with a child;

-when a person importunes, invites, lures or entices, or attempts to importune, invite, lure or entice a child or other person believed by the person to be a child to engage in a prohibited sexual act;

-when a person transmits, receives, buys or sells any notice, statement or advertisement, or a child's name or other descriptive information for the purpose of engaging in, facilitating, encouraging, offering or soliciting a prohibited sexual act.

A crime of the second degree is punishable by five to 10 years imprisonment, up to a \$100,000 fine, or both.

The bill also amends current law to include the Internet in the methods, devices and communications vehicles which when used unlawfully to contact a child may be the basis for a civil court action by a parent, guardian, child advocacy organization or the child, upon reaching the age of majority. Those unlawful contacts include:

(i) Nudity, if depicted for the purpose of sexual stimulation or gratification of any person who may view such depiction.

(3) Any person, including any parent, guardian, or other person legally charged with the care or custody of a child, who causes or permits a child to engage in a prohibited sexual act or in the simulation of such an act if the person knows, has reason to know or intends that the prohibited act may be photographed, filmed, reproduced, or reconstructed in any manner [A> , INCLUDING ON THE INTERNET, <A] or may be part of an exhibition or performance is guilty of a crime of the second degree.

(4) Any person who photographs or films a child in a prohibited sexual act or in the simulation of such an act or who uses any device [A> , INCLUDING ON THE INTERNET, <A] to reproduce or reconstruct the image of a child in a prohibited sexual act or in the simulation of such an act is guilty of a crime of the second degree.

(5) (a) Any person who knowingly receives for the purpose of selling or who knowingly sells, procures, manufactures, gives, provides, lends, trades, mails, delivers, transfers, publishes, distributes, circulates, disseminates, presents, exhibits, advertises, offers or agrees to offer [A> , INCLUDING ON THE INTERNET, <A] any photograph, film, videotape, computer program, video game or any other reproduction or reconstruction which depicts a child engaging in a prohibited sexual act or in the simulation of such an act, is guilty of a crime of the second degree.

(b) Any person who knowingly possesses or knowingly views any photograph, film, videotape, computer program, video game or any other reproduction or reconstruction which depicts a child engaging in a prohibited sexual act or in the simulation of such an act, [A> INCLUDING ON THE INTERNET, <A] is guilty of a crime of the fourth degree.

(6) For purposes of this subsection, a person who is depicted as or presents the appearance of being under the age of 16 in any photograph or film shall be rebuttably presumed to be under the age of 16. (cf: P.L.1995, c.109, s.1)

5. This act shall take effect on the first day of the sixth month after enactment.

SPONSOR:

Heck

LOAD-DATE: January 17, 1998

THE STATE OF TENNESSEE
BILL TEXT
STATENET
Copyright (c) 1998 by Information for Public Affairs, Inc.

TENNESSEE 100TH GENERAL ASSEMBLY

HOUSE BILL 2561

FILED FOR INTRO ON 01/26/98
HOUSE BILL 2561 BY JACKSON

1997 TN H.B. 2561

VERSION: Introduced

VERSION-DATE: January 22, 1998

SYNOPSIS:

AN ACT to amend Tennessee Code Annotated, Title 38, Chapter 6, to create the Office for Internet Child Protection within the Tennessee bureau of investigation.

TEXT: BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. Tennessee Code Annotated, Title 38, Chapter 6, is amended by adding the following as a new section:

Section ____.

(a) The Tennessee bureau of investigation shall, no later than January 1, 1999, create an office within the bureau to be known as the Office for Internet Child Protection. The purpose of such office is to investigate and collect evidence concerning the commission, attempted commission or solicitation to commit a sexual offense against a child in this state by use of computers or the Internet.

(b) The methods of investigating such sexual offenses against children shall be within the discretion of the bureau but such methods shall include sting operations whereby a bureau agent portraying a child places information on the Internet and electronically communicates with persons responding to such information.

(c) The bureau is authorized to apply for, receive and use any grants or other funds, whether state or federal, that are available to conduct such investigations. The bureau is also authorized to use any proceeds it receives from forfeitures and confiscations for the purposes set out in this section.

SECTION 2. This act shall take effect upon becoming a law, the public welfare requiring it.

SPONSOR:

Jackson

LOAD-DATE: January 27, 1998

reconstructed in any manner [A> , INCLUDING ON THE INTERNET, <A] or may be part of an exhibition or performance;

(2) Photographs or films the child in a prohibited sexual act or in the simulation of such an act or who uses any device [A> , INCLUDING THE INTERNET, <A] to reproduce or reconstruct the image of the child in a prohibited sexual act or in the simulation of such an act;

(3) Knowingly receives for the purpose of selling or who knowingly sells, procures, manufactures, gives, provides, lends, trades, mails, delivers, transfers, publishes, distributes, circulates, disseminates, presents, exhibits, advertises, offers or agrees to offer [A> , INCLUDING ON THE INTERNET, <A] any photograph, film, videotape or any other reproduction or reconstruction which depicts the child engaging in a prohibited sexual act or in the simulation of such an act.

[A> (4) VIOLATES ANY PROVISION OF P.L. ,C. (C.) (NOW PENDING BEFORE THE LEGISLATURE AS THIS BILL). <A]

b. In any action brought pursuant to this act, the court shall, upon a finding for the plaintiff, award recovery of three times the amount of damages consisting of financial gains to the defendant resulting from the conduct described in paragraphs (1), (2) and (3) of subsection a. of this section, together with full costs and reasonable attorney's fees. (cf: P.L.1992, c.7, s.3)

4. N.J.S.2C:24-4 is amended to read as follows:

2C:24-4. Endangering Welfare of Children.

a. Any person having a legal duty for the care of a child or who has assumed responsibility for the care of a child who engages in sexual conduct which would impair or debauch the morals of the child, or who causes the child harm that would make the child an abused or neglected child as defined in R.S.9:6-1, R.S.9:6-3 and P.L.1974, c.119, s.1 (C.9:6-8.21) is guilty of a crime of the second degree. Any other person who engages in conduct or who causes harm as described in this subsection to a child under the age of 16 is guilty of a crime of the third degree.

b. As used in this subsection:

(1) "Child" shall mean any person under 16 years of age.

(2) "Prohibited sexual act" means

(a) Sexual intercourse; or

(b) Anal intercourse; or

(c) Masturbation; or

(d) Bestiality; or

(e) Sadism; or

(f) Masochism; or

(g) Fellatio; or

(h) Cunnilingus; or

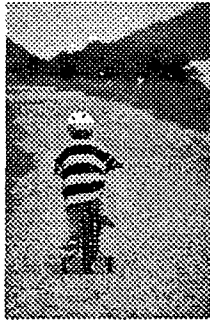
Coordinating and Conducting the Investigation



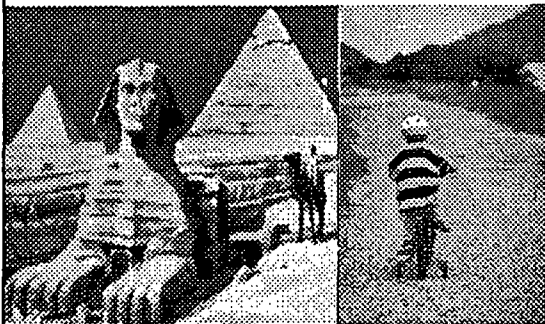
Protecting Children Online

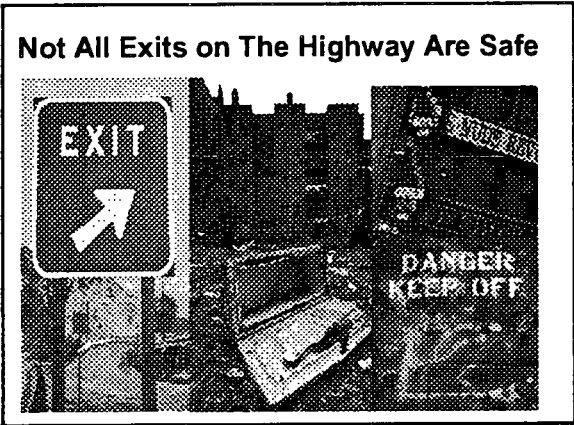
Unit Commander Training

Information Superhighway



Information Superhighway





Dangerous Mix

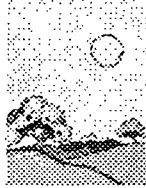
- 10.5 million kids now online
- 45 million by 2002
- 32% of youth aged 16-17 online 5 or more hours per week
- 37% of parents want TV/Internet

Dangerous Mix

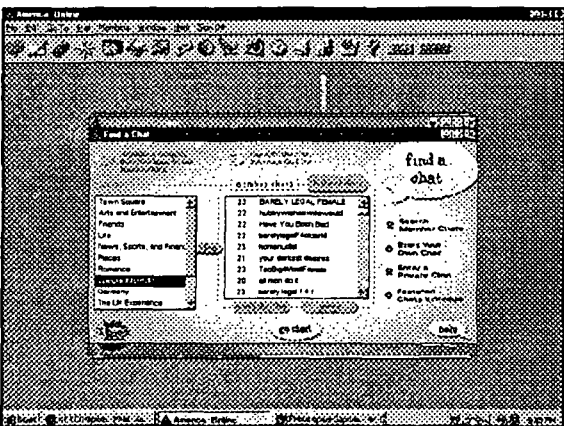
- Anonymous
- Private
- Invisible
- 2/3 of inmates jailed for sex crimes committed offense against a child

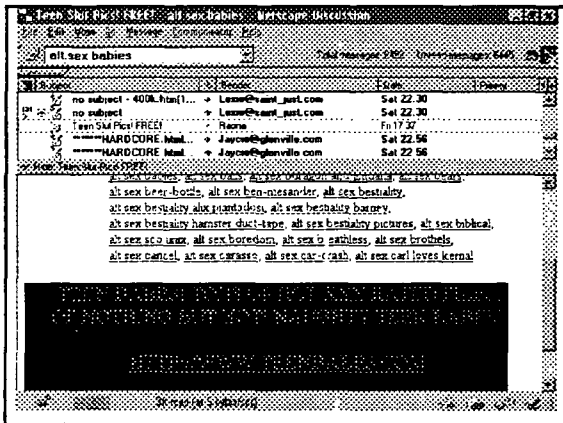
The Dangers

- Web Sites
- Electronic Mail
- Newsgroups
- IRC & Chat Rooms
- FTP









Types of Cases

- Distribution/Manufacturing of Child Pornography
- Possession of Child Pornography
- Endangering the Welfare of a Child
- Obscenity Statutes
- Traveler Cases
- Harassment
- Terroristic Threats
- Organized Conspiracies
- Child Sex Tourism

How The Case Begins

- Visual Evidence: Photos,Pix,Movies
- E-Mail Messages
- Victim-Witness Disclosure
- Concerned Parent or Citizen
- Police Undercover Activity
- Inadvertent Discovery

Responsibility

- **Computer Crimes Unit**
- **Vice Unit**
- **Child Exploitation Unit**
- **All of the Above**
- **None of The Above**
- **Ginsu Approach**

Policies & Procedures

- **State/Federal Law Compliance**
- **Department SOP's and Operations Instructions**
- **Review Undercover Operations Guidelines**
- **Preservation of Electronic Evidence**
- **Prosecutorial Guidance**

Equipment

- **Dedicated Personal Computer**
- **Modem**
- **Printer**
- **Magnetic Media**
- **Software**
- **Hello Line**
- **Undercover Credentials**
- **Tape Recorder - Phone Tap**
- **Caller Id**

Undercover Credentials

- Online Accounts
- Phone
- Address (PO Box, Mail Boxes etc.,)
- Driver's License
- Vehicle Registration
- Credit Cards

Balancing Case Decisions With Resources

- Violator within jurisdiction
- Visit violator
- Violator is outside city limits
- Violator is in another country
- Long term case with intensive support
- Task Force target
- Spider Web Growth of Case

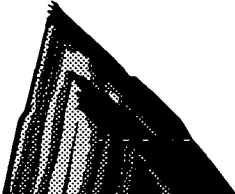
Dedicating Resources

- Pre-search warrant low resource efforts needed
- Undercover Operations: manpower
- Analysis of S/W evidence: methodical & labor intensive
- Computer forensics: time, money, man hours

Challenges for Computer Investigations


Technical Challenges

Legal Challenges



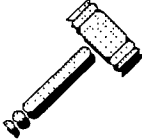
Technical Challenges

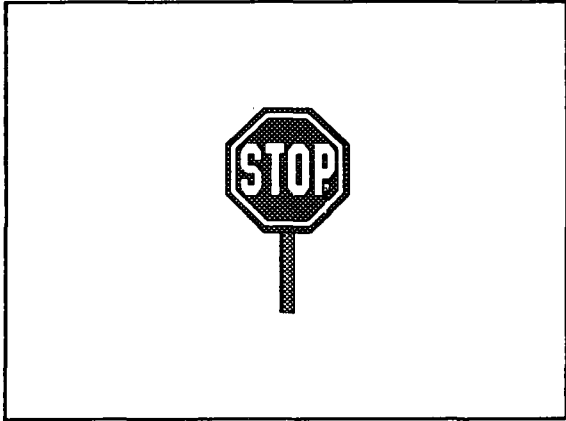
- Hardware, Software, Operating Systems
- Networks
- Passwords, Encryption, Steganography
- Anonymous Remailers
- Spoofing
- Ever Changing Technology



Legal Challenges

- Jurisdictional Boundaries
- Insufficient Case Law
- Law Enforcement Competence
- ECPA
- Privacy Protection Act





Protecting Children Online

Understanding the Structure of the Internet

The Structure of the Internet

- Exponential Growth
- Different types of computers
- Various operating systems
- Variety of organizations
- Controlled Chaos

The Structure of the Internet

- Yet Very Rigid Structure
- Based on Transmission Control Protocol/ Internet Protocol (TCP/IP)
- Current IP Addressing Scheme Allows for 2^{32} Addresses

The Structure of the Internet

Any single computer on the Internet is considered a host or a node. This includes machines such as a massively powerful parallel processing supercomputer or a laptop. The Structure of the Internet does not differentiate between hosts

Domain Name System

The name structure for the Internet follows a convention titled the Domain Name System (DNS). The DNS template is read from left to right and from the more narrow in scope to the more broad. A name consists of several elements or labels each separated by a delimiter (@ or .)

General Format:
account@[subdomain].[subdomain].[...].<domain>

Labels

Labels can be no longer than 63 characters in length; start with a letter; end with a letter or digit and contain only letters, digits or the hyphen.

mikeg@ne-htcia.org

Domain Field

The domain for a name appears as its right-most label. If in the U.S., each host is assigned one of the following domains based on its usage:

gov	Non-military government affiliated
edu	Educational institution
com	Commercial or industrial organizations
org	Other organizations, such as nonprofits
net	Network operations and service centers
mil	Military
arpa	ARPANET members

International Domain Labels

Countries have a domain name assigned to it that corresponds to its two-letter country code.

United states	us
Brazil	br
Ireland	ie
Paraguay	py
England	uk

Subdomain Labels

DNS allows you to breakdown a large group or organization into smaller groups referred to by subdomains.

mgeraghty@shipping.operations.mtg.com

Subdomain Labels

Subdomain for company

mgeraghty@shipping.operations.mtg.com

Subdomains for departments within company

mgeraghty@shipping.operations.mtg.com

Group Department Company

User Label

The left-most label in a DNS name is the user or account name. It is separated from the remaining labels by an @ symbol. The user label usually reflect the identity of the account owner.

User/account label Subdomain for company

mgeraghty@shipping.operations.mtg.com

Subdomains for departments within company

IP Address 32.100.158.195

Internet protocol (IP) address is a unique 32 bit binary number usually represented as 4 fields each representing 8 bit numbers in the range 0 to 255 (called octets) separated by decimal points and identifies a connection to the network. The address consists of a network part and a host part. IP addresses are configured by software; they are not hardware specific. IP Addresses are often hidden from users who instead make use of the domain naming system. Software translates these domain names into IP addresses for routing.

IP Address Classes

There are 5 different address classes. The first byte of the first octet determines the class of the address.

	<u>1st Octet</u>		<u>Network IDs</u>	<u>Host ids</u>
Class A	1-126	1st Octet	126	16,777,214
Class B	128-191	1st 2 Octets	16,382	65,534
Class C	192-223	1st 3 Octets	>2,000,000	254
Class D	224-239	Used for multicasting		
Class E	240-255	Reserved for Future Use		



Electronic Mail Headers

Received from dth-a9@netcom.com (206214 99 8) by in1.0m.net id 900170233 05780-1, Sat, 11 Jul 1999 1057:13 +0000
Received (from errep@usa.net)
by dth-a9@netcom.com (88448 B 4)
id LAA27020 for michael.geraghty@ibm.net, Sat, 11 Jul 1999 1157:09 +0500 (CDT)
Date Sat, 11 Jul 1999 1157:09 +0500 (CDT)
Received from fte-us2-11@netcom.com (204 30 67 75) by dth-a9@netcom.com via errep (V13)
id mra02702 1, Sat Jul 11 1156:35 1999
From ystoye@netcom.com
To michael.geraghty@ibm.net
Message-ID: <1999711125718741@>
Subject: Re: On Service
X-Mailer: NETCOM/ple@v3.25, from NETCOM On-Line Communications, Inc.
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii

E-Mail Addresses

mtg4385@ibm.net

suspect@not.wheretheyouthink.com

An Internet e-mail address has two elements:

Username @ domain.name

The username indicates
the name of the
particular user's mailbox.

The domain name indicates
where the user's mailbox is
located on the Internet.

E-Mail Addresses

From mlawinski@pentagon.gov
To Michael_Geraghty@ibm.net
Subject: Thanks

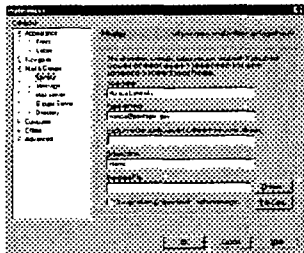
When reading e-mail messages, most e-mail software displays
only the information shown above. It appears this message came
from the e-mail address 'mlawinski@pentagon.gov'.

In reality, the key to the true message originator is buried in the information contained in the entire e-mail header.

```
Received from outbound Princeton EDU (128 112 128 88) by in14m.net id 89627425556736-1,
  Fr, 19 Jun 1988 194305 +0000
Received from IDENT-NOT-QUEUED@postexpress Princeton EDU (port 43600 [128 112 128 131])
  by outbound Princeton EDU with ESMTP id <541576-12 194> Fr, 19 Jun 1988 124220 -0400
Return-Path: <sdongar@princeton.edu>
Received from ml Princeton EDU (ml Princeton EDU [128 112 128 14])
  by postexpress Princeton EDU (8 8 8 8 8) with ESMTP id MAA19475,
  Fr, 19 Jun 1988 124215 -0400 (EDT)
Received from princeton.edu (pr-8c528 Princeton EDU [128 112 11 1 86])
  by ml Princeton EDU (8 8 8 8 12) with ESMTP id 1AA12859 Fr, 19 Jun
Received from friends@edps.com by 81455@newsy.net (8 8 8 4 5) with SMTP
  id GAARZ120 for <AFRIEND@PUBLIC.COM>. Fr, 19 Jun 1988 11 08 36
  -0600 (EST)
1988 124216 -0400 (EDT)
Message-ID: <358A45CB-D128024B@princeton.edu>
Date: Fr, 19 Jun 1988 124900 -0400
From: Jon D'Anger <sdongar@princeton.edu>
Reply-To: <sdongar@princeton.edu>
Organization: Princeton University
Comments: X-Mailer: Mozilla 4.05 [en] (WinNT; i)
MIME-Version: 1.0
To: sfrend@public.com
Subject: Thanks
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

E-Mail Addresses:

Most of today's e-mail software allows the end user to configure the e-mail address placed in outgoing messages. Because of this, the e-mail address is very easily forged and should never be considered the authoritative pointer to the true source of message origination.

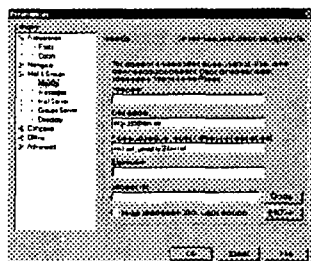


Understanding E-Mail Headers

Some information found in e-mail headers is entered by the end user directly into the e-mail program's configuration.


Example: Netscape Mail

From: mtg4385@bm.net
Reply-To: michael_garaghty@bm.net



The WHOIS Database

Analyzing the Received: headers provided the true origin of the mail message in terms of an IP address, domain name, and date and time the message was sent. But who actually sent the message?

Sender's
Computer:

62-8c528.Princeton.EDU
IP: 128.112.128.61
Fri, 19 Jun 1999
12:42:18 -0400 (EDT)

The IP address in question was used at a particular time. What we need to know now is who to contact to provide a match between a real person, and the date and time the particular IP address was in use.

Public databases on the Internet can be used for research to determine contacts based on the IP address and domain name.

The WHOIS Database

WHOIS can be searched for second-level domain names only. For example :

Valid second-level queries

princeton.edu injersey.com

Invalid second-level queries

ponyexpress.princeton.edu njw.injersey.com

The WHOIS Database

Initial queries can return multiple records. Each record has unique "handle", so specific records can be accessed after the initial query.

whois princeton.edu :

Princeton University (PRINCETON)PRINCETON.EDU 128.112.128.61
Princeton University (PRINCETON-DOM) PRINCETON.EDU



Desired "handle"

The WHOIS Database

whois princeton-dom : Princeton University (PRINCETON-DOH)
Computing and Information Technology 87 P
Sequest Avenue
Princeton, NJ 08544-2007
Domain Name: PRINCETON.EDU
Administrative Contact:
Varian, Lee C. (LCV) lvarian@PRINCETON.EDU
(609) 258-6067 (FAX) (609) 258-3943
Technical Contact, Zone Contact:
Olenick, Peter A. (PAO3) polenick@PRINCETON.EDU
1-609-258-6024 (FAX) 1-609-258-3943
Billing Contact:
Varian, Lee C. (LCV) lvarian@PRINCETON.EDU
(609) 258-6067 (FAX) (609) 258-3943
Record last updated on 13-Feb-98.
Record created on 03-Apr-87.
Database last updated on 11-Jul-98 03:53:40 EDT.
Domain servers in listed order:
DNS1.PRINCETON.EDU 128.112.129.15
NS1C.FVMC.NET 128.123.50.7
NS-HEAT.CERF.NET 192.153.156.3
NS-EAST.CERF.NET 207.252.96.3

Obtaining More Information

What information can we expect from a site to have regarding an e-mail message?

- Mail server logs - Each message passing through a mail server is generally automatically logged. Time of retention for logs varies from site to site, as they take up space on computers.
- Access logs - Use of an IP address is generally logged by access providers. Again, the time of retention for logs varies from site to site, as they take up space on computers.
- The key is to request the information as soon after the event as possible. Otherwise, the offline backup practices of the site will determine availability of the information.

Obtaining More Information

Example from a mail log proving message delivery :

```
From ins6.netns.net :
Nov 22 17:05:26 ins6 sendmail[14002]: RAA14002: from=<kevin@netns.net>, size=502,
class=0, pri=30502, nropts=1, msgid=<01BCF768.C76CFF80.kevin@netns.net>,
proto=SMTP, relay=desm-01-146.fach.netns.net [167.142.120.146]

Nov 22 17:05:27 ins6 sendmail[3725]: RAA14002: to=<kevin@netns.net>,
delay=00:00:01, xdelay=00:00:00, mailer=esmtp, relay=worf.netns.net
[167.142.225.4], stat=Sent (RAA21308 Message accepted for delivery)

From worf.netns.net :
Nov 22 17:05:27 worf sendmail[21308]: RAA21308: from=<kevin@netns.net>, size=669,
class=0, pri=30699, nropts=1, msgid=<01BCF768.C76CFF80.kevin@netns.net>,
proto=ESMTP, relay=ins6.netns.net [167.142.225.6]

Nov 22 17:05:28 worf sendmail[16779]: RAA21308: to=<kevin@netns.net>,
ctaddr=<kevin@netns.net> (13/26), delay=00:00:01, xdelay=00:00:01, mailer=local,
stat=Sent
```

Obtaining More Information

Example from an access log proving originator :

Start of call :

```
Nov 22 17:02:46 ins017 MODEM: S33: CALL_REF >0x08000158< PRI_SLOT >0<
TS >35< SPAN >0< B_CH >0<
Nov 22 17:02:46 ins017 acct 08000158 dial: S33 call arrived.
Nov 22 17:02:46 ins017 sent out answer incoming call for S33.
Nov 22 17:02:57 ins017 acct 08000158 dial: S33 answered the phone using handle 11.
Nov 22 17:02:59 ins017 acct 08000158 dialnet: port S33 kevin succeeded
dest 167.142.120.148
Nov 22 17:03:06 ins017 dialnet: port S33 connection succeeded dest 167.142.120.148
```

End of call :

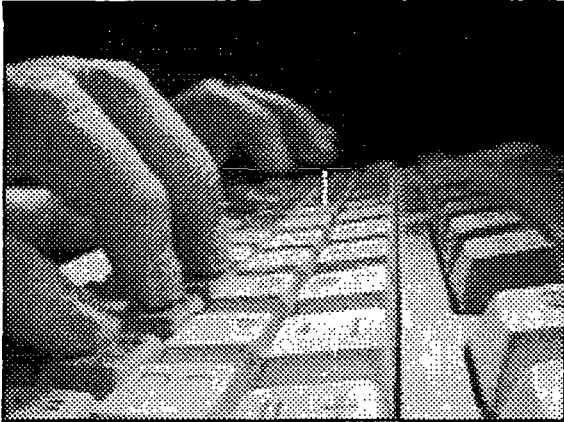
```
Nov 22 17:57:39 ins017 acct 08000158 dial: S33 hung up the phone Call duration 0:55.54.
Nov 22 17:57:39 ins017 acct 08000158 dialnet: port S33 session disconnected
dest dasm-01-146.isdn.netns.net
```

Obtaining More Information

Given an IP address and a time stamp, most providers or sites can find the end user who was using the IP address at the specific time. Knowing who to ask can save valuable time and insure availability of accurate information.

Warrants, court orders or subpoenas are typically required to release exact end user information to law enforcement officials. These requests should contain the IP address and a time stamp including time zone. For e-mail investigations, providing the full e-mail headers is very helpful.





PROTECTING CHILDREN ON-LINE

The Investigation

- Investigative Concerns**
- Have a plan
 - Don't use department's computer system
 - Strict undercover accounts w/ good backstop credentials
 - When/Where is the investigation authorized to be conducted
 - Document and record online sessions
 - Stick with what you know
 - Know when to say when

The Investigation

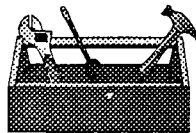
On February 5, 1998 the system administrator of a NJ based Internet Service Provider sent an electronic mail message to the NJSP High Technology Crimes Unit. The sysadmin reported that a web site maintained on his server contained questionable content.

The Investigations

- Case 1- Individual luring young females, transmitting child pornography, case referred from media
- Case 2-Department notified by concerned citizen, and discovers another law enforcement agency.
- Case 3-Phone call from mother of victim.

Investigative Tools

- Whois
- Finger
- Ping
- Traceroute
- Audit Trails & Logs
- Search Engines
- Sniffers
- Protocol Analyzers

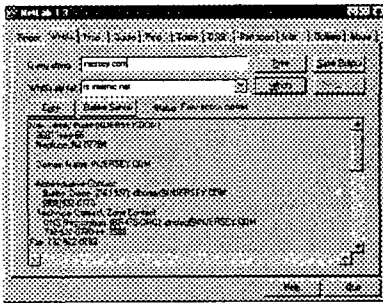


The Whois Database

The National Science Foundation funds a Network Information Center known as the InterNIC. The InterNIC is responsible for registration of IP addresses and domain names ending in .COM, .ORG, .NET, .GOV, and .EDU. InterNIC maintains a public database called the WHOIS database which can be used to find contact information for domain names and IP addresses. The WHOIS database can be queried from the World-Wide Web using a web browser such as MS Internet Explorer or Netscape Navigator. For addresses outside the United States use the Ripe database.

<http://rs.internic.net/cgi-bin/whois>
<http://www.ripe.net>

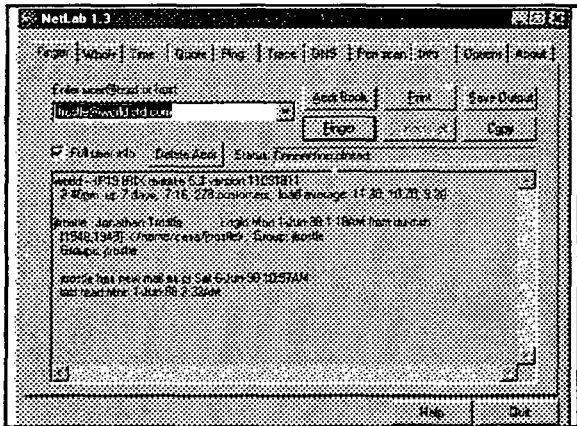
Whois



Finger

Finger is a Unix command which is used to get information on a given user. On systems that allow finger requests, the information returned will include the user's login name, real name, home directory, shell, last time logged in, whether the user has undelivered mail, and the user's plan file.

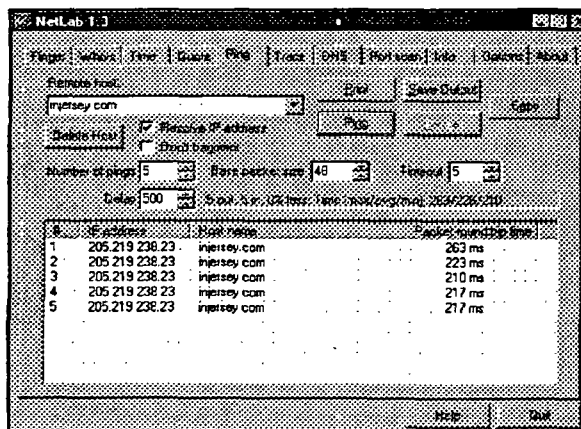
```
htc% finger phillips
Login name: phillips           In real life: Richard D. Phillips
Directory: /home/phillips     Shell: /bin/bash
On since July 12 12.43 02 on ttyb
No Plan
```



Ping

Ping is the networking equivalent of a sonar device and is used to verify that a given Internet address is actually reachable. Ping resolves the hostname to an IP address and sends an echo request to that host on a periodic basis. Each line beginning with "64 bytes..." is the echo reply received from the host. The time field tells you the round trip time for the packet.

```
# ping htc.net.org
PING htc.net.org (206.192.153.4) : 64 data bytes
64 bytes from 206.192.153.4: icmp_seq=0    ttl=254 time=35.9 ms
64 bytes from 206.192.153.4: icmp_seq=1    ttl=254 time=22.1 ms
64 bytes from 206.192.153.4: icmp_seq=2    ttl=254 time=26.7 ms
```

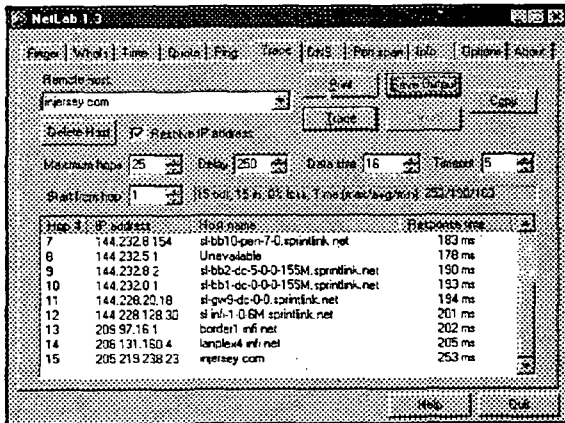


Traceroute

A utility that traces a packet from your computer to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes. Using traceroute is useful in order to determine the delivery path of a packet.

In Windows 95 traceroute is named "tracert" and can be invoked at the DOS command line using the following syntax:

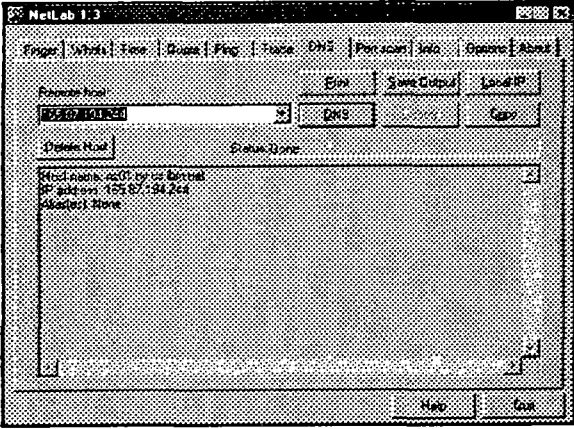
```
c:\tracert samplehost
```

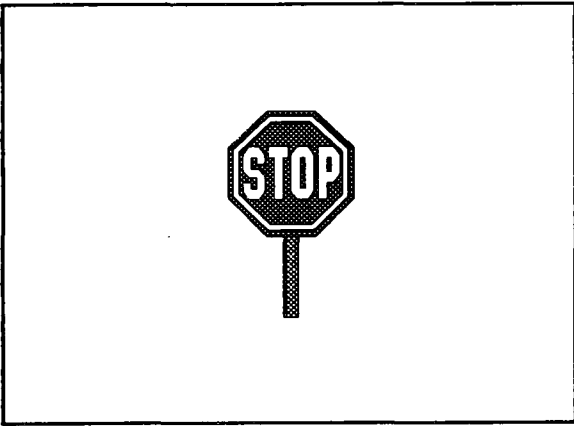


Nslookup

Nslookup will look up and show the corresponding DNS or IP address for a given an IP address or a hostname address. It is similar to whois.


Syntax:
#nslookup hostname





Search Engines

<http://www.dogpile.com>
<http://www.zevally.com/>
<http://www.searchenginewatch.com/>
<http://www.sibery.net/all.html>
<http://www.infopace.com/>
<http://www.mamms.com/>
<http://www.pcworld.com/cgi-bin/www/aw7D-4850>
<http://www.ferretsoft.com/methernet/>
<http://www.eskjesens.com/>
<http://www.virtualbrary.com/research/>
<http://www.netbot.com/>
<http://www.allworlds.digital.com/>
<http://www.jisuloh.com/>
<http://www.metacrawler.com/>
<http://www.dogpile.com/>
<http://www.primacomputing.com/search.htm>
<http://www.figsurfd.com/cleveland/edu/2002/>
<http://www.cornet.com/multimedia/frames/>
<http://www.zdnet.com/product/internetuser.html>
<http://www.jimrhino.com/intfind/>
<http://www.infopacinc.com/>
<http://www.lookup.com/lookup/search.html>
<http://www.howhere.com/>
<http://www.switchboard.com/>
<http://204.254.70.82/poc11v2.html>
<http://www.djshwa.com/>
<http://www.backup.com/engines.html>
http://www.yahoo.com/Computers_and_Internet/Internet/World_Wide_Web/Searching_the_Web/
<http://www.sibery.net/all.html>
<http://www.dreamscape.com/franvad/search.html>


 US 1-800-4NUMBLED
 Incorporated 1-201-478-2028
 The Marketing Information Company



If you have questions regarding privacy, please call us at: 1-800-4NUMBLED
 For more information visit us at: www.4numbled.com

[Displaying matches 1 of 3]

Name	Address	Phone
William H. Cavigley	1401 W. Chippewa St., Apt. 101, Oak Brook, IL 60121-2801	(630) 572-4325
William H. Cavigley	1401 W. Chippewa St., Apt. 101, Oak Brook, IL 60121-2801	(630) 572-4325
William H. Cavigley	1401 W. Chippewa St., Apt. 101, Oak Brook, IL 60121-2801	(630) 572-4325

[Displaying matches 1 of 3]

© 1999 Database America, Inc.
 All Rights Reserved.



 PeopleFinder


Residential Directory Assistance
 Get connected to America.

Enter a last name to search for or press a key to search for

First Name:
 Last Name:
 City:
 State:

Or look up someone by clicking just this phone number below:
 Phone:

Special Use Names? [Businesses](#) [Hotels](#) [Fax](#) [E-mail](#) [Search](#) [Send](#)


 US 1-800-4NUMBLED
 Incorporated 1-201-478-2028
 The Marketing Information Company

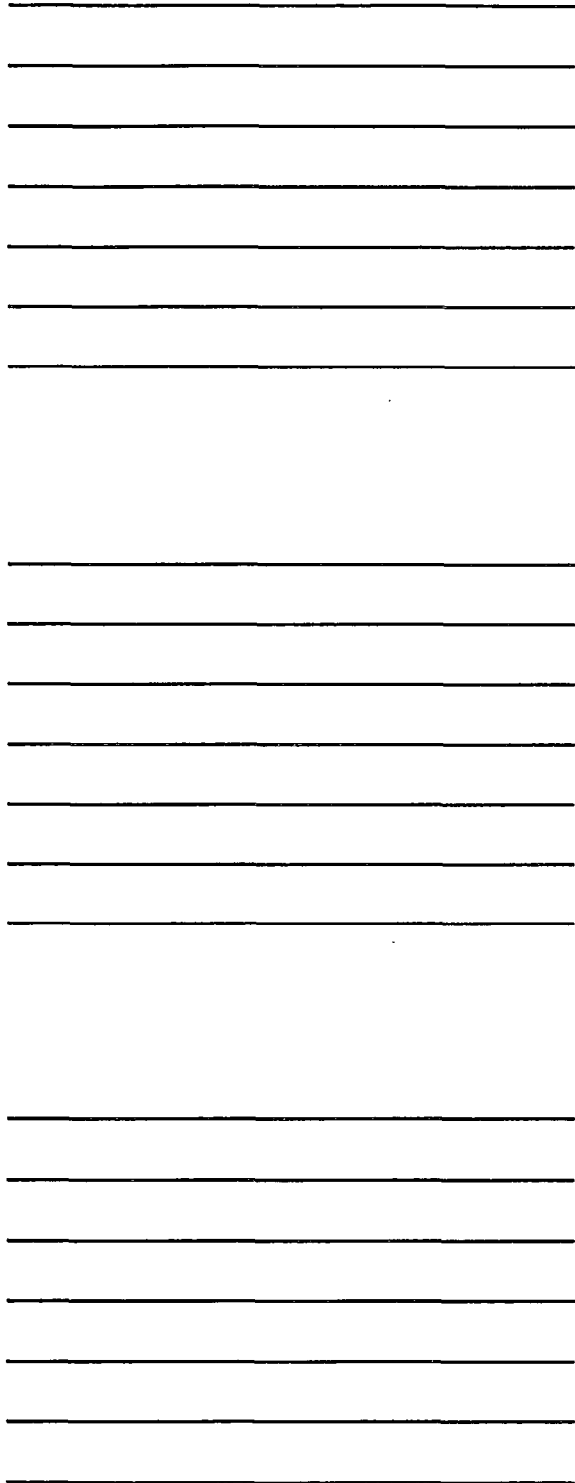
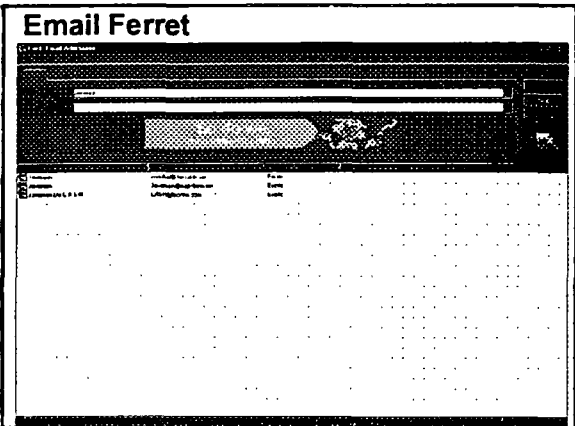
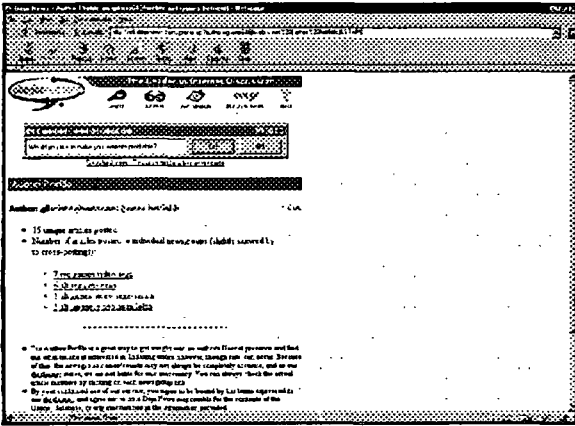
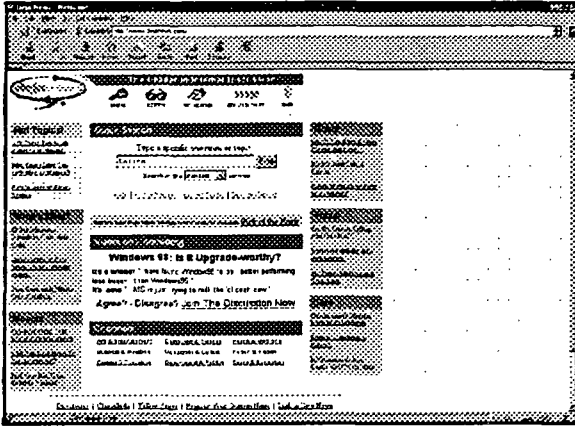
If you have questions regarding privacy, please call us at: 1-800-4NUMBLED
 For more information visit us at: www.4numbled.com

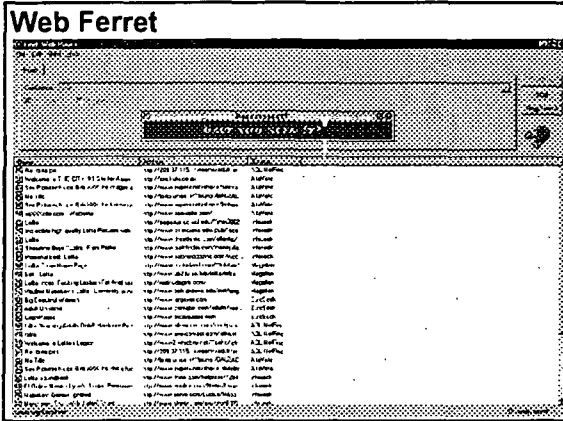
[Displaying matches 1 of 1]

Name	Address	Phone
William H. Cavigley	1401 W. Chippewa St., Apt. 101, Oak Brook, IL 60121-2801	(630) 572-4325

[Displaying matches 1 of 1]

© 1999 Database America, Inc.
 All Rights Reserved.





Unix

A basic understanding of the Unix operating system will go a long way to making your computer related investigations much simpler. Recommended texts include Unix for Dummies and Unix for MS-DOS Users.

Last

The last command will provide you with the logins for users on a particular system. The syntax is last username.

```

# last root
root    pts/0    s119-32-181-78-1  Sun Jun  7 14:19  still logged in
x11root pts/0     ppp827-twev.laje  Sun Jun  7 11:53 - 12:55 (01:03)
x11root pts/0     ppp827-twev.laje  Sun Jun  7 11:40 - 11:58 (00:01)
xconr1r ftp      s01-149.ec1isp.  Sun Jun  7 11:20 - 11:20 (00:00)
jaccu  ftp      882.ACQUA.COM    Sun Jun  7 07:21 - 07:22 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sun Jun  7 05:57 - 06:07 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sun Jun  7 05:07 - 05:07 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sun Jun  7 02:02 - 02:02 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sun Jun  6 23:30 - 23:35 (00:05)
jaccu  ftp      882.ACQUA.COM    Sat Jun  6 19:31 - 19:32 (00:00)
x11root pts/0    s119-32-188-158- Sat Jun  6 07:13 - 07:27 (01:14)
jaccu  ftp      AM2.ACQUA.COM    Sat Jun  6 07:01 - 07:02 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sat Jun  6 00:15 - 00:15 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sat Jun  6 02:05 - 02:05 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sat Jun  6 02:02 - 02:02 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sat Jun  6 02:02 - 02:02 (00:00)
jaccu  ftp      AM2.ACQUA.COM    Sat Jun  6 02:02 - 02:02 (00:00)
xconr1r ftp      0088.slaff.lajer Fri Jun  5 19:42 - 19:44 (00:02)
xconr1r ftp      005-129.ec1isp.  Fri Jun  5 17:48 - 17:52 (00:03)
jaccu  ftp      882.ACQUA.COM    Fri Jun  5 17:31 - 17:32 (00:00)
jajj   ftp      100-20.127.27   Fri Jun  5 17:15 - 17:15 (00:00)
jajj   ftp      100-20.127.27   Fri Jun  5 17:14 - 17:14 (00:00)
jaccu  ftp      200-148.64.8    Fri Jun  5 17:12 - 17:14 (00:01)
  
```

Electronic Records

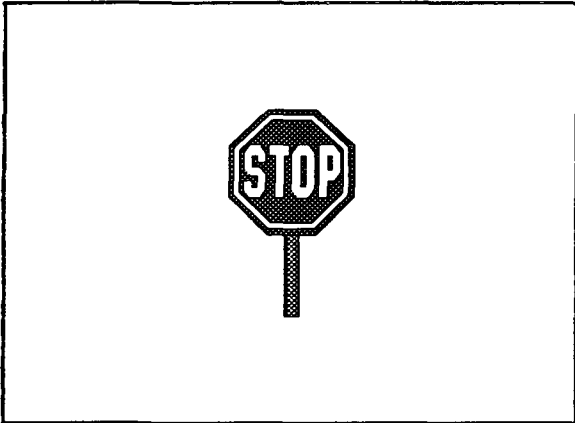
- Account start and disconnect dates
- Billing/Credit card information
- Screen names or nicknames used
- Violations or complaints on record
- Terminated or active (current) account
- LOGS : connecting/disconnecting times
- IP info...Internet Protocol Addresses

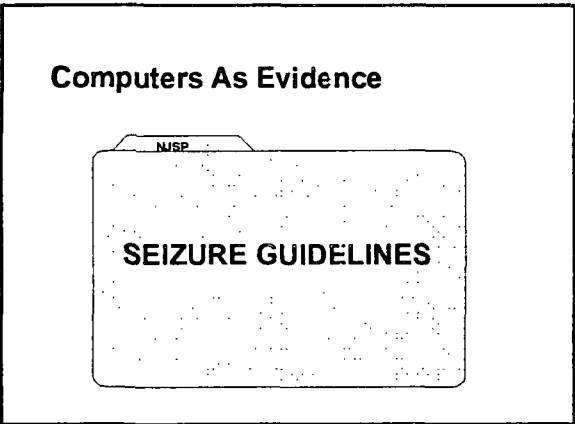
Investigative Methods

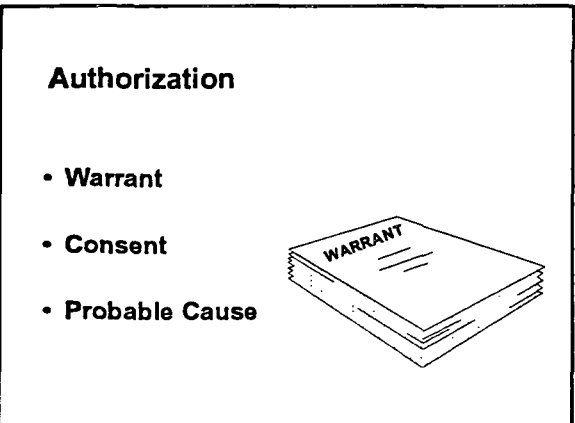
- Physical Surveillance
- Victim-Witness Interview
- Pre-text phone Call
- Pen Register
- Electronic Surveillance
- Undercover Approach
- Informant Contact
- Sting Operation
- Advanced Techniques (sniffers,datascoptes..)

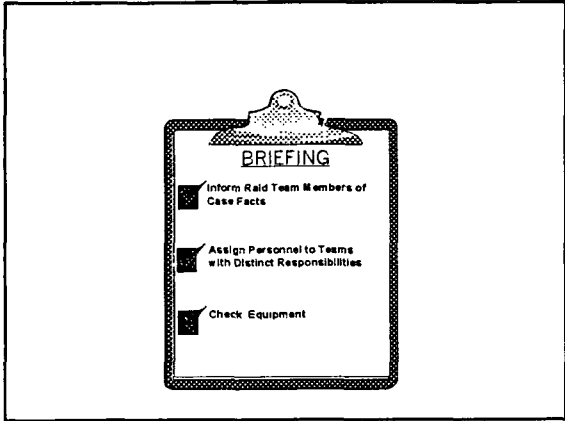
Keys to Success

- Preservation of Evidence
- Swift action to collect electronic audit trails ("electronic bloody foot prints")
- Focus on identifying the actual violator behind the internet address
- Exploiting corroborative computer evidence
- Support, resources and time...



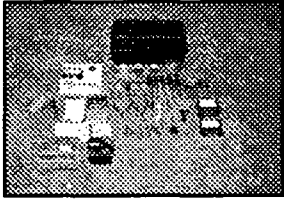







Raid Preparation: Tools

- Screw drivers
- Wire Cutters
- Hammer
- Cables
- Floppy disks (color code)
- Floppy Sleeves
- Batteries (CMOS, regular, etc.)
- Software
- Magnetometer or compass
- Laptop computer
- Cameras



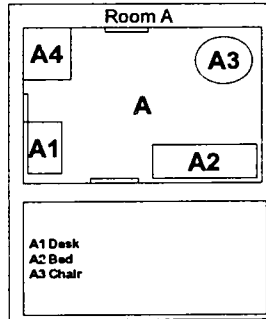
Executing the Search

- Secure the Premises
- Organize the Scene
- Photograph the Scene

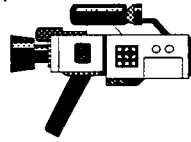


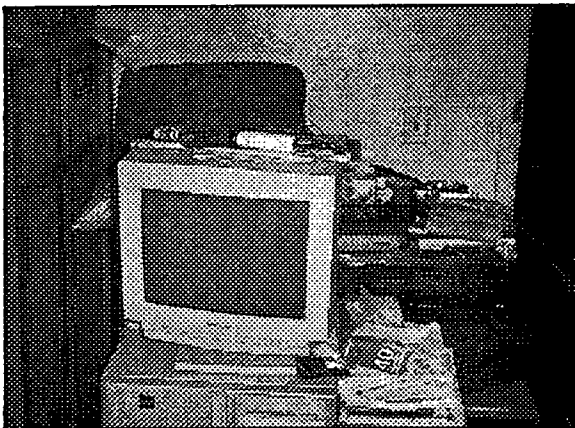
Organize the Scene

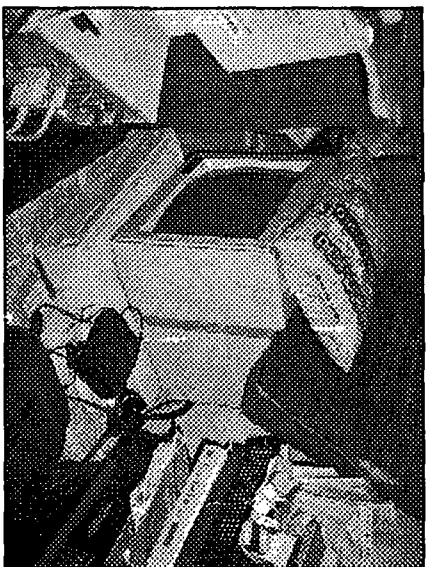
- Diagram the Site
- Label Rooms
- Sub-Label Components

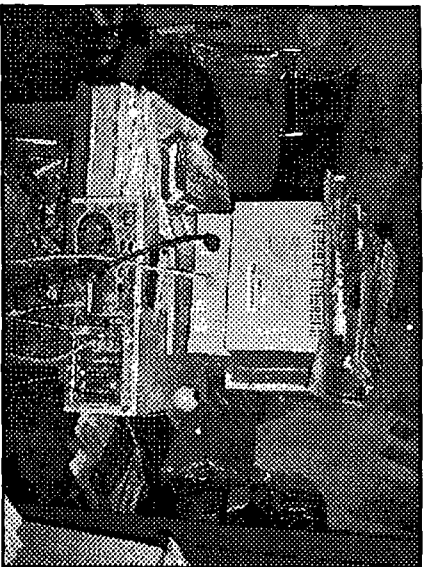


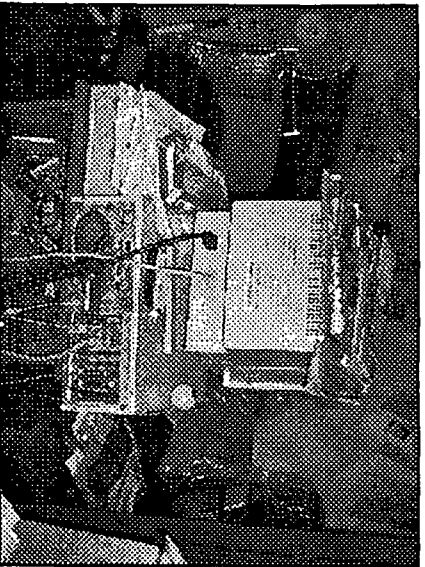
- ☒ Chair, Stools
- ☒ Holes, Doodies or Paper, Hair, Computer
- ☒ Boxes, Boxes, Boxes, Manuals
- ☒ Computer and a 1
Cable, etc.

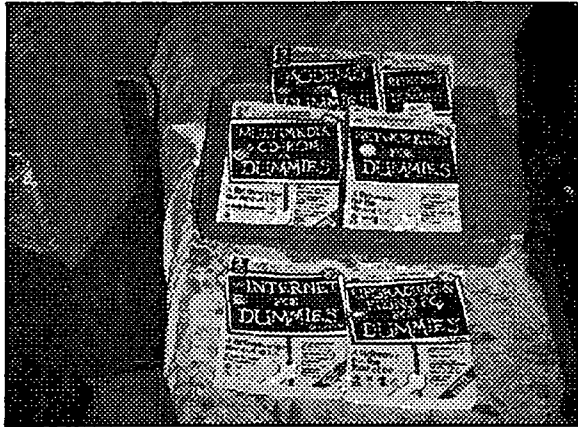


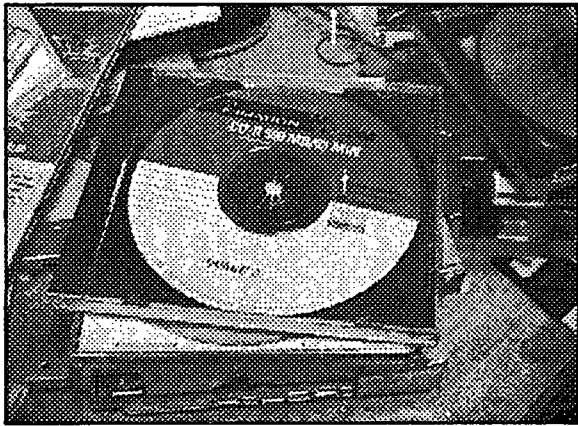












A LITTLE KNOWLEDGE CAN BE DANGEROUS

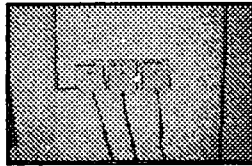
- Sophisticated computer users can easily bobby trap the computer with destructive programs. These programs are intended to destroy evidence. Safeguard the computer, prevent anyone from taking a quick "peek" that could engage these destructive devices.
- Additionally, evidence can be retrieved after destructive means have been used to attempt to destroy evidence, but the retrieval hinges on the safe recovery methods that are performed in the lab.

WHAT ITEMS TO LOOK FOR

- Radio Scanners.
- Telephone access devices.
- Hacking Literature.
- Software to facilitate the crime.
- Credit Card receipts/list.
- Storage Devices: Zip, Jaz, Sysquest or Tape Drives
- Credit Card readers.

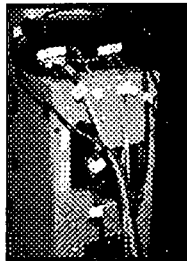
Processing the Scene

- Disconnect modem lines from wall, note numbers.
- Disconnect phone lines from wall.
- Photograph the entire crime scene.
- Photograph monitor if on.
- If a diskette is in a drive, don't touch, seal with tape to prevent removal.



Processing the Scene

- Cover keyboards with cardboard to protect keys.
- Photograph and diagram wiring.
- Tag both ends of all wires. Tag wire ends even if not connected.
- Tag components and record ID information.



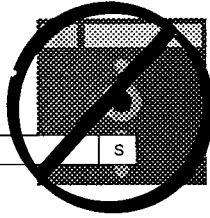
PROCESSING THE SCENE

- Only disassemble to facilitate transport.
- Pack and pad components in boxes.
- Label ends of boxes.
- Look for indicia of ownership.
- Leave copy of inventory and warrant with owner.



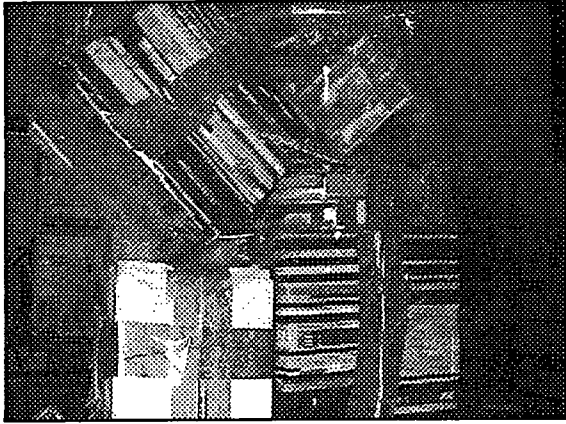
Transportation and Storage

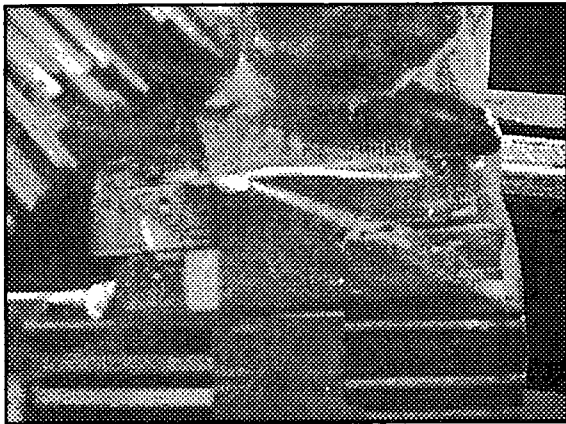
- Don't transport near radio antennas or power supplies.
- Keep media away from electromagnetic fields.
- Store in dry, clean location with moderate temperature.
- Store floppy disks in sleeves and inside disk storage containers.
- Clearly label components with a "DON'T TOUCH OR OPERATE" warning.



WHAT NOT TO DO

- Do Not Unplug Memory Phones, Fax , or Modems From Power Source !
- Never examine or turn on/off Computer.
- Note: If situation warrants turn off computer by pulling plug from rear of computer.

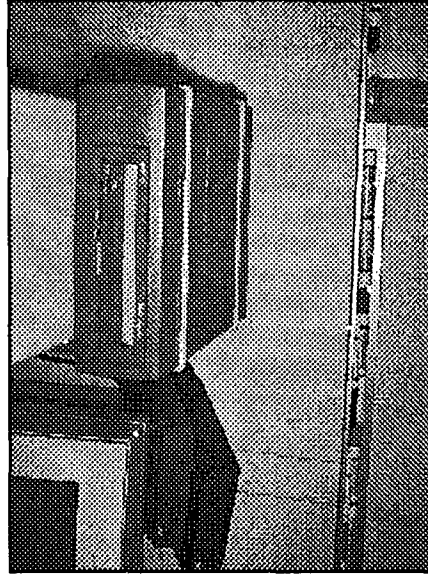
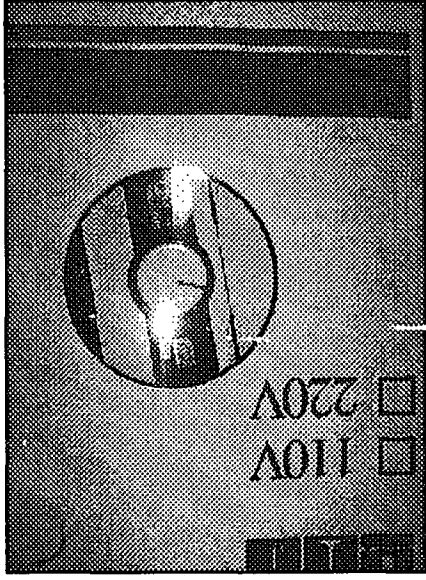
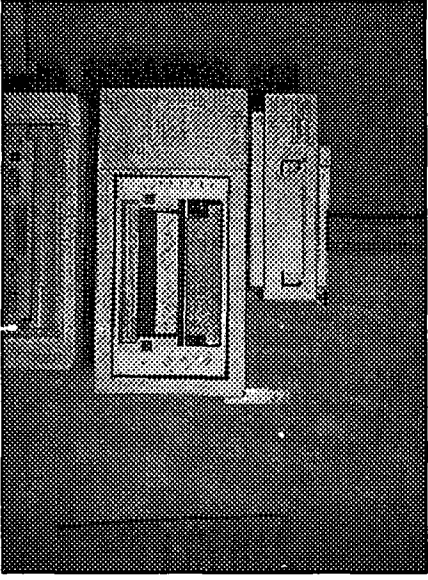




Storage Devices and Magnetic Media

- Used to store digital information
- May be part of the computers system unit or a separate peripheral
- Consists of a device to read and write the data and a magnetic media to store the data on.
- Capacity measured in the amount of bytes of information they will store

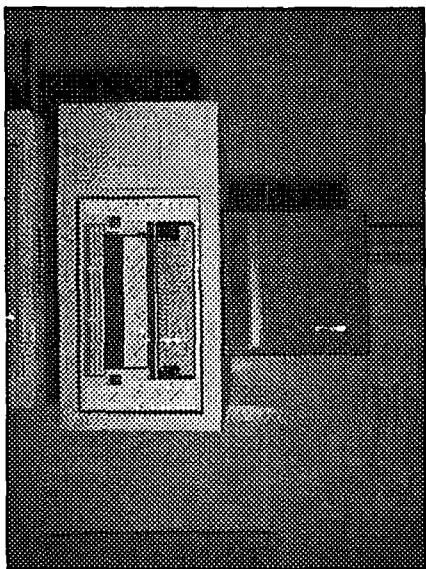
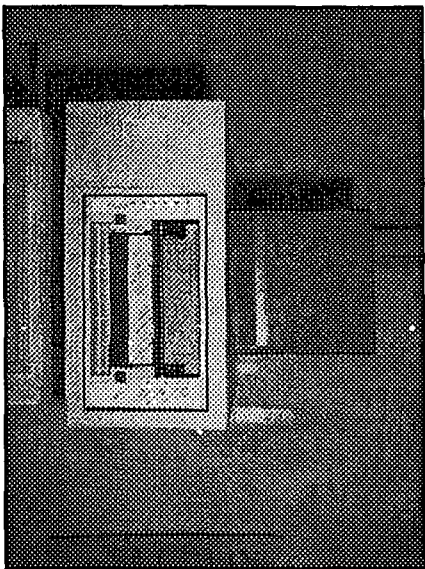
PCO 12



Vertical lines for notes.

Vertical lines for notes.

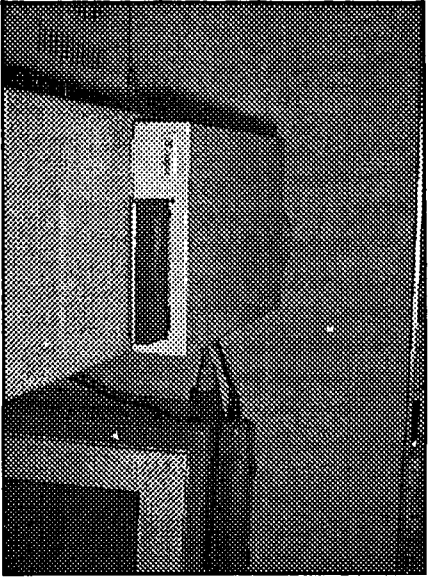
Vertical lines for notes.

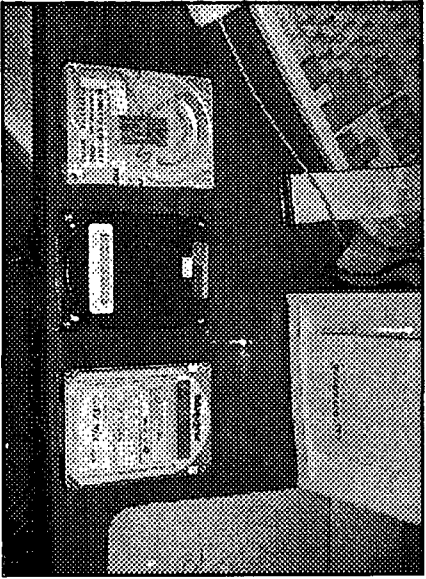


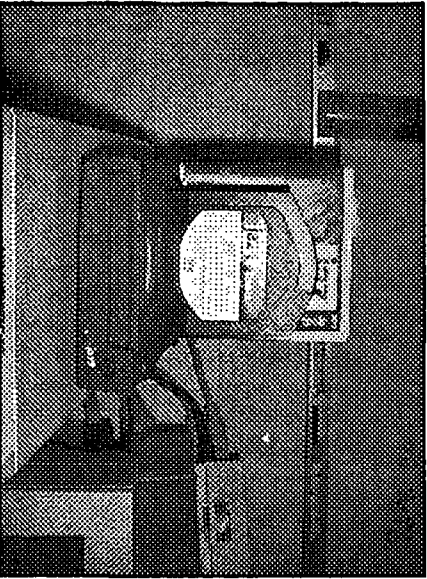
Vertical lines for writing.

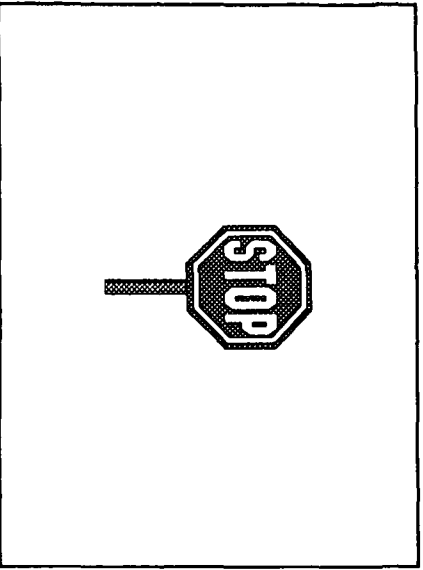
Vertical lines for writing.

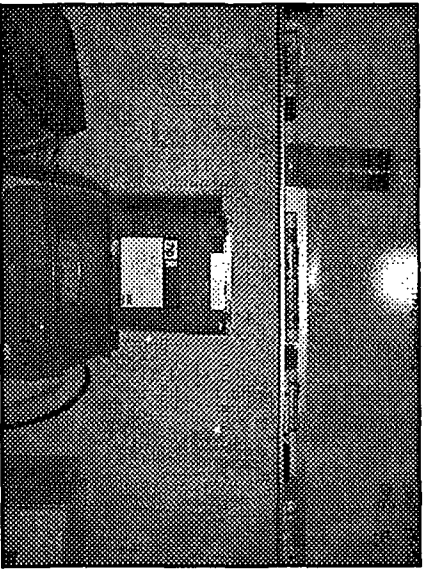
Vertical lines for writing.

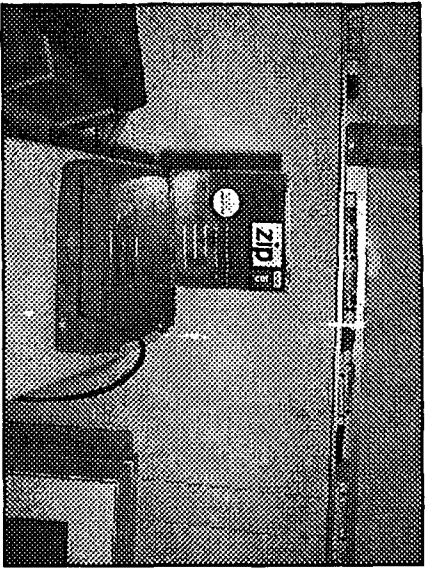












With an average picture size of 50,000 bytes

- You could store 20,000 images on one jaz drive
- You could store 400,000 on a DAT tape

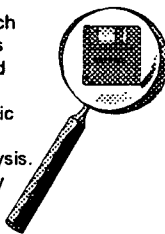
ecob

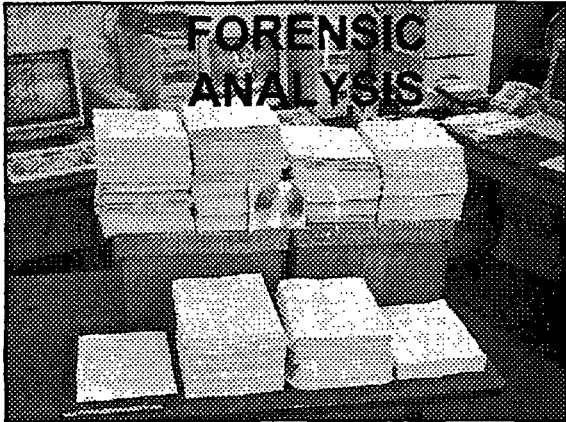
SUBMITTING EVIDENCE FOR ANALYSIS

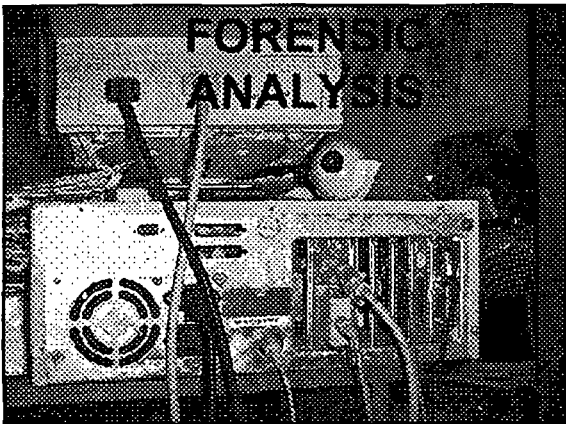
- Identify by serial number and mark all equipment vouchered. Count the floppies and categorize!
- Prepare Request for Laboratory Analysis and Letter of Transmittal.
- Attach copy of search warrant, subpoena or consent.
- Fully describe incident and be specific about the information you need retrieved.
- Remember, The forensic analyst has no knowledge of your case.
- There is no "Evidence key" on the computer.

Forensic Data Analysis

Forensic Data Analysis is the process in which computer evidence is analyzed. This process requires specialized tools and equipment and an advanced knowledge of computer and operating systems. In order to have electronic evidence admitted in court, the analyst must prove that he is qualified to perform the analysis. In addition, the analyst must be able to testify to the fact that the integrity of the evidence has been maintained throughout the chain of custody and analysis process.







Courtroom Presentation

- You may have to educate a judge and jury
- Use standard terms, Microsoft Dictionary
- Expect the unexpected!
- Can you rebuild offenders' system, prove it worked?
- Video Capture devices to prepare videotapes
- Will the defense hire their own expert?
- What is level of expertise of your examiner?
- Will you be able to present policies?

Help on the Technical Front

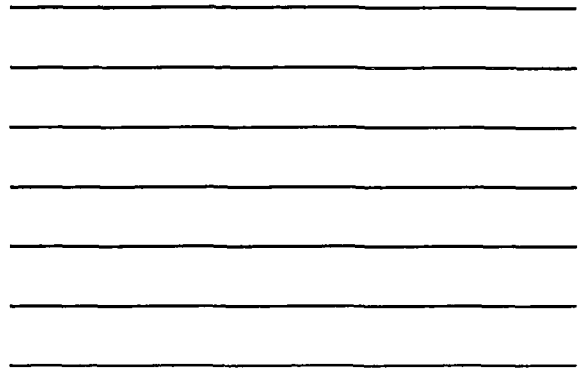
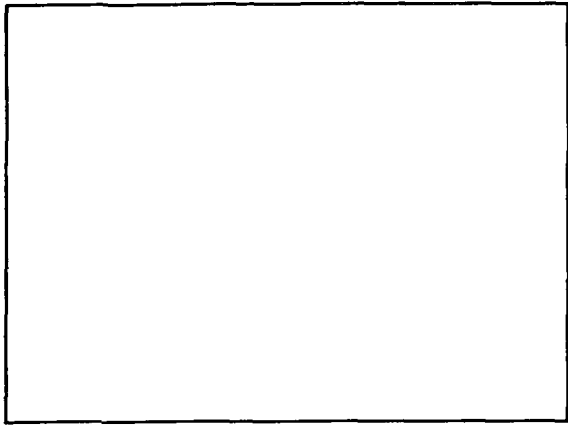
- Northeast Chapter of the High Technology Crime Investigators Association (www.ne-htcia.org)
- International Association of Computer Investigations Specialists (www.iacis.org)

Bibliography

- Netscape Communicator (www.netscape.com)
- Eudora Mail (www.eudora.com)
- Deja News Newsgroup Search Engine (www.dejanews.com)
- Webferret; Mailferret, NewsFerret, (www.ferretsoft.com)
- Netlab (www.eb.uah.edu/~adanil)
- Mirc (<http://www.mirc.co.uk>)
- Free Agent (www.forteinc.com)
- Quickview Plus (www.inso.com)

CONTACTING US

- **Sergeant James Doyle**
 - New York City Police Department
 - Computer Investigations & Technology Unit
 - (212) 374-4247 Fax: (212) 374-4249
 - jrdoyle@ix.netcom.com
- **Sergeant Michael Geraghty**
 - New Jersey State Police
 - High Tech Crime Unit
 - (609) 882-2904
 - mtg4385@ibm.net





High Technology Crimes Unit

On-Line Undercover Operations Guidelines

The following procedures and protocols are being introduced as guidelines at this time in an effort to standardize the approach to the investigation and prosecution of cases developed On-Line. Internet and On-Line investigations and the fact that this area of law enforcement is an extremely new area of law and is subject to challenges both by the defense and the Courts, these guidelines will serve this unit and the law enforcement community by setting standards that will. As we pursue our investigative objectives, we must continue to show a good faith effort in investigating these cases in the absence of any established case law in the area. These guidelines are to be followed in all cases involving undercover Internet or On-Line operations. Any deviations from these guidelines can be made on a case by case basis as investigative situations arise.

Overview

RECORD KEEPING PROTOCOL

Undercover Participation Record Keeping:

All members **MUST** document the date of each and every undercover activity, the type of activity (i.e. America OnLine, Compuserve, Internet, etc.), the case number or operation name, the name and badge number of the member, the undercover identity used for each instance, and the time on and off for all undercover activity. Each unit engaging in undercover on-line investigations will be responsible for maintaining said logs. Separate entries will be made for each area of undercover activity (i.e. individual entries are to be maintained for activity on America Online, Internet Relay Chat, etc.). Example entries are attached.

Online Activity Record Keeping

Officers **MUST** maintain complete records of all online activity. Officers will utilize the software relevant to the communication software they are using to log online activities. These programs are referred to as "logging" programs. For America Online activity options for both chat and session logging will be utilized, Both types of logs document all user interface with the activity occurring in the

computer program and all other online activity. For Internet Relay Chat, software, specifically MIRC, a logging option exists and should be turned on to record all activities. All logs are started after the initialization of the INTERNET programs, but before any online activity occurs.

File Naming Convention (Logs)

All on line activity, for each session will be logged to a clean 3.5" diskette. Volume label of the diskette should reflect case# to differentiate it, use the DOS "label.com" command. The diskette will be inserted into the A:\ drive prior to sign on. Once the logging option is enabled the log files will be named accordingly:

- 1) Chat log will be opened and named (A:\(Date of activity)"chat.log" - i.e. 0123ch01.log); -Multiple sessions on the same date can be indicated by adding to the final digit of the filename and stored in the appropriate directory
- 2) Session log will be opened and named (A:\(Date of activity) "sess.log" - i.e. 0123sn01.log) Multiple sessions on the same date can be indicated by adding to the final digit of the filename and stored in the appropriate directory
- 3) Log Instant Messages box will also be checked to log instant message chat between undercover Troopers and targets. There should be a check mark in the box to indicate enabled.

After the undercover activity is completed and prior to signing off AOL, the undercover officer MUST CLOSE ALL LOGS BEFORE EXITING THE PROGRAM. This will enable the log file to be written to the floppy diskette. The disk is then write protected by opening the write protect notch on the floppy diskette located on left side of diskette. The disk is then re-inserted into the a:\drive and copies of the logs are made to the C:\OLI\OLLOGS (On Line Investigations, On Line Logs) directory on the hard drive for later use in investigative activity. The floppy disks are once again removed and are then filed in a locked filing cabinet. The placement of these floppy disks into storage is noted by the creating officer in a hard copy notebook documenting the floppy disk label, date and the accessing officer. These floppy disks are never accessed again, but are maintained as original recordings. The label of the diskette will indicate filenames stored on disk, case#, date and investigator. **If there is no diskette, it did not happen.**

Instant Messages

It is common for undercover officers and targets to converse on line using the Instant Message (AIM@) function of AOL. When ever IM's are used to converse electronically with a target, a record of such conversation should be made for ease of accessing this information for later investigation needs. It is not mandatory because the information is also recorded through the overall logging function previously described in this memo. The process of recording and saving the IM's is as follows:

- 1) While an IM box is open and the undercover officer is conversing with a target, it is important that the IM box remain open throughout the entire conversation.
- 2) The IM box can be minimized but should never be closed or portions of the entire conversation will not be saved.
- 3) Once the conversation has concluded, the text of the box should be highlighted and the file - saves as - function invoked.

The file should be named as follows:

("IM(target name).log") - i.e. IMRUDO99.log.

The file will default to the a:\ drive because all other chat and session logs are all ready being saved to that drive. Upon completion of the undercover activity, these files should be printed out and put in the appropriate case files for reference by the assigned investigator preparing the search warrant.

Directory Tree Structure

The following directory tree format on the investigative computer hard drive will be implemented to aid the investigators in evidence collection and retrieval. The directories and sub-directories are logically established on the hard drive. The Directory Tree structure is as follows: C:\..

\OLI

\98-01 (Case Number Designation) were copies of all logs are kept.

SCREEN NAME of TARGET- 0 byte file

\Images - Images received are stored

\LOGS-

\TO - All E-mail sent to Target by U/C

\FROM - All E-mail received from Target

\TXT -Text E-mail messages provided by
AOL

\Inactive

Screen names- 0 Byte files

SAR FILE outline prelim and closing

\

E-Mail Download Record Keeping

When e-mail is generated by on-line activity, the downloading of the resulting messages is specifically recorded. E-mail generally arrives in two forms-text messages, and text messages accompanied by computer generated graphics. In either case, the text messages are recorded in the same way. Prior to any email downloading, the downloading officer MUST first establish target directories and sub directories in the appropriate manner as described above. The actual downloading and record keeping for graphics is described in the following section.

A hard copy notebook in which the downloading officer MUST record his/her name, the date and time of the downloading, and the undercover name of the account that is downloaded. The downloading of text messages and text messages that also include an attached computer generated graphic image is done using the logging option of the program from which the mail was generated. Before beginning the downloading activity. **This E-Mail log is created by opening the "Session Log" option on AOL.** In addition, the downloading officer should check the Log Instant Messages box in the event other targets IM the downloading officer during the download process. The log file is saved to the computers hard drive and the following name is given to the file:

C:\OLI\CASE NUMBER\ (date of download) "email.log" - i.e
1223emai.log.

The downloading of computer graphic image files are directed to the target APICS@ sub directory responsible for its transmission. Often times, a target will send the same computer graphic image on more than one occasion. Each transmission of the computer graphic by the target is potentially a felony violation. Accordingly, each picture needs to be saved regardless of how many times it is sent. If the computer prompts the download officer that a "File Already Exist" in a targets subdirectory, the downloading officer will create a new sub directory under the APICS@ sub directory named "DUPES." Each time the computer prompts the downloading officer that a "File Already Exist" a new sub directory will be created (DUPES2; DUPES3; etc).

In addition each E-mail message which accompanies the graphic image MUST be saved in the target "From" sub directory. All E-mail associated with a particular target can later be printed by the investigator assigned to the search warrant application or can be printed and forwarded to the appropriate law enforcement agency upon a referral.

Contact with Targets through E-mail

At times it is necessary to further contact targets and engage them (him/her) in further E-mail conversation. When ever an undercover officer sends an E-mail to

a target, that activity MUST be recorded and saved. In addition, any E-mail response from the target MUST also be recorded and saved. Accordingly, when ever an E-mail message is sent to a target, the message will be saved in the following manner using the **File - Save As** function:

E-MAIL SENT TO:

C:\OLI\CASENUMBER\LOGS\TO.

The name of the file will be in the following format: (first 2 letters of name, date, "TO.doc") - i.e. TA1223TO.doc.)

E-MAIL RECEIVED FROM:

C:\OLI\CASENUMBER\LOGS\FROM.

The name of the file will be in the following format: (first 2 letters of name, date, "FR.doc") - i.e. TA1223FR.doc)

NOTE: In many instances, numerous E-Mails are received from the target by the U/C on the same date. The file will be named with alphabetical letters a,b,c,d, etc. to denote multiple E-Mail message occurring on one date, i.e. TA1223Fa.doc.

All E-mail contact between the undercover and the target should be printed out and put the case folder for reference by the assigned investigator preparing the search warrant.

Seizure/Analysis of Evidence

It is the standard operating procedure of the undercover operation that no illegal files of any kind are ever transmitted, only received. Based on the reception of these files, search warrants are sought to search for the computer or related computer storage device that holds the file that was originally used in the transmission to the undercover. These computers or computer storage devices are then forensically searched by a computer forensic investigative specialist for evidence or presence of these files.

Additional equipment is used for the analysis of seized computers. The originals must be secured as evidence and a "cloned" hard-drive created to function as a working copy. At least one hard drive with memory capabilities similar to that set forth earlier in this memo must be obtained for this purpose.

COMPUTER CRIME SCENE CHECKLIST

- Label Each Room-
- Sub-Label the components in the room
- Diagram the Site
- Assign Areas of responsibility
- Photo or video the entire scene
- Photo or video any notes, doodles or papers near the computer
- Photo or video the computer, from all sides
- Set Up Laptop with Seized Items Database
- Check the scene with a compass or magnetometer
- When seizing evidence carefully note its location
- Test phone jacks for tone and retrieve number
- Seize software and manuals you will need to process evidence- especially proprietary or non-mainstream software
- Seize notes, scribbles, and notebooks, concentrate on area around computer work area
- Check for concealed compartments
- Tag both ends of cabling
- Record component identifiers, mark evidence with no serial numbers
- Transport

This list is not all-inclusive.

Source: SEARCH, Inc. reprinted with permission

CRIME SCENE TOOL KIT

- **Screwdriver-** Phillips for cases
- **Screwdriver-** Small Slotted for peripherals
- **Small Diagonal cutters-**cutting nylon wire ties
- **Rubber bands-** to wrap cables to facilitate transport
- **Color Tape or Coded Buttons-** for tagging cabling and terminus
- **Small Scissors-** for cutting tape
- **Wire Ties-** to wrap cables to facilitate transport
- **Boxes-** for transporting
- **Digital or 35 mm Camera-** To record Crime Scene, screen capture
- **Indelible markers-** for marking
- **Evidence tags-** Adhesive, can be pre-made with software
- **Bootable Floppies-** Should only be used in presence of experts, at minimum should have disklok and autoexec.bat modified to load on boot.
- **Rubber Gloves-** to preserve latents and as a health precaution
- **Tape-** Masking, Plastic
- **Evidence tape-** To secure floppies and CD-ROMs in computers
- **Packing material**
- **Standard Telephone-** to check modem lines
- **Video camera**
- **Hammer or nail puller-** to remove cable fasteners
- **Laptop-** On large seizures a database can facilitate logging
- **Power Strip-** for investigator use if bringing laptop and printer
- **Batteries or power adapters for electronic equipment-** especially cell phones

This list is not all-inclusive.

Source: SEARCH, Inc. reprinted with permission

Internal Parts Inventory Sheet

(HTCU Use Only - Detail of Inside Components)

Division Case #	HTCU Case #:	Submitting Agency Case #:	Rank/Name:	Badge #:
-----------------	--------------	---------------------------	------------	----------

Computer Description:	Evidence Tag #:	Date:	Signature:
-----------------------	-----------------	-------	------------

Item	Qty	Computer	MB		Manufacturer	Model #	Serial #
		Fixed Drive					
		Fixed Drive					
		Fixed Drive					
			Occupied				
			YES	NO			
		Slot 1	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 2	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 3	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 4	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 5	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 6	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 7	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 8	<input type="checkbox"/>	<input type="checkbox"/>			
			<input type="checkbox"/>	<input type="checkbox"/>			

Additional Comments: (switch settings, markings, listing of bad tracks, monitor switches, etc.) (Continued comments on back or continuation sheets)

Raid Site - Inventory Worksheet

(Search Warrant Site or Initial Inventory of Computer and all Peripherals)

Date:	Case #:	HTCU Case #:	Crime(s)
Start Time:	End Time:		Victim's Name: (Known to Department)
Rank/Name	Badge Number:	Dept Name:	
Unit	Unit Code	Location of Search/Seizure (Street Address, Apt. #, City, State)	
Inventoried By (Rank/Name/Badge #):		Submitted By (Name and Badge #):	Phone Number
Signature:		Submitting Agency	Submitting Agency Case #:

Yes	No	Question
<input type="checkbox"/>	<input type="checkbox"/>	Was the computer running at the time of Seizure?
<input type="checkbox"/>	<input type="checkbox"/>	Was the screen of the computer photographed?
<input type="checkbox"/>	<input type="checkbox"/>	Was the computer unplugged at the power supply?
<input type="checkbox"/>	<input type="checkbox"/>	Were the computer location & connections photographed and labeled?
<input type="checkbox"/>	<input type="checkbox"/>	Were Safepark Diskettes put in all the diskette drives?
<input type="checkbox"/>	<input type="checkbox"/>	Was it booted after Seizure?
<input type="checkbox"/>	<input type="checkbox"/>	If booted, were control disks used?
<input type="checkbox"/>	<input type="checkbox"/>	Was computer connected to modem?
<input type="checkbox"/>	<input type="checkbox"/>	After disconnecting from wall jack, was line checked for tone?
<input type="checkbox"/>	<input type="checkbox"/>	Was phone line checked for # (958) and traced to computer? LIST NUMBERS BELOW
<input type="checkbox"/>	<input type="checkbox"/>	Was computer case opened (List additional comments on back of this sheet)?

Voucher #	Peripheral	Markings on Front	Manufacturer	Model #	Serial #

Comments:

INTERNET SERVICE PROVIDERS

NETCOM:

- **Basic wording for subpoenas**
- **IP Address: "all account information with the following IP address on**
 - **DATE**
 - **TIME** Include the time zone of target computer, Netcom records are maintained in Pacific Time.
- **User name-**
- **Make sure non disclosure is on face of subpoena**
- **User can set software to delete messages off server as soon as they are downloaded. If user doesn't set it that way, Netcom will save most recent 5 MB of space.**
 - **FAX# 408-881-3050**
 - **Legal # 408-881-3026- Also for Search warrants which are required for e-mail text and headers**
 - **They will honor letters to preserve**

AOL

- **Read e-mail will remain on AOL servers for three to five days after user reads it; however they can be remarked new and stay for five more days**
- **Unread e-mail stays for 5 days, at which time AOL purges it**
- **Notify AOL immediately if e-mail is evidence**
- **Screen names can be subpoenaed for**
 - **subscriber info**
 - **Name and Address**
 - **Other Screen names**
 - **Last Session**
 - **Billing Info**
 - **IP address log ins**

HOTMAIL- Now owned by Microsoft

Yahoo:

408 731 3300

Address Subpoenas to:

John Place

3400 Central Expressway

Suite 201

Santa Clara, CA 95051

IP Addresses can be disclosed only for classifieds

INVESTIGATIVE ANALYSIS REPORT

To: Detective XXXXXX
Unit Name)
From: Forensic Analyst
Computer Investigation Unit
(Unit Phone Number)
Date: Date
Re: EXAMINATION OF EVIDENCE UNDER INVOICE# xxxxx LAB# xx/97

SUMMARY

I have examined and analyzed investigatory evidence submitted by Detective XXXXX of Vice Enforcement Squad and itemized on Property Clerk's Invoice number xxxxx. All items referenced were marked in the format CIU-xx. My findings are as follows:

➤ THIS SYSTEM DID CONTAIN ELECTRONIC IMAGES FILES OF CHILD PORNOGRAPHY

A complete detailed Forensic Processing Report follows.

GENERAL PROCEDURES

The following outlines standard processing procedures used in examining all fixed and removable media:

1. The examining computer system is a Police Department owned DOS based Pentium 100 MHz CSS Lab PC, running under MS-DOS 6.22 and Windows for Workgroups 3.11. The operating system software is licensed to run on this computer. The system is equipped with one 5.25" floppy drive and one 3.5" floppy drive, both capable of reading/writing to both high and low density floppy diskettes. 1 6X CD-ROM drive (SCSI read only), 1 Pinnacle Micro CD-ROM writer (SCSI), 1 Iomega Jaz drive (1gig), 1 Iomega Zip drive (100mb), 2- 2 gig Internal Western Digital Hard drives (scratch). 1-Seagate 8000 tape drive. The video system is VGA and is capable of displaying at least 256 simultaneous colors at 640 x 480 dpi.
2. Diskettes measuring 5.25" are write-protected by placing an adhesive write protect tab over the write protect notch. Diskettes measuring 3.5" have their write protect notch opened. Both of these actions prevent any accidental writing to the diskettes by the examining system. In the event copies are needed prior to analysis, an exact image is made using **AnaDisk** version 2.08 by Sydex Corporation.
3. Prior to hard drive analysis an exact duplicate of the hard drive is made using Image MAsster 500 IDE, Intelligent Computer Solutions. In addition, an image of the original hard drive is created utilizing **Safeback** version 1.1 Sydex Corporation. The image files are archived to CD-ROM or tape for future reference.



4. *Note: Due to the fact that DOS assigns drive letters automatically, the evidence hard drive when attached to it's Central Processing Unit is normally drive C:, when the hard drive is removed and installed as a slave in a lab computer and disklok.exe is executed the hard drive is then assigned the next drive letter which would be D:, so therefore during the examination of the evidence drive and any screen captures are performed the drive letter would be D:.*

SPECIFIC FINDINGS

Comments and findings which resulted from the examination and processing of all submitted hardware and software follows. Findings have only been provided regarding diskettes or files, which either contain relevant information or was specifically requested by the investigator.

Hardware

Invoice xxxxxx, Item #2, is a TriGem computer serial number QS133002539 containing a single IDE Conner CFS1621A 1548-MB hard drive and 16MB RAM. The embedded serial number for this drive is FJBBNA2. The computer was properly set up and no attempt was made by the owner/operator to conceal data through the use of passwords, data encryption or manipulation of the operating system. The system date and time were correct. Drive parameters in CMOS are 16 heads, 3146 cylinders and 63 sectors with a normal geometry.

Physical Analysis

1. The investigatory drive was installed on forensic lab computer #2 and set up to be the slave IDE drive.
 - A virus check was performed with negative results, report saved as "\reports\fp5797.txt..
 - The AUTOEXEC.BAT and CONFIG.SYS files were examined. The files were normal and there were no lines REMarked out as to indicate special settings for programs that no longer resided on the computer.
 - *Fdisk* was executed and reported one 100% DOS partition. The DIR command was executed and generated the directory listings then saved to file DIR5797.TXT and saved to a directory "\reports".
 - Norton's *Unerase* was used to Unerase any recoverable files. Erased files were recovered and saved to a folder "\erased". Files of evidentiary value consisting of electronic images were recovered and printed as CIU#1, a directory listing of files recovered was compiled as "\reports\direras.txt".
 - The following files specifically requested by the investigator were found to reside on the subject computer's hard drive:

<u>FILE:</u>	<u>DIRECTORY</u>	<u>CIU#</u>
♦ Rik1.jpg	C:\PONTIAC	CIU#2
♦ Rik2.jpg	C:\PONTIAC	CIU#3
♦ Rik3.jpg	C:\PONTIAC	CIU#4
♦ Rik4.jpg	C:\PONTIAC	CIU#5
♦ Cumshot.avi	C:\AUDI	CIU#6
♦ Stand. avi	C:\AUDI	CIU#7



- CIU#6 and CIU#7 are windows based video files (.avi) which are digitized movies
- CIU#6: 97 frames of a male masturbating
- CIU#7: 178 frames of a male masturbating.

A search was made for Joint Photographic Experts Format (JPG), Graphics Interchange Format (GIF), Tagged Image File Format (TIF), UNIX to UNIX Encoded (UUE) or Bit Mapped Images (BMP, RLE) for pornographic images with positive results.

The following subdirectories contained pornographic images or movie files, not all files were of a pornographic nature.

VAUDI	36 AVI files	CIU#8
\CORSICA	2 JPG files 1AVI files	CIU#9
\GALLON	18 MPG files	CIU#10
\PONTIAC	986 files, (GIF, JPG)	CIU#11
\USERS	270 files, (BMP, GIF, JPG, PCX)	CIU#12
\WORKDESK	5 files (JPG, GIF)	CIU#13
\X-CELEBS	23 files (JPG, GIF)	CIU#14

The directory listing of the above subdirectories were printed and labeled as shown. All of the images were printed as 1" X 1" thumbnail image files and attached to the directory listing. All of the above items have been archived to the CD-ROM accompanying this report.

The files in \Gallon were ".MPG" and in order to print a sample a screen capture program was utilized to capture the first frame of each movie file.

The hard drive was searched for text files or evidence of electronic communications detailing sexual relations between adults and children. It is noted that the subject computer had the following Internet related software installed:

- Netcom- software to connect to the Internet
- Mirc, New MIRC, software enabling one to electronically chat on the internet
- Quickcam, CuSeeME,- software when used with a computer attached camera can send realtime video over the Internet to another individual
- Microsoft NetMeeting- software utilized to set up an electronic conferencing between individuals computers

\PROGRAMS\NETMEETING\RECEIV~1\	3 JPG files
\PROGRAMS\NETMEETING\SPEEDD~1\	5 CNF files
\WINDOWS\DESKTOP\MYBRIE~1\	3 TXT files

Above printed as CIU#15.

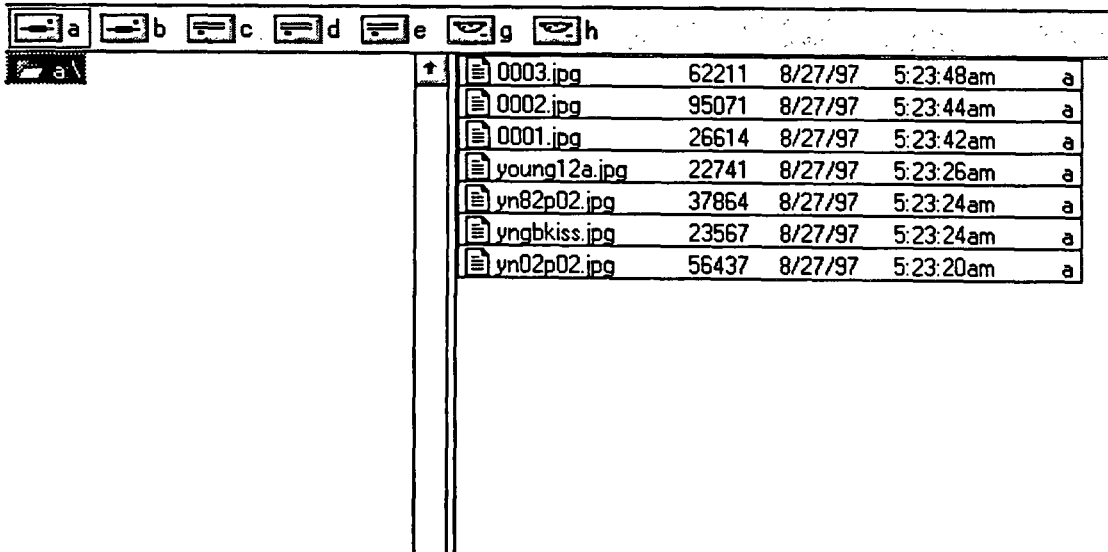


The following directories yielded logs of electronic chats between the operator of the subject's computer and other individuals. A representative sample was reviewed which showed the conversations to be of a sexual nature directed towards minors. These logs are printed, with each file a separate record of the conversation, the files are separated by a separator page indicating the name of the file and the file creation date. A directory listing accompanies each directory output.

- LOGS IN DIRECTORY \newmirc\mirc CIU#16
- LOGS IN DIRECTORY \mirc CIU#17

2. Invoice H005108, Item #4, two beige 3.5 high density floppy diskettes, marked with shield #4152, identified as recovering officer, Detective Robert Chambers #4152 of the 52 PDU. These diskettes were marked CIU #57_97D1 and CIU #57_97D2. The disks were write protected and examined. Disk 57_97D1 was unreadable, DOS reporting an unrecoverable disk error. A copy of this disk was made with *ANADISK* and *Norton Utilities 8.0* was utilized to repair the disk. The following are screen captures of the directory entries for each disk: Each diskette contained images of child pornography.

DISK S7_97D1 (Recovered Disk)



File Name	Size	Date	Time	Attr
0003.jpg	62211	8/27/97	5:23:48am	a
0002.jpg	95071	8/27/97	5:23:44am	a
0001.jpg	26614	8/27/97	5:23:42am	a
young12a.jpg	22741	8/27/97	5:23:26am	a
yn82p02.jpg	37864	8/27/97	5:23:24am	a
yngbkiss.jpg	23567	8/27/97	5:23:24am	a
yn02p02.jpg	56437	8/27/97	5:23:20am	a

The above files were outputted and printed as CIU#18.

DISK S7_97D2

File Name	Size	Date	Time	Attr
co002453.jpg	29818	7/25/97	7:15:48am	a
chris3.jpg	4092	7/25/97	7:15:46am	a
chris4.jpg	10289	7/25/97	7:15:46am	a
bb49a.jpg	9192	7/25/97	7:15:44am	a
bb003046.jpg	27865	7/25/97	7:15:42am	a
b003.jpg	74313	7/25/97	7:15:38am	a
arcx0001.jpg	85709	7/25/97	7:15:36am	a
arc00030.jpg	33807	7/25/97	7:15:32am	a
arc00003.jpg	43504	7/25/97	7:15:30am	a
als-8903.jpg	43078	7/25/97	7:15:28am	a
akids12.jpg	49994	7/25/97	7:13:50am	a
akids11.jpg	84883	7/25/97	7:13:46am	a
ab-2.jpg	53142	7/25/97	7:13:44am	a
349.jpg	42418	7/25/97	7:13:42am	a
2bys9fuk.jpg	19072	7/25/97	7:13:40am	a
2boy2.jpg	24264	7/25/97	7:13:38am	a
14robby.jpg	33504	7/25/97	7:13:36am	a
13cam.jpg	60799	7/25/97	7:13:34am	a
11yrhd02.jpg	42086	7/25/97	7:13:32am	a
11-jerem.jpg	27650	7/25/97	7:13:30am	a
11asshol.jpg	12052	7/25/97	7:13:30am	a
10yold.jpg	20615	7/25/97	7:13:28am	a
08-18j.jpg	9550	7/25/97	7:13:26am	a
10boy11.jpg	24990	7/25/97	7:13:26am	a
0006-03t.jpg	25950	7/25/97	7:13:24am	a
0005.jpg	83586	7/25/97	7:13:22am	a
#boyhrd1.jpg	21110	7/25/97	7:13:20am	a
lnuts.gif	52144	7/25/97	7:13:18am	a
!2!b14~1.jpg	62652	7/25/97	7:13:16am	a

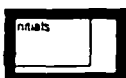
The above files were outputted and printed as CIU#19.

THE ABOVE IS A COMPLETE DESCRIPTION OF MY EXAMINATION OF THE SUBMITTED EVIDENCE.

END ANALYSIS

(Forensic Examiner)

(Supervisory Review)



mIRC has several features that may be used for this purpose. Most of the information it can obtain you must disregard as user configurable, but the DNS look-up feature is reliable. In mIRC's main/status window entry field, type "/dns" followed by the person's nickname, "/dns pedoperv" for example. Usually you will then see his lettered address on the Internet and the numerical equivalent. Every computer connected to the Internet has an IP address.

This information shows which Internet Provider the person is using, and it shows the person's individual address at that provider with his current connection. Coupled with the exact time, it will enable the Internet Provider to identify the person's account. With that information, they may even be able to review his past activity.

To discern the Internet Provider's name look to the last portion of the lettered address. For example, from "**** Resolved tpm229127.gte.net to 207.115.229.127" you can determine that the Internet Provider is "gte.net" otherwise known as GTE, the large U.S. phone company and ISP. If you only see a numbered address, no problem, the Provider's name can still be obtained from the first three segments of the address, as you will see near the bottom of the next paragraph.

To obtain the perpetrator's Internet Provider's contact information (for police investigative use or to determine which law enforcement agency to contact), use the On-Line Digger Engine to look up the email address, postal address, and phone number(s) of the contacts for that organization. Try entering "gte.net" to see how it works. If you did not get a lettered address when you did a /dns lookup with mIRC, you may still determine the Provider's name by entering only the first three segments of the numerical IP address, e.g., "207.115.229" of "207.115.229.127" would retrieve the same info as "gte.net." For the On-Line Digger Engine on our site, you may enter the whole IP numbered address.

If you are making a report to law enforcement and expect them to investigate the individual, make sure you send all the information and evidence you have on the perpetrator, including any logs of statements he typed, to the investigative police agency and/or Internet Provider. Do not send illegal child pornography to the provider. It is generally okay to give it to the police, but you may wish to contact them prior to sending it.

Consult PedoWatch's growing international list of investigative agencies that will investigate your report. Law enforcement officers, please do not drop cases because the perpetrators prove to be outside your jurisdiction. Forward the evidence to the appropriate contact. Report List:
<http://pedowatch.org/report.htm>

Type 2 Spammer: Careful clueless spammer/warez d00d, attempting pseudonymity

The key to identification of the pseudoanonymous perpetrator is finding as many "sharp edges" as possible to the post. By "sharp edges", we mean unique characteristics which can lead one to the real poster. Even messages posted via chained anon remailers can contain "sharp edges" (for example, in a distinctive signature used by the poster in a previous, non-anon posting). Remember, all the major web-spider based search engines (AltaVista, HotBot, Excite, Webcrawler) can search for absolutely any text on any web page...and some (AltaVista, DejaNews, Excite) can do so for the Usenet, as well.

Here's an example of a guy who thought he was posting "anonymously":

-----begin Spam quote-----
Path: ...!usenet.eel.ufl.edu!bofh.dot!news.atlantic.net!
ppp-gnv-fl-039.atlantic.net!user

From: DonJuanToupe@all.net (Don Juan Toupe)
Newsgroups: alt.binaries.slack
Subject: F*#K da police!
Date: 4 Jun 1996 04:19:54 GMT
Organization: lovegodz
Lines: 4
Message-ID: [DonJuanToupe-0406960138120001@ppp-gnv-fl-039.atlantic.net>
NNTP-Posting-Host: ppp-gnv-fl-039.atlantic.net

Let's get to trading

—

do it if it feels good.....

-----end Spam quote-----

Note hallmarks of Type II post: faked nym instead of real name, faked (usually somewhat humorous)e-mail return address, intact path, intact nntp posting host, *Unique fake organization name*, intact X-Newsreader line (usually; not so in this case).

Suggested approach depends on which "sharp edge" sticks out the most. Our goal is rapidly to get the perp's REAL name and city of residence; from this, all else (phone number, map to house, DMV records-- ha ha, only serious) can be obtained.

Why is the perp's real name important?

Why don't we just hand the case over to the ISP: "Some bozo calling herself zeus@mountolympus.com is spamming our site/newsgroup-- tell her to stop it."?

Consider: Most ISP abuse sysops are INUNDATED with requests from rank newbies for aid in persecuting/burning at stake UCE or Usenet spammers. Few of these requests give the sysop ANY sharp edges with which to start investigating the issue. If we, as good Netizens, have free mental cycles to burn on hunting down these scum, the enforcement action from the responsive ISP sysop can proceed IMMEDIATELY-- usually, one strongly-worded e-mail from the ISP sysop restating the ISP's TOS is enough to get most Type I and Type II spammers to swear off spamming forever (or at least to stay the hell out of our newsgroup).

Thus, one search scheme would be:

1) Do AltaVista and/or DejaNews search for bogus@name.com to look for times when the poster included her real name. Especially zoom in on alt.test.* hierarchy posts, as these may contain at least one instance of posting "in the clear" as the spammer fine-tuned her newsreader's configuration.

2) Do AltaVista/DejaNews search on any "sharp edge" that sticks out:
Example: This warez d00d (above) used the Organization: lovegodz on all of his Usenet posts. He forgot to remove same when posting pseudoanon to a.b.s. We searched for Organization: lovegodz (as well as for posts containing his sig), found all his posts to alt.baldness, and from thence found his narcissitic website, which was chock full of juicy personal information.

Other promising "sharp edges": trailing user name in path (...!news.foo.com!imamoron), funky newsreaders (ZippityDooDah News Alpha 0.9), unique sig components. Look hard. You are smarter than the Type II Spammer. The Force has power over weak minds.

3) What if the perp used "X-No-Archive: yes" in her headers and steps 1 and 2 have failed? You may get lucky, and find a follow-up to a previous post by the bad guy which was not posted without "no-archive". Otherwise, the old fashioned way might work: go to a relevant Usenet newsgroup, sort the posters by author name, and look for the dude "by hand". Yes, when this involves 5000 plus articles in alt.binaries.warez.ibm-pc, the task can be tedious...which is why Spam-slamming is for the patient hunter.

4) After finding real name, go through steps enumerated above for Type 1 Spammer. If you are unable to find the real name and/or username, then give the ISP as much information as possible (several relevant posts *with full headers*)-- their NNTP logs may be able to pinpoint the perp.

Type 3: Professional SpamDude, posting pseudo-anon from possibly rogue ISP

This is where the task can become difficult, and even dangerous. A number of these professional SpamDudes take retaliatory action against netizens who attempt to oppose their flagrant net.abuse (e.g., via e-mail bombing, threatening e-mail [bogus lawsuit threats are de rigueur], posting user information to sex-related newsgroups for the purpose of having others do their harassment for them, etc.). Be very sure that you have taken *strong* precautions to prevent this from harming your net.life before going up against a Jeff Slaton-type SpamDude.

Here's an example:

-----Begin SpamQuote-----
Path: netnews.worldnet.att.net!worldnet.att.net!ix.netcom.com!
super.zippo.com!zdc-e!newsfeed.gte.net!igmg.com!
From: IGMG [igmg@hotmail.com>
Newsgroups: alt.binaries.slack
Subject: Post your message to EVERY newsgroup for \$35.00 74559601490745
Date: Fri, 13 Dec 1996 13:15:24 EST
Organization: Internet Global Marketing Group [igmg@hotmail.com>
Lines: 48
Expires: +3days
Message-ID: [121319961315241490745igmg@hotmail.com5960>
NNTP-Posting-Host: npr236127.gte.net

To reply to this message use the email address at the end...

I have developed a Windows 95 and Windows NT Internet Marketing Solution that will revolutionize the way you conduct direct marketing over the Internet.

[snip]

If you want more information or want to purchase a copy for yourself contact IGMG at igmg@hotmail.com

If money is tight now, then it was tight last week too, and it will continue to be tight until you do something to attract PAYING customers to your site. It's true, how many people do you think are reading this same message you are right now? Think about it and contact igmg@hotmail.com

Thanks For Your Time -

IGMG
igmg@hotmail.com

This message was posted using Internet Global Marketing Software.
Post your business advertisement to over 28,000 newsgroups at once.
Custom software and cdrom's with millions of email address's
For more information contact igmg@hotmail.com

-----end SpamQuote-----

It is obvious that a reverse search for igmg@hotmail.com via IAF will come up empty, and that fingering same will be fruitless. The Spammer's reply e-mail address in these cases is almost always a "one-time cipher"-- a recently-created throw-away account. They *know* they are going to be inundated with complaints, even e-mail bombs (which S.P.[U.T.U.]M. does not condone); they are hoping that the benefits (several hundred clueless Spam-Dude-wannabe positive responses) will outweigh the risks (loss of their throw-away account).

Thus, in these cases, massive retaliation is usually called for:

- 1) Before doing *anything*, however, carefully search:
news.admin.announce Announcements for news administrators. (Moderated)
news.admin.net-abuse.bulletins Bulletins of action re net abuse.(Moderated)
news.admin.net-abuse.email Discussion of abuse of email systems.
news.admin.net-abuse.policy Discussion of net abuse policy. (Moderated)
news.admin.net-abuse.sightings Sightings of net abuse. (Moderated)
news.admin.net-abuse.usenet Discussion of abuse of the Usenet system.

...for evidence that the Usenet Ghods are aware of the situation and are taking action to identify and neutralize the Spammer. Oftentimes, these professional SpamDudes leave a trail of slime across thousands of newsgroups, generating *tons* of counterproductive back-spamming complaints. Don't go there. Go underground, dig for data on the Spammer, and post only the juicy, new tidbits that aren't already yesterday's news.

- 2) Analyze the path carefully. In this instance, we have a very strange path that has been tampered with, ending in: `newsfeed.gte.net!igmg.com!`
--note that the final host in a non-forged path should not end with ! but rather something like "news.foo.net", or "news.foo.net!user", or "news.foo.net!not-for-mail". Thus, we can assume that IGMG.COM is bogus,

Newsgroups: news.admin.net-abuse.usenet,news.admin.net-abuse.email
Subject: Re: How do I trace an IP address spam?
Message-ID:
References:
Organization: Despams 'r' us Rogue Midwest Office

In article , "William A. Levinson"
wrote:

>A pornographic Web site spammed an all-ages newsgroup to which I
>subscribe, and posted a link to an IP address. I tried NSTRACE at
><http://zeus.lyceum.com> which supposedly traces IP addresses, but it came
>back with a "nonexistent address." The link, unfortunately, is quite
>functional though.
>
> A spam that includes a domain name, of course, can be traced with
>InterNIC's WHOIS function.

So can an IP address, but it a bit more complex.

The complexity comes from the way IP addresses are registered with the InterNIC. They are allocated to providers who assign them in variously sized vlocks to cutomers who may or may not have those blocks registered. Conceivably an address could match a dozen entries, and while the most direct responsibility is in the owner of the smallest block containing the address, there are all sorts of evasive games that can be played.

As for how to look up an address, you can start with the complete address and just work upwards. I'll use a completely bogus address for the examples. To start just try the complete address:

whois 255.123.34.56

If that gets nothing (likely) try:

whois 255.123.34.0

That should get something for any address above 192.0.0.0. For addresses below that mark (which is the division between historical Class B and Class C networks) try

whois 255.123.0.0

Which would work for Class B addresses. Below 128.0.0.0 are Class A nets, which would be registered as a whole and found with:

whois 255.0.0.0

Note that as you go up from sub-C nets to A nets you are looking at an increasing likelihood that the registered owner of the address space has in fact assigned the specific address you want to someone else, and that they've further reassigned it, with no sub-registrations. PSI is one of the worst offenders in this area, because they are one of the few major

and that a whois on domain IGMG.COM would be a waste of time.

3) Look at the return e-mail address...look **very** carefully, and you will see that the e-mail address in the "from" section has been forged as well: igmg@hotmail.com (with a capital "I") does not equal igmg@hotmail.com! Thus, we note some of the trademark concatenated deceptions of the professional SpamDude. However, we are not deterred.

4) Even the Subject: line has been tampered with: Note unique spam message ID to attempt to fool the cancelbots (each message would therefore seem different to a bot which counts instances of a unique header/subject line, even though the content was the same).

5) The nntp posting host is usually the hardest "sharp edge" to forge. Remember, however, that the professional SpamDude is likely VICTIMIZING the posting ISP, especially if it is a major backbone provider (GTE.NET, UU.NET, etc.). This is sometimes done via open NNTP servers-- Usenet servers which allow anyone in the world to utilize their computers to post messages. Oftentimes, the ISP has no idea that they have left this security "backdoor" wide open-- a fact exploited by the alt.religion.scientology vertical spam flooder, among others.

Our next mission is to:

---determine if hotmail.com is a rogue ISP that was created for the purpose of spamming, or a victim of this Spammer

AND, if rogue, or if the Spammer name is the same as the administrative contact name via Internic Whois,

---To determine the upstream ISPs supplying service to the rogue ISP, so as to cut them off at the knees.

In this instance, we went to hotmail's website (<http://207.82.169.123/about.html>) and found lots of contact info on this apparently non-rogue ISP, enabling us to identify the domains of the administrators, as well as the upstream ISPs.

BUT, you ask, what if all you have on a Spammer is an IP address, of the form 123.45.679.910? Then, you must resolve the IP address into a DNS name via NSLOOKUP or DIG...or, if that fails, attempt to run a traceroute on the IP address. For a good explanation of how traceroute works, along with more info on this DNS thang, check this out.

New Addition: What if all you have is a numeric IP address, but it doesn't resolve via NSLOOKUP into a valid DNS name?

Good question.

Here's an even better answer:

-----Quoted article from news.admin.net-abuse.usenet:-----

Date: Sat, 28 Jun 1997 19:35:01 -0500

From: bill@scconsult.com (Bill Stewart-Cole)

providers with an A net (38.*) and their incentive to subregister their space to customers is very low.

--

Bill Stewart-Cole bill@scconsult.com
I'm not spam-blocked because I like playing the hardass net-fascist.

Cruelty to the clueless on Usenet is my way of dealing with stress.

-----end quote of Usenet article-----

{S.P.U.T.U.M. Control sez: That sig really gets me hot!}

Ahem. Back to our discussion, already in progress...

How do we determine upstream ISPs for rogue services (SpammmDuuude.com, for example)? Either via traceroute, looking for the last DNS name above the domain in question; or via Internic search for the DNS host names:

-----example!-----

Path: ...!hunter.premier.net!news.cais.net!news.ac.net!imci4!
newsfeed.internetmci.com!in3.uu.net!mae-east.nntp.mfs.net!nntp.ianet.com!
nude.sexplaza.com!usenet
From: melanie@sexplaza.com
Subject: visit our web site!
Newsgroups: alt.binaries.slack,alt.angst,alc.suicide,alt.basement.graveyard
Date: Mon, 29 Jul 1996 10:34:10 EDT
Lines: 5
Message-ID: [431ubb@sexplaza.com>
Reply-To: melanie@sexplaza.com
NNTP-Posting-Host: nf12.ppp.ianet.com
X-Newsreader: Forte Agent .99d/15.123
Xref: alt.binaries.slack:8123 alt.angst:97413 alc.suicide:418
alt.basement.graveyard:4563

Big butts, big boobs, everything you want!
Visit our radical news web site at <http://www.sexplaza.com>
and I promise that we'll give you free blowjobs and all that good stuff.

Love, Melanie

Here we go again with these Canadians...

Sex Plaza (SEXPLAZA-DOM)
6433 Jarry E, suite 200
St-Leonard, Quebec H1P 1W1
Canada

Domain Name: SEXPLAZA.COM

Administrative Contact, Billing Contact:

Doucet, Michel (MD306) michel@CONNECTMMIC.NET
+1 514-332-6642

Technical Contact, Zone Contact:

Salhany, Joseph (JS550) jsalhany@CONNECTMMIC.NET
+1 (514) 332-6642

Record last updated on 10-Jan-96. Record created on 02-Dec-95.

Domain servers in listed order:

CASPER.MMICLINK.NET 204.236.104.4
MMIC.CONNECTMMIC.NET 199.166.219.5

And now, for the upstream (posting) ISP:

Ichthus Access Networking, Inc. (IANET2-DOM)
712 Chestnut St.
Kenova, WV 25530-1511
USA

Domain Name: IANET.COM

Administrative Contact, Technical Contact, Zone Contact, Billing Contact:

Adkins, Garry P. (GA86) adking@IANET.NET
(304) 453-5757

Record last updated on 26-Jun-96.

Record created on 15-May-95.

Domain servers in listed order:

PIRANHA.IANET.NET 204.183.217.3
DNS.IANET.NET 204.183.217.2

Hey, guys, isn't ICHTHUS about, like,
CHRISTIANITY... as in Jesus? Hmm, do you
know what is passing through your servers...
You do now.

Buh bye.

—
SubGenius Police, Usenet Tactical Unit (Mobile), AKA S.P.U.T.U.M.
Berserker Lairds of Overkill Wetware/Mechanoyeti Enforcers
Unit XIII: Death Walks Among You
<http://www.sputum.com/>

-----end quote-----

[Note that we uncovered other leads to Upstream ISPs of sexplaza:

CASPER.MMICLINK.NET 204.236.104.4
MMIC.CONNECTMMIC.NET 199.166.219.5

which were, in fact, useful later {led us to fonorola.net contact info}.
IANET.NET appeared to be an unwitting victim in this case.].

Type I Spammer: Stupid clueless newbie, barely able to post in the clear

A Spam article appears on a.b.s. with the following characteristics:

-----begin Spam quote-----
Path: ix.netcom.com!ix.netcom.com!news-res.gsl.net!news.gsl.net!
usenet.eel.ufl.edu!hookup!chi-news.cic.net!ddswl!news.mcs.net!
news.abs.net!jspivey
~~~~~  
From: an538425@anon.penet.fi --Note misspelling of anon.PENET.fi--  
sign of a true pro  
Newsgroups: alt.2600.hackerz,alt.2600.phreakz,alt.2600.warez,  
alt.binaries.misc,alt.binaries.slack,alt.binaries.warez,  
alt.binaries.warez.ibm-pc,alt.binaries.warez.ibm-pc.d,  
alt.binaries.warez.ibm-pc.dos,alt.binaries.warez.ibm-pc.old,  
alt.bio.hackers,alt.hacker,alt.hackers.groups,alt.warez.ibm-pc,  
alt.warez.ibm-pc.apps,alt.warez.ibm-pc.old  
Subject: !!Help with DETROIT 1115 !!!!  
Date: 28 Jul 1996 22:05:56 GMT  
Organization: ABSnet Internet Services, Inc.-(410)-685-2000 -sales@abs.net  
Lines: 9  
Message-ID: [4tgo85\$ehh@news.abs.net>  
NNTP-Posting-Host: ppp103.bcpl.lib.md.us  
X-Newsreader: News Xpress Version 1.0 Beta #3  
Xref: ix.netcom.com alt.2600.hackerz:3493 alt.2600.phreakz:1807  
alt.2600.warez:7009 alt.binaries.misc:146348 alt.binaries.slack:8098  
alt.binaries.warez:19901 alt.binaries.warez.ibm-pc:543268  
alt.binaries.warez.ibm-pc.d:7196 alt.binaries.warez.ibm-pc.dos:2622  
alt.binaries.warez.ibm-pc.old:13458 alt.bio.hackers:2856  
alt.hacker:16141 alt.hackers.groups:981 alt.warez.ibm-pc:4333  
alt.warez.ibm-pc.apps:10372 alt.warez.ibm-pc.old:3688

I'm running detroit 1115 on at 5x86 32 meg system. When I run ppp  
type appz I get an error message. Example like cuteftp or mIRC.  
Here's the error message:

"A fatal exception 0E has occurred at 0028:C0F4BED2 in VXD WSOCK(01) +  
00000ED2"

Then the app closes. What does this mean? How can I fix it? Post a  
messages... Thanks

-----end Spam quote-----

Classic hallmarks of Type I Newbie: real user name in path, ISP contact  
phone number in organization, terrible formatting, multiple copies of  
same message in post (inadvertent extra "paste"), AOL or .edu-ish domain  
name.

If the poster has had the stupidity to post with her real name and/or home  
address, we have her. This almost always means that the path information

and nntp posting host have not been forged...

Thus:

1) Perform whois do domainname.com if U.S. domain. Update! (5 Apr 98) The handling of Network Point of Contact info, etc., has recently changed; go to Arin Whois or enter (Unix) whois -h whois.arin.net <ip address> to find "information on networks, autonomous system numbers (ASNs), networks-related handles, and other related points of contact (POCs)." As always, U.S. Department of Defense MILNET info should be sought at <http://nic.ddn.mil/cgi-bin/whois>. [Thanks to Jay Isaacs <jay.r.isaacs@mci.com> for reminding us to update this section...Slack!] If you find the official Internic whois server slow, you may want to bookmark one of the whois servers geographically near to you. If the domain is from outside the U.S., Internic may or may not have the contact info in its database. For European sites, check out RIPE; alternative site is RIPE via WAIS. For other foreign sites, we have found that visiting the ISP's website ([www.ispname.com](http://www.ispname.com) or [www.ispname.net](http://www.ispname.net)) yields contact info in a flash (especially recommended for all the Canadian spam-originating ISPs cropping up nowadays).

2) Attempt to finger user@host.com...this will likely yield great results for .edu accounts, mediocre results for small ISPs, and poor results for nationwide ISPs (which routinely do not accept finger requests, even from the same domain). Another method of getting at a spammer's e-mail address is by using the technique described here to telnet to the mail port (25) of the spammer's SMTP host (more useful for UCE e-mail spam, but thrown in for completeness).

3) Reverse e-mail search via IAF to confirm real name/look for other accounts perhaps more precious to the spammer. If you have a name (e.g., MMF Names list), but need an e-mail address, try searching the awesome WhoWhere? site.

4) Send e-mail complaint to administrative sysop you found listed in internic database, or the alternative abuse e-mail address used by the ISP (see our FAQ or the Spam FAQ for details).

Be polite. Consider using the complaint form from the "Get That Spammer!" site. Emphasize the fact that the offender contravened the ISP's Terms of Service (TOS)/Acceptable Use Policy (AUP) by committing net.abuse.

5) [Optional] AltaVista/DejaNews search for further info on poster (prior posts to alt.depression, alt.recovery.gerbils, etc.).

Never underestimate the intimidation value to the anti-Spammer of narcissistic spammer websites.

6) [Optional] Use 411, Switchboard, or LookupUSA to get the spammer's phone number-- especially if he is a Make Money Fast (MMF) spammer. If the spammer lives outside the United States, try here. Know the address but not the area code? No problem. Proceed to <http://www.555-1212.com/> and punch in the city to get the area code... or vice versa. After you get the area code, you get a bonus prize-- a link to one of the most complete phone number search pages around.

7) [Optional] Map MMF perpetrator's location in 3-space via vicinity.com (after all, they gave you their address!).

8) [Optional] Post all of the above to your newsgroup + news.admin.net-abuse.misc and/or news.admin.net-abuse.usenet. Do **\*not\*** quote the entire message or ("Bob" help us) binary-- the full header plus a few characteristic lines will do (make sure the MMF Spam "names list" remains intact). Do **\*not\*** backspam info to the 100 sites the original

spammer used, however, else you will be defeating the purpose of SpamSlamming which is {class?}

"Conserving Bandwidth!".

Thank you.

9) [Optional] If warez are involved (illegally copied software), then the Software Publishing Association (piracy@spa.org; Peter Beruk, Domestic Anti-Piracy, (202) 452-1600 ext. 314 [pberuk@spa.org]), the FBI nccs@fbi.gov, and/or the security sysop of the ISP (e.g., security@netcom.com) may need to be alerted.

10) [Optional] If MMF is involved, especially if it is a repeat MMF from the same user, then the U.S. Postal Inspectors Service Postal Fraud hotline (jccheezum@uspis.gov), the IRS Net Abuse Division (net-abuse@nocs.insp.irs.gov), the FTC (crc@ftc.gov or uce@ftc.gov [e-mail fraud], and/or the National Fraud Information Center nfic@internetMCI.com]; <http://www.fraud.org/nficmail.htm>) may need to be alerted.

The method for accomplishing this is similar to those used for IRC, but simpler.

Every computer on the Internet has an address. A web address can be used to learn who owns the host machine and where the machine is located.

Usually the nationality of the address is immediately apparent. The suffixes ".com" ".org" ".net" ".gov" ".edu" are generally on U.S. servers; whereas, other nations generally employ an extension indicating the country, e.g., the ".br" extension in the address "<http://www.ongba.org.br/org/cedeca/>" indicates it is in Brazil.

To find the contact information for the host company, simply enter the root address in the On-Line Digger Engine on this site. (Note: our engine is fairly comprehensive, but it is not yet able to return "whois" information for every country, unless you manually enter that obscure nation's whois server. We will continue to update the engine, and would appreciate your input if you know of a whois server we should add.)

Most illegal web sites are hosted on someone else's server, and often the host company is unaware of the site's content.

If the perpetrators' site is on their own server, or if they have a virtual server account with their own domain name, the digger engine results may only display the contact information that the perpetrator provided InterNic or a similar service. You can investigate further using the IP block holder's identity. More advanced information on this will be posted here at a later date.

If the site has child pornographic images or other illegal content, the information returned by the on-line digger engine should be sufficient to determine which regional law enforcement agencies to contact. Use the list on our Report! page.

What to do once you have traced the site?

If you are a law enforcement investigator, contact the root company hosting the perpetrator's site and obtain his identity, address, and other account information from them. They may also be able to provide you with further incriminating evidence. As a for-profit business, they may want to immediately terminate

the perpetrator's account, which may not interfere with your investigation, and is probably a very good thing, as it will prevent others from downloading the material. But keep it in mind, and discuss it with them. If you do not, they may go so far as to tip off the perpetrator before you can get a warrant to search his hard drive.

If the site is a commercial site, it is possible that the perpetrator owns his own machine. In such a case, you would not want to inform the contacts returned by the online digger engine. As mentioned before, we will post more advanced techniques here soon.

Oftentimes times the perpetrator and his host company will prove to be outside your jurisdiction. Please forward all your evidence and notes to investigators who do have jurisdiction and do what you can to see that they pursue it. Our contact with investigators indicates a majority of out-of-jurisdiction instances are simply dropped, often because of a lack of information on whom to forward it to. You may consult our Report! international report receiving contacts...it is far from complete but may be of use. (Please help us expand it.)

Our feedback indicates that two out of three forwarded investigations are resumed by the receiving office.

Take a moment to step back and look at law enforcement efforts as a whole. You can see how inefficient the current practice of searching the Internet solely for perpetrators in one small jurisdiction is. Interagency cooperation is essential for efficiency.

If you are a private citizen, the process is a bit simpler, generally. Input the site address in our online digger engine and then contact investigative authorities in the area of the server company.

The tricky part here is getting the information to the right investigators. If you merely send it to the email address of U.S. Customs, they may or may not follow up on your lead. Currently they are very unresponsive. Despite explicitly instructing Internet users to contact them with any information of illegal child pornography activity, they do not seem to be acting on such reports, and they are presently not even replying with an indication that the information was received...something that could be set as an auto response.

If you want to insure that your report will receive attention, it is best to speak on the phone with an investigator in an appropriate office. In the U.S. you may wish to call the FBI in the area of the perpetrator. Or you may be even better received by the local police or sheriffs office, provided they have investigators capable of Internet and computer crime investigation.

Some good contacts are listed on our Report! page.

Follow through is the most important element.

Date: \_\_\_\_\_

**CONSENT FOR REMOVAL OF COMPUTER AND OTHER  
RELATED MATERIAL**

I \_\_\_\_\_, do give permission and consent to Det. \_\_\_\_\_, shield # \_\_\_\_\_ of Police Department. to remove my computer, floppy disks, manuals, books and any other related material for examination. No promises or threats have been made by anyone, the \_\_\_\_\_ property will be vouchered and I will receive a receipt for all property.

Signature: \_\_\_\_\_

Witness: \_\_\_\_\_

Witness : \_\_\_\_\_

USE ONLY AFTER PERP IS APPREHENDED, AOL WILL FREEZE E-MAIL AND  
TERMINATE ACCOUNT

Your Unit  
Address  
Date

America On Line Incorporated  
22000 AOL Way  
Dulles, Virginia 21066

Re: Preservation Request

Dear Mr. Ryan:

It is requested that a block be placed on the America On Line account subscribed  
to by the following:

Name:  
Address:  
Telephone:

Screen Name:  
Possible AOL Account  
Credit Card:

Through an official criminal investigation, the (Your Department) has determined  
that the above individual has an active account with America On-Line Incorporated, and  
it is known that this account has been used to participate in the trading of sexually  
explicit pornographic images via the personal computer (May modify: to engage minors  
in conversation for the purposes of sexual exploitation, etc)

You are being advised that a search warrant was executed at the (residence,  
address) on DATE. It is anticipated that a search warrant will be executed at your office  
in the near future.

Sincerely Yours,

**SOFTWARE NECESSARY:**

Should all be registered to undercover account, "Hello" Phone (Fictitious) caller id blocked, return calling blocked, fictitious mailbox

**UNDERCOVER INTERNET ACCOUNT**

**ie:** netcom,. Ibm net

**Commercial Service:**

AOL, Compuserve, Prodigy

**WINDOWS 95:**

Check Registry, Make sure no police Department references

**Investigative Software**

Netscan Tools

NetLab

Free Agent, Forte

Web Ferret Pro, Ferret Soft

Mirc

FTP Program, CuteFTP ot WS\_FTP

Vueprint

ThumbsPLus, Cerious Software

Winzip

Dexter

Icull

Netmeeting from Microsoft

MS Office Professional

**If Seizing Systems:**

Disklok on a bootable floppy



U/C Caller: \_\_\_\_\_  
Date: \_\_\_\_\_

Time Started: \_\_\_\_\_  
Time Ended: \_\_\_\_\_

Recorded: yes/no

Fictitious company name

e.g: Uplink Network Corporation, PO Box 4000, Bridgeton, MO. 63044-9718

### Survey Questionnaire

Hello my name is Cathy Upjohn of the Uplink Corporation. We are offering 50 free hours of On-line service on any commercial service of your choice (Prodigy, Delphi, Compuserve or America On Line) for answering our questions. It will take only two minutes of your time and we send you via mail our software with the ten free hours of usage for your input.

1. What type of computer do you own?
  
  
  
  
  
  
  
  
  
  
2. Do you own a modem, if so what speed?
  - a. Internal or external
  - b. What brand
  
  
  
  
  
  
  
  
  
  
3. Do you own any other type of computer such as a laptop?
  - a. Does it have a modem, what speed?
  
  
  
  
  
  
  
  
  
  
4. Who in your household uses the computer most frequently?
  
  
  
  
  
  
  
  
  
  
5. Which computer do you use most frequently?
  
  
  
  
  
  
  
  
  
  
6. Do any of your computers have multimedia capability?
  
  
  
  
  
  
  
  
  
  
7. Is it utilized for business, childrens homework, entertainment?

8. Are you a member of any online service? If so, which one?
9. What do you like most about your online service?
10. What do you like least about our online service?
11. Do you own or are a Systems operator of a Bulletin Board or Webmaster?
12. What time of day do you use the computer most frequently?
13. Do you use it most frequently at home or work?
14. What is your occupation?
15. And which online service do you want? We have Delphi, America On line, CompuServe, Prodigy and Imagination network.
16. Where can I mail the software to? **(Be sure to get his/her name with the address)**

Thank you for assisting us in our survey and your software should arrive within 12 to 14 working days.

June 23, 1997

From:

To: David Piskur, Legal Matters/Subpoenas

Subject: **SUBPOENA FOR SUBSCRIBER INFORMATION**

1. I am submitting a subpoena to release information on the following user:

123456, 789900

2. This screen name was used on CompuServe during the commission of Aggravated Harassment and the identity of the subscriber is needed to determine the perpetrator of this crime.

3. I am also sending the subpoena through the mail as you requested. Please call me if there are any questions, and thank you for your assistance.

June 11, 1997

From:

To:

Subject : **REQUEST SUBPOENA**

1. It is requested that you issue a subpoena to Juno Online Services to release subscriber information and all other screen names for the following screen names:

Name@JUNO.COM

2. This screen name was used on Juno Online Services during a commission of the crime of Criminal Impersonation and this information is needed to identify the subject of this investigation.

3. The subpoena can be directed to the attention of:

Russell Farhung  
Juno Online Services  
120 West 45 St.  
New York, NY

4. This matter is assigned to Det.

June 17, 1997

From: Unit  
To:  
Subject : **REQUEST SUBPOENA**

1. It is requested that you issue a subpoena to CompuServe to release subscriber information for the following user:

xxxxxxx, 704

2. This screen name was used on CompuServe during the commission of Aggravated Harassment and the identity of the subscriber is needed to determine the perpetrator of this crime.

3. The subpoena can be directed to the attention of:

David Piskur  
CompuServe Legal/Subpoena  
52000 Arlington Centre Blvd.  
Columbus, OH 43220  
tel# (614) 457-8600; FAX (614) 457-9665

4. This matter is assigned to Det. Sxyz under Case# 30, telephone Thank  
you for your assistance.

December 23, 1997

From: Unit

To:

Subject : **REQUEST SUBPOENA**

1. It is requested that you issue a subpoena to Bell Atlantic Subpoena Group of 1095 Avenue of the Americas, Room 2900, New York, N.Y., 10036 to the attention of Mary Ann Gainer (212 395-0523) for subscriber and billing information, published or non-published, and related information for the telephone number listed below:

Phone Number

2. This information is needed to identify the subject in an investigation of Aggravated Harassment assigned to Det. Xyz under Case #, telephone

September 22, 1997

From  
To:  
Subject: **REQUEST SUBPOENA**

1. It is requested that you issue a subpoena to AT&T Wireless Services Investigative Group located at 1211 Avenue of the Americas, New York, N.Y. to the attention of Sharon Momo, telephone number (212) 334-0802 for subscriber and billing information and other related information for the telephone number listed below:

(Phone Number

2. This information is needed to identify the subject of an investigation of crime .This matter is assigned to Det. Xz under Case #bb telephone Thank you for your assistance.

February 6, 1998

**From:**

**To:** Deputy Commissioner, Legal Matters

**Subject :** REQUEST SUBPOENA

1. It is requested that you issue a subpoena to America Online to release subscriber information and all other screen names for the following screen names:

Screen Name

2. These screen names were used on America Online and are needed for the identification of persons committing Aggravated Harassment investigated under Case #007.

3. The subpoena can be directed to the attention of:

Justyna Kilbourne  
America Online Legal Division  
22000 AOL Way  
Dulles, VA 20166  
tel# (703) 265-2745; FAX (703) 265-2305

4. This matter is assigned to Det. Xyz under Case #76, telephone.  
Thank you for your assistance.



October 3, 1997

From:  
To:  
Subject: **REQUEST SUBPOENA**

1. It is requested that you issue a subpoena to US West Communications, Custodial Records, located at 1801 California St. Room #3250, Denver, Colorado, 80202 for subscriber information and records of outgoing telephone calls (LUDS and tolls) for the numbers listed below for the time period between 12:01 AM on August 28 and 3:00 AM on August 29, 1997:

Phne Numbers

2. This information is required to identify the subject of an ongoing investigation concerning This matter is assigned to

November 14,1996

From:  
To:  
Subject : **REQUEST SUBPOENA**

1. It is requested that you issue a subpoena to Spry Net to release subscriber information and all other screen names for the following screen name:

Name @sprynet.com

2. This information is needed to identify the subject of an on going investigation involving . A member of the service receiving threatening e-mail .

3. The subpoena can be directed to the attention of:

Cindy Honma  
Sprynet  
3535 128th Ave SE  
Bellview, Washington 98006

4.

December 11,1996

From:  
To:  
Subject : **REQUEST SUBPOENA**

1. It is requested that you issue a subpoena to U.S. Sprint, known as Sprint Communications: located at 9221 Ward Parkway Suite 400, Kansas City, MO 64114 Att: subpoena compliance group Tel# 913-624-4734 Fax# 913- 624-4706 for all subscriber and billing information for the following number:

(800) 786-8241  
Pin# 129357

2. This information is required to identify the subject of an ongoing investigation concerning

**POLICE DEPARTMENT  
CITY OF NEW YORK**

December 4, 1997

**From:** Commanding Officer, Computer Investigation and Technology Unit

**To:** Deputy Commissioner, Legal Matters

**Subject :** REQUEST DEPUTY COMMISSIONER'S SUBPOENA

1. It is requested that you issue a subpoena to Bell Atlantic Subpoena Group at 1095 Avenue of the Americas, Room 2900, New York, NY 10036 to the attention of Mary Ann Gainer, (212) 395-0523 for records of incoming telephone calls to the number listed below for the 24 hour period from 12:01 AM on November 14, 1997 to 11:59 PM on November 14, 1997:

(212) 529-8440

2. This request for the processing of an "N-File" search requires the following instructions to be included in the subpoena:

"All calls and listings derived from a special computer run regarding calls to Classic Sports Network located at 300 Park Ave. South, New York City, for the telephone number (212) 529-8440 for the time period beginning at 12:01 AM on November 14, 1997 and ending 11:59 PM on November 14, 1997. This special computer run is a billing tape search. Stephen Greenberg, President of Classic Sports Network located at 300 Park Ave. South, New York City, telephone number (212) 529-8000 has given consent for this file search and that the company has agreed to pay for the cost of this search".

3. This information is required to identify the subject of an ongoing investigation concerning Computer Tampering 1. This matter is assigned to Detective Gerard Schoenacher under Case #065, telephone 212-374-4247. Thank you for your assistance.

Detective Gerard Schoenacher  
Computer Investigation and Technology Unit

**FIRST ENDORSEMENT**

Commanding Officer, C.I.T.U. to the Deputy Commissioner, Legal Matters, December 4, 1997.  
I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski  
Commanding Officer, C.I.T.U.

**POLICE DEPARTMENT  
CITY OF NEW YORK**

December 23, 1997

**From:** Commanding Officer, Computer Investigation and Technology Unit

**To:** Deputy Commissioner, Legal Matters

**Subject: REQUEST DEPUTY COMMISSIONER'S SUBPOENA**

1. It is requested that you issue a subpoena to Bell Atlantic Subpoena Group at 1095 Avenue of the Americas, Room 2900, New York, NY 10036 to the attention of Mary Ann Gainer, telephone (212) 395-0523 for records of outgoing telephone calls (LUDS and tolls) for the number listed below for the time period between 1:00 AM on November 14, 1997 to 11:00 PM on November 14, 1997 for the below listed number:

(212) 539-1363

2. This information is required to identify the subject of an ongoing investigation concerning Computer Tampering 2. This matter is assigned to Det. Gerard Schoenacher under Case #065, telephone 212-374-4247. Thank you for your assistance.

Det. Gerard Schoenacher  
Computer Investigation and Technology Unit

**FIRST ENDORSEMENT**

Commanding Officer, Computer Investigation and Technology Unit to the Deputy Commissioner, Legal Matters, December 23, 1997. I certify that the records requested are required for the above investigation.

Lieutenant Christopher Malinowski  
Commanding Officer, C.I.T.U.

COURT OF THE CITY OF NEW YORK  
COUNTY OF NEW YORK

-----  
IN THE MATTER OF AN APPLICATION FOR A  
WARRANT TO SEARCH THE PREMISED LOCATED AT  
\_\_\_\_\_ EAST \_\_\_ STREET, Apt. # \_\_  
NEW YORK, NEW YORK.  
-----

AFFIDAVIT IN SUPPORT OF  
SEARCH WARRANT

Det. \_\_\_\_\_, being duly sworn, deposes and says:

1. I am a Detective, Shield # \_\_\_\_\_, assigned to the \_\_\_\_\_ Squad/  
Unit of the New York City Police Dept., and as such I am a public servant of the kind  
specified in C.P.L. Section 690.05 (1).

2. I have been a Police Officer for \_\_\_ years and a Detective for \_\_\_ years  
and have been assigned the \_\_\_\_\_ Squad/Unit for \_\_\_ years and have [list expertise  
in crime being investigated, such as training or specific knowledge in the area of this type  
of crime investigation where possible].

3. I am currently assigned to an ongoing investigation of [describe the  
investigation].

4. This affidavit is submitted in support of an application for a warrant to  
search the designated premises to wit: \_\_\_\_\_ Street, Apt. # \_\_ New York, New  
York, where there is reasonable cause to believe that the following property may be  
found: [list property for that type of investigation, such as guns, drugs, business records,  
etc., and then the computer-related property...],  
computers and computer systems, computer hardware including peripherals and cables,  
computer software stored on any media such as floppy disks or CD ROMs, removable  
media such as external hard drives or data cartridges, devices used to store computer data  
such as tape backup systems or CD ROM reader/writers, computer communication  
equipment such as printers and modems, servers, workstations together with system  
documentation, operating logs, instruction manuals or any other material describing the  
operation of any computer, computer system or computer-related procedure. Moreover,  
as set forth below, there is reasonable cause to believe that this property constitutes  
evidence or tends to demonstrate that an offense was committed or that a particular  
person participated in the commission of said offense.

5. My basis for believing that the property is in the above stated location(s) is  
as follows: [describe personal observations, past investigations, registered informants,  
etc.).

WHEREFORE, deponent respectfully requests that the Court issue a warrant and order seizure in the form annexed authorizing a search of premises to wit: \_\_\_\_\_ Apt. # \_\_, New York, New York and search occupants if present therein for [list property for that type of investigation, such as guns, drugs, business records, etc., and then the computer-related property...], computers and computer systems, computer hardware including peripherals and cables, computer software stored on any media such as floppy disks or CD ROMs, removable media such as external hard drives or data cartridges, devices used to store computer data such as tape backup systems or CD ROM reader/writers, computer communication equipment such as printers and modems, servers, workstations together with system documentation, operating logs, instruction manuals or any other material describing the operation of any computer, computer system or computer-related procedure and all items used to facilitate or evidencing violations of Penal Law Article \_\_\_ and directing that if such evidence be found, it be brought before the Court without unnecessary delay. No previous application has been made in this matter to any other Judge, Justice or Magistrate.

\_\_\_\_\_  
Detective \_\_\_\_\_  
Shield # \_\_\_\_\_, NYPD, \_\_\_\_\_ Squad/Unit

Sworn to before me this  
\_\_\_\_\_ day of November, 1997

\_\_\_\_\_  
Judge of the Criminal Court

CRIMINAL COURT OF THE CITY OF NEW YORK  
COUNTY OF NEW YORK

-----  
IN THE MATTER OF THE APPLICATION  
OF DET. \_\_\_\_\_  
OF THE NEW YORK CITY POLICE DEPARTMENT  
FOR A SEARCH WARRANT  
-----

THE NAME OF THE PEOPLE OF THE STATE OF NEW YORK  
TO ANY POLICE OFFICER IN THE CITY OF NEW YORK

Proof by affidavit having been made this day before me that there is reasonable cause to believe that certain property, to wit, [list property for that type of investigation, such as guns, drugs, business records, etc., and then the computer-related property...], computers and computer systems, computer hardware including peripherals and cables, computer software stored on any media such as floppy disks or CD ROMs, removable media such as external hard drives or data cartridges, devices used to store computer data such as tape backup systems or CD ROM reader/writers, computer communication equipment such as printers and modems, servers, workstations together with system documentation, operating logs, instruction manuals or any other material describing the operation of any computer, computer system or computer-related procedure is located at the premises, to wit: \_\_\_\_\_ Street Apt. # \_\_, New York, New York and is [stolen, unlawfully possessed, has been used or is possessed for the purpose of being used, to commit or conceal the commission of an offense or constitutes evidence or tends to demonstrate that a n offense was committed to wit: [crime].

YOU ARE THEREFORE COMMANDED [at any time of the day or night,] to make an immediate search at the above-described premises, to wit: \_\_\_\_\_ Street, Apt. # \_\_, New York, New York and search of occupants therein, for [list property for that type of investigation, such as guns, drugs, business records, etc., and then the computer-related property...], computers and computer systems, computer hardware including peripherals and cables, computer software stored on any media such as floppy disks or CD ROMs, removable media such as external hard drives or data cartridges, devices used to store computer data such as tape backup systems or CD ROM reader/writers, computer communication equipment such as printers and modems, servers, workstations together with system documentation, operating logs, instruction manuals or any other material describing the operation of any computer, computer system or computer-related procedure and if you find such property or any part thereof to bring it before the Court without unnecessary delay. This warrant must be executed within 10 days of the date of issuance.

\_\_\_\_\_  
Judge of the Criminal Court

Dated:



COURT OF THE CITY OF NEW YORK  
COUNTY OF NEW YORK

-----  
In the matter of the application of Detective \_\_\_\_\_,  
shield # \_\_\_\_\_ of the New York City Police Department,  
Computer Investigation and Technology Unit,  
for a Search Warrant authorizing the search of computer equipment,  
to wit: [number] computer[s] vouchered under NYPD invoice #G \_\_\_\_\_,  
recovered from 111 \_\_\_\_\_ St., New York, New York.  
-----

STATE OF NEW YORK                    )  
                                                  ) ss:  
COUNTY OF NEW YORK                )

Detective \_\_\_\_\_, New York City Police Department, shield  
# \_\_\_\_\_, being duly sworn, deposes and says:

1. I am the applicant herein and am a public servant of the kind specified in  
C.P.L. Section 690.05 (1), my title being Detective, \_\_\_\_\_ Computer  
Investigation and Technology Unit of the New York City Police Department.

2. I have been a Police Officer for eighteen years and have been a Detective  
for eight years and during the course of that time a have been assigned to the Computer  
Investigation and Technology Unit. I have attended seminars and conferences concerning  
the forensic examination of computers given by SEARCH, HTCIA, National White  
Collar Crime Association FinCEN among others, am a current member of HTCIA and  
have assisted in presentations to various NYPD units in the area of computer crime  
investigation.

3. This affidavit is submitted in support of an application for a warrant to  
search files stored inside computer equipment, to wit: [number] computer[s] recovered  
from 111 \_\_\_\_\_ St., New York, New York ("the target computer[s]"), where there is  
reasonable cause to believe that the following property may be found: (a) [databases  
containing gambling records, electronic images depicting child pornography, etc.]; (b)  
electronic communications detailing the [sale, purchase, transfer, etc.] of the [files,  
images, etc.] described above. Moreover, as set forth below, there is reasonable cause to  
believe that this property constitutes evidence or tends to demonstrate that an offense was  
committed or that a particular person participated in the commission of said offense.

4. My basis for believing that the property is in the above-stated  
location is as  
follows: I was informed by [investigator's name] of [Squad, Unit or Agency name] that  
[tell their story].

5. The foregoing constitutes grounds for my belief.

WHEREFORE, deponent respectfully requests that the Court issue a search warrant and order seizure in the form attached (i) authorizing a search of files stored inside computer equipment vouchered under NYPD invoice # \_\_\_\_\_, recovered from \_\_\_\_\_ Street, New York, New York for (a) [databases containing gambling records, electronic images depicting child pornography, etc.]; (b) electronic communications detailing the [sale, purchase, transfer, etc.] of the [files, images, etc.] described above, and (ii) directing that if such evidence is found, it be brought before the Court. The deponent also requests permission to decode protective passwords, download data from the computer, convert or transfer such data to storage in another device. No previous application in this matter has been made to this Court or to any other Judge, Justice or Magistrate.

\_\_\_\_\_  
Detective \_\_\_\_\_  
Shield #2416, NYPD, CITU

\_\_\_\_\_  
[assigned ADA]  
APPROVED: Assistant District Attorney

Sworn to before me this  
\_\_\_\_\_ day of November, 1997

\_\_\_\_\_  
Judge of the Criminal Court

CRIMINAL COURT OF THE CITY OF NEW YORK  
PART AR-1, COUNTY OF NEW YORK

---

IN THE MATTER OF THE APPLICATION OF

Det. \_\_\_\_\_ of the  
\_\_\_\_\_ Squad/Unit of the  
New York City Police Department for a  
Search Warrant to search \_\_\_\_\_ Street,  
Apt. # \_\_, New York, New York

---

TO ANY POLICE OFFICER OF THE CITY OF NEW YORK

Proof by affidavit having been made this day before me by Det. \_\_\_\_\_, shield # \_\_\_\_\_ of the \_\_\_\_\_ Computer Investigation and Technology Unit, that there is reasonable cause to believe that certain property [belonging to (subject of investigation/defendant) and] constituting evidence to wit: [computer databases containing gambling records, electronic images depicting child pornography, etc.]; electronic communications detailing the sale, purchase and/or transfer of the [files/images] described above, may be found in files inside computer vouchered under NYPD invoice # \_\_\_\_\_, which was recovered from \_\_\_\_\_ Street, New York, New York.

YOU ARE THEREFORE COMMANDED, at any time of the day or night, to search the computer vouchered under NYPD invoice # \_\_\_\_\_ which was recovered from \_\_\_\_\_ Street, New York, New York, for (a) [databases containing gambling records, electronic images depicting child pornography, etc.]; (b) electronic communications detailing the [sale, purchase, transfer, etc.] of the [files, images, etc.] described above, and if you find such property or any part thereof to bring it before the Court without unnecessary delay. You are also authorized to decode protective passwords, download data from the computer, convert or transfer such data to storage in another device.

This warrant must be executed within ten days of the date of issuance.

\_\_\_\_\_  
Judge of the Criminal Court

Dated: New York, New York

\_\_\_\_\_

STATE OF NEW YORK  
COUNTY COURT : COUNTY OF ERIE

---

In the Matter of the Application of  
Michael G. McCartney, for a Search  
Warrant Authorizing the Search of  
1 Huntington Quadrangle, Suite 2S12,  
Caraccia & Co, CPA, in the City  
of Melville, County of Suffolk, State of New York.

---

APPLICATION BY AFFIDAVIT  
FOR A SEARCH WARRANT

STATE OF NEW YORK)  
COUNTY OF ERIE) SS.:  
CITY OF BUFFALO)

Michael G. McCartney, being first duly sworn, hereby deposes and states as follows:

#### INTRODUCTION

I am an Investigator with the New York State Attorney General's Office Criminal Division currently assigned to the Criminal Prosecutions Bureau (hereinafter "NYSAG"), Buffalo, New York, and have been an Investigator with the NYSAG since 1995. During my work with the NYAG, I have had the opportunity to conduct, coordinate and/or participate in over fifty (50) investigations relating to the sexual exploitation of children. I have also had the opportunity to observe and review numerous examples of child pornography in all forms of media including computer media. I make this affidavit in support of an application for a search warrant for a computer system located at 1 Hunington Quadrangle, Suite 2S12, Caraccia and Co. CPA's, in the City of Melville, County of Suffolk, State of New York. There is probable cause to believe that a search of this premises will result in the seizure of evidence relating to the possession, receipt and transmission of images depicting sexual conduct by a child less than sixteen years of age in violation of New York State Penal Law, Article 263. A number of those computer graphic images were "posted" to the Usenet Newsgroups via the internet, hereafter

known as Usenet, and made available to various members/users of Usenet.

2. I have been assisted in this investigation by Special Agent (SA) Steven MacMartin of the United States Customs Service (USCS) who is currently assigned to the Office of the Special Agent in Charge, Buffalo, New York and who has been an officer of the USCS for approximately seventeen (17) years. SA MacMartin is currently acting as the Child Pornography Investigation Coordinator for the Special Agent-in-Charge, Buffalo, NY, and has had the opportunity to conduct, coordinate and participate in over one hundred (100) investigations relating to the sexual exploitation of children. He has also had the opportunity to observe and review numerous examples of child pornography in all forms of media including computer media, to discuss and review these materials with endocrinologists and pediatricians, and has received training and instruction from experts in the field of investigation of child pornography. I have also been assisted by Investigator Martin J. Harrington currently assigned to the Attorney General's Organized Crime Task Force. Inv. Harrington worked for the Buffalo Police Department for 24 years, including 17 years as a detective with the Vice and Narcotics Unit, during which time he had the opportunity to conduct, coordinate and/or participate in numerous investigations relating to the exploitation of children.

3. Your affiant, along with SA MacMartin, other USCS agents, Investigators with the NYSAG's OCTF and the New York State Police, are responsible for investigating violations of Customs and other federal laws as well violations of New York State Penal Law. This includes violations of federal law regarding the importation and knowing receipt of prohibited and/or restricted merchandise, including child pornography and material related to the sexual exploitation of

children as well as violations of New York State laws regarding the Sexual Performance by a Child. As an Investigator for the NYSAG your affiant is authorized to investigate activities involving New York State Penal Law violations involving the Sexual Performance by a Child pursuant to New York State Penal Law, Article 263. Section 263.15 makes it a class D felony for any person, knowing the character and content thereof, to produce, direct or promote any performance which includes sexual conduct by a child less than sixteen years of age. In addition, since November 1, 1996, it has been a class E Felony to possess such materials (New York State Penal Law, Section 263.11).

4. Your affiant has fully discussed the facts and circumstances surrounding this investigation with Inv. Harrington and SA MacMartin who have overseen an undercover investigation out of the Buffalo Office of USCS. Your affiant has participated in the undercover operation with Customs since March, 1996. The investigation surrounds the transmission and receipt of child pornography across county, state and national boundaries through the use of Usenet Newsgroups ("Usenet"). Usenet is essentially a multi-user Bulletin Board Service ("BBS") which allows its users to create and transmit (Post) articles or messages to the Newsgroup. The postings are then accessed by other users of Usenet. Usenet also allows users to post and attach computer files in various forms including computer generated graphic image files. In order for transmissions to occur, each Usenet user has some form of Internet access and is identified with a "screen name" consisting of a combination of letters and/or numbers selected by the customer. The "suspect" subject to this investigation has been identified as using the following "screen name":

CUKYLUVR.

## DEFINITIONS

5. New York State Penal Law, Section 263.00, et. seq. defines, for the purposes of Section 263.15, and/or Section 26.11 the following terms:

(1) "Sexual Performance" means any performance or part thereof which includes sexual conduct by a child less than sixteen (16) years of age;

(3) "Sexual Conduct" means actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sadomasochistic abuse, or lewd exhibition of the genitals

(4) "Performance" means any play, motion picture, photograph or dance. Performance also means any other visual representation exhibited before an audience.

(5) "Promote" means to procure, manufacture, issue, sell, give, provide, lend, mail, deliver, transfer, transmute, publish, distribute, circulate, disseminate, present, exhibit or advertise, or to offer or agree to do the same.

6. For purposes of this affidavit, unless otherwise specifically indicated, the term "computer" refers to the box that houses the central processing unit (CPU), along with any internal storage devices (such as internal hard drives) and internal communications devices (such as internal modems capable of sending/receiving electronic mail or FAX cards) along with any other hardware stored or housed internally. Thus, "computer" refers to hardware, software and data contained in the main unit. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package, the term "computer system" is used. Information refers to all the information on a computer system including both software applications and data.

7. The term "computer hardware" as used in this affidavit refers to all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices; peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

8. The term "computer software" as used in this affidavit refers to digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

9. The term "computer-related documentation" used in this affidavit refers to written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.



10. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric, or other special, characters) usually operates as a "digital key" to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

#### INTERNET SERVICE PROVIDERS (ISPs)

11. Based upon your affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your affiant knows that the INTERNET is a world wide computer network which connects computers and allows communications and the transfer of data and information across state and national boundaries. Individuals that utilize the INTERNET can communicate by using electronic mail (hereinafter referred to as "E-mail"). E-mail is an electronic form of communication which can contain letter type correspondence and graphic images. E-mail is similar to conventional paper type mail in that it is addressed from one individual to another and is usually private. E-mail usually contains a message header which gives information about the individual that originated a particular message or graphic, and importantly, the return address to respond to them. Individuals that have an INTERNET E-mail address have a subscription to, membership, or affiliation with, an organization or commercial

service which provides access to the INTERNET computer network. A provider of INTERNET access is referred to as an INTERNET SERVICE PROVIDER or ISP.

### USENET NEWSGROUPS

12. Based upon your affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your affiant knows that Usenet Newsgroups is an intergral part of communication on the Internet. Newsgroups allow the user to take part in communities of people interested in particular topics. Newsgroups are similiar to electronic message board services or electronic bulletin boards. In fact, the newsgroups are very similiar to the physical bulletin boards located at places such as grogery stores where people are free to post and retrieve messages in printed hard copy. The major difference is that since these newsgroups are distributed through the Internet, one can find over 30,000 topics and millions of people, in these globe-spanning discussions. A user of a newsgroup can read postings of interest, or can participate in posting discussions. Newsgroup names usually reflect their focus. For example, Alt.Sex.Pedophilia, Alt.Sex.Incest, Alt.Sex.Teen. When a user posts a newsgroup message, readers around the world will be able to read and respond to it.

13. In addition to posting messages, a user of newsgroups can attach computer files, including but not limited to, graphic image files to their posting to allow a reader of the post to download that attached computer file.

## CONDUCT OF INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY

14. Pursuant to my training and experience, as well as the training and experience of other law enforcement personnel, I have learned that:

a) Child pornography is not readily available in retail establishments; accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contact with other individuals who have it available.

b) The use of computers to traffic in, trade, collect child pornography and obscenity has become one of the preferred methods of obtaining obscene and child pornographic materials. An individual familiar with a computer can use it, usually in the privacy of his own home or office, to interact with another individual or a business offering such materials in this country or elsewhere in the world. The use of a computer provides individuals interested in obscenity or child pornography with a sense of privacy and secrecy not attainable by other media. It also permits the individuals to contact and interact with many more individuals than through the use of the mails.

c) Persons involved in sending or receiving child pornography tend to retain it for long periods of time. The images obtained, traded and/or sold are prized by those individuals interested in child pornography. In addition to their "emotional" value, the images are intrinsically valuable as trading/selling material and therefore are rarely

destroyed or deleted by the individual collector. Graphic image files can be maintained on the computers built-in hard drive or on storage disks. This tendency is enhanced by the increased sense of security that a computer affords.

### THE UNDERCOVER INVESTIGATION

14. On March 7, 1996, the USCS office of the Special Agent in Charge, Buffalo, NY began an undercover investigation into the transmission of child pornographic images involving the "INTERNET", under the direction of SA MacMartin. The INTERNET is a world wide computer network which connects computers and allows communications and the transfer of data and information across state and national boundaries. Individuals that utilize the INTERNET can communicate via the usenet as described above. The experience of SA Steven MacMartin, your affiant, and other agents and investigators is that the "INTERNET" is the newest and most popular medium by which child pornographic images are transmitted and/or traded.

15. During this investigation, the agents have participated in newsgroup activities on hundreds of newsgroup topics. Agents have downloaded and/or viewed hundreds of newsgroup postings many of which have contained computer generated graphic images which depict child pornography.

16. The standard operating procedure of the undercover operation has been that agents of the SAC/BU, and those investigative agencies working with agents of the SAC/BU, sign onto the Internet and participate in the activity which occurs in newsgroups known to be frequented by

users who desire to collect and post computer generated graphic images which depict preteen child pornography. Examples of such newsgroups are: Alt.binaries.pictures.erotica.early-teens.

Based on all of the previously observed activity in the above described newsgroup, it appears that the main goal of the participants in these newsgroup is to post and download computer generated graphic images of preteen child pornography among themselves. SAC/BU agents observe this activity and download and investigate the postings.

17. **CUKYLUVR**: On May 24, 1997, while participating in the activity available on the INTERNET Usenet Newsgroup Alt.binaries.pictures.erotica.early-teens, an individual, known by the e-mail address Cukyluvr@Luv.the.news, posted twenty (20) messages determined to contain twenty (20) computer generated graphic images depicting child pornography to the above referenced newsgroup. Specifically on May 24, 1997, Agents from USCS SAC Buffalo had accessed the Usenet Newsgroup Alt.binaries.pictures.erotica.early-teens, and observed numerous postings from **CUKYLUVR** which had computer generated graphic files attached. Agents were successful in downloading such postings. The following graphic image files were attached to postings by **CUKYLUVR** and downloaded to a computer terminal in Erie County: blosex55.jpg; blosex56.jpg; blosex58.jpg; joy02.jpg; joy03.jpg; joy03a.jpg; joy03b.jpg; ll-e1-15.jpg; ll-e1-29.jpg; ll-e1-af.jpg; ll-n1-08.jpg; ll-n1-11.jpg; ll-n3f22.jpg; ll-n3f23.jpg; ll-n3f25.jpg; ll-n4-40.jpg; ll-n3f24b.jpg; mt1a001.jpg; mt1a005.jpg; and mt1a025.jpg. A copy of the graphic image files are attached to this affidavit as Exhibit "A."

18. Your affiant states that based upon my experience in the undercover operation, as well as the training and experience of SA MacMartin and Investigator Harrington, the majority of the

graphic images referred to in paragraph 17 above depict children under the age of sixteen engaged in sexual conduct as defined by the New York Penal Law. These graphic images were posted to the Usenet Newsgroup Alt.binaries.pictures.erotica.early-teens by CUKYLUVR and it is more likely than not that he has retained these graphic images.

19. On May 24, 1997, an investigation was begun regarding the identity of the screen name CUKYLUVR@luv.the.news. It was determined from an analysis of the information contained in the posting message that the screen name address CUKYLUVR@luv.the.news was a fictitious Internet address. The investigation revealed that the postings were being transmitted from the Internet Service Provider (ISP) Tofu.Alt.Net. Information was developed which revealed that Tofu.alt.net was owned and operated by Altopia Corporation, Seattle Washington.

20. Information provided by subpoena from Altopia Corporation revealed that CUKYLUVR was subscribed to by Stephen J. Caraccia. The information revealed that the account was active and that it had been established on March 3, 1997. Although Altopia Corporation does not require a subscriber to furnish an address to sign up with Altopia, the information indicated that the customer claimed to be a resident of New York State. The information further revealed that Stephen J. Caraccia's Internet address was Caraccia@ix.netcom.com.

21. Information provided by subpoena from Netcom.com revealed that Caraccia@ix.netcom.com was subscribed to by Stephen J. Caraccia, Caraccia & Co. CPA's, 1 Hunington Quadrangle, Melville, NY 11747-4407, telephone number 516-249-6439.

22. Based upon information obtained by subpoena from NYNEX, your affiant conducted an analysis of the Local Usage records for 516-249-6439, subscribed to by Caraccia and Co. CPA's, 1 Huntington Quadrangle, Suite 2S12, Melville, New York. The information reveals that on 05/23/97 at approximately 2:02 p.m., 516-249-6439 place a call to 516-633-6470. Your affiant states that the later telephone number, 516-633-6470 is a Netcom.com access number which allows a computer modem to connect to the Netcom server. Therefore it is more likely than not that the computer used in the transmission of the computer graphic image files is located at 1 Huntington Quadrangle, Suite 2S12, Melville, New York

23. According to the records of the New York State Department of Motor Vehicles, Stephen J. Caraccia, date of birth 7/24/63, possesses a valid New York State driver's license, that indicates a P.O. Box 580, Syosset, New York.

24. According US Postal Inspectors, P.O. Box 580, Syosset, New York is subscribed to by Stephen Caraccia, 227 Jackson Avenue, Syosset, New York . The post box subscription also has a reach telephone number of 516-249-6410. Telephone records reveal that 516-249-6410 is the main telephone number for Caraccia and Co. CPA's, 1 Hunington Quadrangle, Melville, New York.

25. Investigators from the New York State Attorney Generals Office conducted a surveillance of Caraccia and Co. CPA's, 1 Hunington Quadrangle, Meville, NY. The business is described as

a three sets of three buildings, each comprised of a North, Central and South building. Caraccia and Co. CPA's is located in building number 1. Caraccia and Co. CPA's is located in the West Corridor on the second floor in building number 1. The suite number "2S12" is located on a blond wood door. In addition, the names BART & SCHWARTZ ATTORNEY AT LAW, CARACCIA AND CO, CPAS, and LB MANAGEMENT CO are printed in silver block style letters. Attached as Exhibit "B."

26. Your affiant states that based upon my experience, as well as the training and experience of Deputy Chief Investigator Harrington, the majority of the graphic images referred to in paragraph 17 above depict children under the age of sixteen engaged in sexual conduct as defined by the New York Penal Law. These graphic images were posted to the USENET newsgroup by "CUKYLVR" and it is more likely than not that he has retained these graphic images.

27. Your affiant states that the above subscriber information and related material indicates that it is more likely than not that the computer utilized to promote the sexual performance by a child less than 16 years of age is located at Caraccia and Co, CPA's, 1 Huntington Quadrangle, Suite 2S12, Melville, New York.

**CPL, SECTION 690.35(4)(b) "NO KNOCK" REQUEST**

28. Based upon information developed during this investigation, it is possible that other individuals may have access to the computer which contains copies of the graphic image files maintained by the individual responsible for their transmission, receipt and storage.



29. Based upon my experience and training, as well as the experience and training of other investigators trained in the search, seizure, storage and retrieval of computer data, your affiant states that the "evidence" or property sought may be easily and quickly destroyed or disposed of by an individual utilizing a short series of key strokes or computer commands. In addition, an individual may be able to activate "booby-traps" or other forms of computer security programs which could render the data sought inaccessible or unusable, as well as reverse the process to restore it.

#### CONCLUSION

30. Based upon your affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting.

31. Based upon the foregoing, there is probable cause to believe that the files, documents, and attachments identified in ¶ 14-24, and business records and related documents pertaining to the acquisition, possession and distribution of graphic computer images depicting the sexual performance/sexual conduct of children less than 16 years of age in violation of Article 263 of the New York Penal Law are located on the premises at Caraccia and Co, CPA's, 1 Huntington

Quadrangle, Suite 2S12, Melville, County of Suffolk, State of New York.

32. There is further probable cause to believe that these records are maintained in files, computer storage facilities or other data storage facilities, and that, within these files, there are records--namely, correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles, documents, photographs, negatives, photographic slides or other visual depictions or equipment--used to depict child pornography materials.

33. Additionally, your affiant believes that evidence of violations of N.Y. Penal Law, Section 263 are contained or concealed in the tapes, cassettes, cartridges, streaming tape, commercial software and manuals, hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk applications programs, data disks, system disk operating systems, magnetic media-floppy disks, tape systems and hard drive and other computer related operating equipment, which depict or are used to depict child pornographic materials contrary to the laws of New York State.

34. Based on all the foregoing, there is probable cause to believe that child pornography, and other evidence of the use of computers to possess and promote the sexual performance/sexual conduct by a child less than 16 years of age set forth in the attached search warrant, will be found on the premises located Caraccia and CO, CPA's, 1 Huntington Quadrangle, Suite 2S12, Melville, New York and under the control of individual or individuals therein, and/or other individuals unknown, and that those items of child pornography constitute evidence of the sexual

performance/sexual conduct by children under the age of sixteen (16) years of age contrary to the laws of New York State.

WHEREFORE, your affiant respectfully requests that a warrant be issued authorizing Investigators of the New York State Attorney General's OCTF and the New York State Police, with the appropriate assistance from other law enforcement officers, to enter the premises at Caraccia and CO, CPA's, County of Suffolk, State of New York. and therein search and seize the following items:

1. Visual depictions: blosex55.jpg; blosex56.jpg; blosex58.jpg; joy02.jpg; joy03.jpg; joy03a.jpg; joy03b.jpg; ll-e1-15.jpg; ll-e1-29.jpg; ll-e1-af.jpg; ll-n1-08.jpg; ll-n1-11.jpg; ll-n3f22.jpg; ll-n3f23.jpg; ll-n3f25.jpg; ll-n4-40.jpg; ll-n3f24b.jpg; mt1a001.jpg; mt1a005.jpg; and mt1a025 and or other computer graphic files which depict children in a sexually explicit manner contrary to law.

2. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices such as computer disks, magnetic media-floppy disks, tape systems, hard drives, disk drives, tape drives, transistor-like binary devices, and other memory storage devices; and any external attachments peripheral input/output devices such as keyboards, printers, scanners, plotters, video display monitors, and optical readers; and related communications devices such as modems, cables and connections, recording equipment, RAM or

ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

3. Computer software, that is, digital information which can be interpreted by a computer and any of its related components, which may be stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics , or spreadsheet programs), utilities, compilers, interpreters, and communications programs; computer related documentation, that is, written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

4. Business records, correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles, documents which reflect the receipt, purchase, transmission and/or distribution of materials depicting children in a sexually explicit manner.

5. Any, photographs, negatives, photographic slides or other visual depictions or equipment, used to depict child in a sexually explicit manner.

SEALING OF THIS AFFIDAVIT

35. It is respectfully requested that because this investigation is on-going and may be compromised by disclosure of this application that the Court issue an order pursuant to which this Application by Affidavit be filed and maintained under seal until further order of this Court.

---

MICHAEL G. McCARTNEY

Investigator, New York State Attorney General's Office

Sworn to and subscribed before

me this \_\_\_\_\_ day of January, 1998.

---

\*\*\*\*\* , Judge

\*\*\*\*\* Court

New York, New York

STATE OF NEW YORK  
\*\*\*\*\* COURT : COUNTY OF NEW YORK

---

In the Matter of the Application  
for a Search Warrant Authorizing the  
Search of residence located at 253 Ramona  
Avenue, in the City of Staten Island,  
County of Richmond, State of New York.

---

**APPLICATION BY AFFIDAVIT  
FOR A SEARCH WARRANT**

STATE OF NEW YORK     )  
COUNTY OF ERIE        )     SS.:  
CITY OF BUFFALO        )

Michael G. McCartney, being first duly sworn, hereby deposes and states as follows:

**INTRODUCTION**

1. I am an Investigator with the New York State Attorney General's Office Criminal Division currently assigned to the Criminal Prosecutions Bureau (hereinafter "NYSAG"), Buffalo, New York, and have been an Investigator with the NYSAG since 1995. During my work with the NYSAG, I have had the opportunity to conduct, coordinate and/or participate in over fifty (50) investigations relating to the sexual exploitation of children. I have also had the opportunity to observe and review numerous examples of child pornography in all forms of media including computer media. I make this affidavit in support of an application for a search warrant for a computer system located at 253 Ramona Avenue, Staten Island, New York, in the County of Richmond, State of New York. There is probable cause to believe that a search of this premises will result in the seizure of evidence relating to the possession, receipt and transmission of images depicting sexual conduct by a child less than sixteen years of age in violation of New York State Penal Law, Article 263. A number of those computer graphic images were transmitted via the Internet, utilizing the Internet service provider "America On Line", located in

Vienna, Virginia, hereafter known as AOL, to various members/subscribers of AOL.

2. Your affiant, along with other investigators of the OCTF and with Investigators with the New York State Police, Special Investigations Unit (hereinafter "NYSP-SIU") have been investigating violations of New York State Penal Law relative to child pornography and material related to the sexual exploitation of children as well as violations of New York State laws regarding the Sexual Performance by a Child. As an Investigator for the NYSAG, your affiant is authorized to investigate activities involving New York State Penal Law violations involving the Sexual Performance by a Child pursuant to New York State Penal Law, Article 263. Section 263.15 makes it a class D felony for any person, knowing the character and content thereof, to produce, direct or promote any performance which includes sexual conduct by a child less than sixteen years of age. Section 263.11 makes it a Class E Felony for any person, knowing the character and content thereof, to possess such materials.

3. The investigation surrounds the transmission and receipt of child pornography across county, state, and national boundaries through the use of electronic mail (hereinafter referred to as "E-mail"). Furthermore, the suspect involved in such transmissions and/or receipt of such transmissions utilized an electronic communications service provider known as "America Online" located in Vienna, Virginia. All such transmissions must go through AOL's server located in Vienna where such transmissions are temporarily stored by AOL. Furthermore, all of the persons who transmitted or received the E-mail hereinafter described have or had accounts with AOL.

4. In order for transmissions to occur, each AOL customer has a "screen name" consisting of a combination of letters and/or numbers selected by the customer. The "suspect" subject to this investigation has been identified as using the following screen name of "GINTHEPIT". This suspect has sent and received from/at a residence in Staten Island New York, computer graphic images of children less than 16 years of age engaged in sexual conduct , via AOL, to and from other members/subscribers of AOL .

### DEFINITIONS

5. New York State Penal Law, Section 263.00, et. seq. defines, for the purposes of Section 263.15, and/or Section 263.11 the following terms:

- (1) "Sexual Performance" means any performance or part thereof which includes sexual conduct by a child less than sixteen (16) years of age;
- (2) "Sexual Conduct" means actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sadomasochistic abuse, or lewd exhibition of the genitals.
- (3) "Performance" means any play, motion picture, photograph or dance. Performance also means any other visual representation exhibited before an audience.
- (4) "Promote" means to procure, manufacture, issue, sell, give, provide, lend, mail, deliver, transfer, transmute, publish, distribute, circulate, disseminate, present, exhibit or advertise, or to offer or agree to do the same.

6. For purposes of this affidavit, unless otherwise specifically indicated, the term "computer" refers to the box that houses the central processing unit (CPU), along with any internal storage devices (such as internal hard drives) and internal communications devices (such as internal modems capable of sending/receiving electronic mail or FAX cards) along with any other hardware stored or housed internally. Thus, "computer" refers to hardware, software and



data contained in the main unit. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package, the term "computer system" is used. Information refers to all the information on a computer system including both software applications and data.

7. The term "computer hardware" as used in this affidavit refers to all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices; peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

8. The term "computer software" as used in this affidavit refers to digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics , or

spreadsheet programs), utilities, compilers, interpreters, and communications programs.

9. The term "computer-related documentation" used in this affidavit refers to written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

10. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric, or other special, characters) usually operates as a "digital key" to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

#### **INTERNET SERVICE PROVIDERS (ISPs)**

11. Based upon your affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your affiant knows that the INTERNET is a world wide computer network which connects computers and allows communications and the transfer of data and information across county, state and national boundaries. Individuals that utilize the INTERNET can communicate by using E-mail. E-mail is an electronic form of communication

which can contain letter type correspondence and graphic images. E-mail is similar to conventional paper type mail in that it is addressed from one individual to another and is usually private. E-mail usually contains a message header which gives information about the individual that originated a particular message or graphic, and importantly, the return address to respond to them. E-mail may have attachments which take the form of additional text or graphic images.

12. The visual depictions referred to below are in the form of "computer graphic files". All of the E-mail described below contained "attached" computer graphic files and such files were photographs that have been digitalized into computer binary format. Once in this format the graphic file can be viewed, copied, transmitted, and/or printed. Computer graphic files are differentiated by the type of format convention by which they were created. Two common types of computer graphic files encountered are those in JPEG (Joint Photographic Electronics Group) format having the ".jpg" file extension, and the GIF (Graphic Interchange Format) format having the ".gif" file extension. In addition, there are two primary video graphic files which can display motion picture graphics. The formats encountered are in AVI (Audio Visual Interleaved) format having the ".AVI" file extension, and MPEG (Motion Picture Experts Group) format having the ".MPG" file extension. There are also other formats.

13. I am aware that individuals that have an INTERNET E-mail address must have a subscription to, membership, or affiliation with, an organization or commercial service which provides access to the INTERNET computer network. A provider of INTERNET access is referred to as an INTERNET SERVICE PROVIDER or ISP. One such ISP is AOL.

## CONDUCT OF INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY

14. Pursuant to my training and experience, as well as the training and experience of other law enforcement personnel, I have learned that:

a) Child pornography is not readily available in retail establishments; accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contact with other individuals who have it available.

b) The use of computers to traffic in, trade, collect child pornography and obscenity has become one of the preferred methods of obtaining obscene and child pornographic materials. An individual familiar with a computer can use it, usually in the privacy of his own home or office, to interact with another individual or a business offering such materials in this country or elsewhere in the world. The use of a computer provides individuals interested in obscenity or child pornography with a sense of privacy and secrecy not attainable by other media. It also permits the individuals to contact and interact with many more individuals than through the use of the mails.

c) Persons involved in sending or receiving child pornography tend to retain it for long periods of time. The images obtained, traded and/or sold are prized by those individuals interested in child pornography. In addition to their "emotional" value, the images are intrinsically valuable as trading/selling material and therefore are rarely destroyed or deleted by the individual collector. Graphic image files can be maintained on the computers built-in hard drive or on storage disks. This tendency is enhanced by

the increased sense of security that a computer affords.

### THE INVESTIGATION

15. On March 7, 1996, the United States Customs Service (hereinafter "USCS") in Buffalo, NY began an undercover investigation into the transmission and receipt of child pornographic images involving the INTERNET. Individuals that utilize the INTERNET can communicate by using E-mail. On or about March 14, 1996, Investigators from the NYSAG began working jointly with USCS in this undercover operation. Since October 1, 1996, Investigators from the NYSP-SIU have also been assisting in the investigation. It is the experience of your affiant that the "INTERNET" is the newest and most popular medium by which child pornographic images are transmitted and/or traded.

16. In this undercover operation, agents of the USCS, investigators of the NYSAG and the NYSP-SIU have actively participated in conversations held on the ISP AOL. As noted earlier, an ISP is an organization or commercial service which provides access to the INTERNET computer network; AOL is such a provider.

17. This investigation has resulted in the execution of over 100 search warrants, 35 arrests, and 30 convictions worldwide. During the undercover operation, investigators were physically located in Erie County, New York, were logged onto AOL and would converse with persons for the purpose of trading child pornographic material among other pedophiles. Investigators have conversed electronically with numerous suspects about trading child pornography and have received thousands of images. Your affiant has reviewed hundreds of the images traded and which, based on the training and experience of your affiant, depict the sexual

performance/sexual conduct by a child less than 16 years of age as defined in the New York State Penal Law.

18. Deputy Chief Investigator Martin J. Harrington, NYSAG, was informed by John Ryan, Assist General Counsel for AOL that an individual using the screen name "GINTHEPIT" was sending suspect graphic images over the INTERNET via AOL. AOL provided documentation that on August 10, 1997 at 2:55 a.m., "GINTHEPIT" sent a file entitled "!!!11TAMM.JPG" through AOL E-Mail to 22 separate AOL screen names. A copy of this picture is attached as Exhibit "A". AOL also provided documentation that on August 10, 1997 at 2:52 a.m., "GINTHEPIT" sent a file entitled "09PEE.JPG" through AOL E-Mail to 22 separate AOL screen names. A copy of this picture is attached as Exhibit "B".

19. On September 9, 1997, Investigators from the NYSAG, while located at a computer terminal in Erie County, New York, using an undercover identity (Investigators) had a typed, electronically transmitted conversation (E-mail) with a person or persons using the screen name "GINTHEPIT." During the E-Mail conversation on September 9, 1997, Investigators asked "GINTHEPIT" if he wanted to trade pictures. On September 11, 1997, at 2:29 p.m., a person or persons using the screen name "GINTHEPIT" composed an E-Mail which stated that "i love to trade and i have a large selection also." Your affiant states that this reference to trading and having a "large selection" refers to "GINTHEPIT" have a large selection of child pornography on his computer.

20. Based upon my experience and training the graphic images referred to above,

including those sent to and those received by "GINTHEPIT" depict the sexual performance/sexual conduct of a child less than 16 years of age.

21. Based upon my experience and training it is more likely than not that the files sent and received by "GINTHEPIT" remain in the computer's internal hard drive and/or on computer hardware such as storage disks unless these files have been specifically "deleted" by "GINTHEPIT". However, because these files and images are valuable to those who possess them, continued on-going, long-term possession is more likely than not.

22. AOL provided the following information for the individual using the screen name "GINTHEPIT": The AOL account is subscribed to by Michael Plotkin, 253 Romona Avenue, Staten Island, NY; day and evening telephone phone is (718) 966-8116; the method of payment is listed as Visa in the name of Michael Plotkin at that address. AOL account information also revealed that the account was active and listed screen names as follows: "GINTHEPIT"; "BoZoNe10".

23. According to the records of the New York State Department of Motor Vehicles, Michael Plotkin, date of birth 3/12/79, has a valid New York State Driver's License permit and lists an address as 253 Romona Avenue, Staten Island, NY.

24. According to the business records of Bell Atlantic, (718) 966-8116 is subscribed to by T Plotkin, 253 Romona Avenue, Staten Island, County of Richmond, State of New York.

25. According to the records of AOL, on September 11, 1997 at 2:11 p.m., "GINTHEPIT" signed on to the AOL system and remained on line for 16 minutes.

26. According to the business records of Con Edison, Tyrone Plotkin has been the name on the account for the utilities bills at 253 Ramona Ave, Staten Island, New York since July 13, 1990.

27. On or about November 21, 1997, an Investigator from the New York State Attorney Generals Office conducted a surveillance of 253 Ramona Avenue, Staten Island, New York. The Investigator observed a 1998 Toyota, blue, bearing New York Registration H580NJ parked on the street in front of 253 Ramona Avenue. In addition, a 1996 BMW, red, bearing New York Registration N680KZ was parked in the driveway of 253 Ramona Avenue. According to New York State Department of Motor Vehicle records, H580NJ and N680KZ are registered to Tyrone A. Plotkin, 253 Ramona Avenue, Staten Island, New York, date of birth 11/10/51 Attached as Exhibit "C" are two photographs of the residence. The residence at 253 Ramona Avenue is described as a single family, single story wood frame structure with a brick front. The numbers "253" are located on the left side of the front door just above the mail box. The residence is on the west side of the street located mid-block between Nippon Avenue to the North and Huguenot Avenue to the South.

28. Your affiant states that based upon my experience and training, the majority of the graphic images referred to in paragraph 18 above depict children under the age of sixteen



engaged in sexual conduct as defined by the New York Penal Law. These graphic images were transmitted by "GINTHEPIT" and it is more likely than not that he has retained these graphic images.

29. Your affiant states that the above subscriber information and related material indicates that it is more likely than not that the computer utilized to promote the sexual performance by a child less than 16 years of age is located at 253 Ramona Avenue, in the City of Staten Island, County of Richmond, State of New York.

**CPL, SECTION 690.35(4)(b) "NO KNOCK" REQUEST**

30. Based upon information developed during this investigation, it is possible that other individuals may have access to the computer which contains copies of the graphic image files maintained by the individual responsible for their transmission, receipt and storage.

31. Based upon my experience and training, as well as the experience and training of other investigators trained in the search, seizure, storage and retrieval of computer data, your affiant states that the "evidence" or property sought may be easily and quickly destroyed or disposed of by an individual utilizing a short series of key strokes or computer commands. In addition, an individual may be able to activate "booby-traps" or other forms of computer security programs which could render the data sought inaccessible or unusable, as well as reverse the process to restore it.

## CONCLUSION

32. Based upon your affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting.

33. Based upon the foregoing, there is probable cause to believe that the above-mentioned files, documents, and attachments and business records and related documents pertaining to the acquisition, possession and distribution of graphic computer images depicting the sexual performance/sexual conduct of children less than 16 years of age in violation of Article 263 of the New York Penal Law are located on the premises at 253 Ramona Avenue, in the City of Staten Island, County of Richmond, State of New York.

34. There is further probable cause to believe that these records are maintained in files, computer storage facilities or other data storage facilities, and that, within these files, there are records--namely, correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles, documents, photographs, negatives, photographic slides or other visual depictions or equipment--used to depict child pornography materials.

35. Additionally, your affiant believes that evidence of violations of N.Y. Penal Law, Section 263 are contained or concealed in the tapes, cassettes, cartridges, streaming tape, commercial software and manuals, hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk applications programs, data disks, system disk operating systems, magnetic media-floppy disks, tape systems and hard drive and other computer related operating equipment, which depict or are used to depict child pornographic materials contrary to the laws of New York State.

36. Based on all the foregoing, there is probable cause to believe that child pornography, and other evidence of the use of computers to possess and promote the sexual performance/sexual conduct by a child less than 16 years of age set forth in the attached search warrant, will be found on the premises located at 253 Ramona Avenue, in the City of Staten Island, County of Richmond, State of New York and under the control of individual or individuals therein, and/or other individuals unknown, and that those items of child pornography constitute evidence of the sexual performance / sexual conduct by children under the age of sixteen (16) years of age contrary to the laws of New York State.

WHEREFORE, your affiant respectfully requests that a warrant be issued authorizing Investigators of the New York State Attorney General's Office and the New York State Police, with the appropriate assistance from other law enforcement officers, to enter the premises located at 253 Ramona Avenue, in the City of Staten Island, County of Richmond, State of New York and therein search and seize the following items:

1. Visual depictions: “!!!TAMM.JPG” and “09PEE.JPG” or other computer graphic files which depict children in a sexually explicit manner contrary to law.

2. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices such as computer disks, magnetic media-floppy disks, tape systems, hard drives, disk drives, tape drives, transistor-like binary devices, and other memory storage devices; and any external attachments peripheral input/output devices such as keyboards, printers, scanners, plotters, video display monitors, and optical readers; and related communications devices such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

3. Computer software, that is, digital information which can be interpreted by a computer and any of its related components, which may be stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs; computer related documentation, that is, written, recorded, printed,

or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

4. Business records, correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles, documents which reflect the receipt, purchase, transmission and/or distribution of materials depicting children in a sexually explicit manner.

5. Any photographs, negatives, photographic slides or other visual depictions or equipment, used to depict child in a sexually explicit manner.

**SEALING OF THIS AFFIDAVIT**

45. It is respectfully requested that because this investigation is on-going and may be compromised by disclosure of this application that the Court issue an order pursuant to which this Application by Affidavit be filed and maintained under seal until further order of this Court.

\_\_\_\_\_  
MICHAEL G. McCARTNEY

Investigator, New York State

Attorney General's Office

Sworn to and subscribed before  
me this \_\_\_ day of January, 1998.

\_\_\_\_\_  
, Judge  
Court

Buffalo, New York

STATE OF NEW YORK  
SUPREME COURT : COUNTY OF ERIE

---

In the Matter of the Application of  
Michael G. McCartney, for a Search  
Warrant Authorizing the Search of an  
apartment residence, located at  
573 Grand Street, Apartment D 1204  
in the City of New York, County of New York,  
State of New York.

---

**APPLICATION BY AFFIDAVIT  
FOR SEARCH WARRANT**

STATE OF NEW YORK)  
COUNTY OF ERIE ) SS.:  
CITY OF BUFFALO )

Michael G. McCartney, being first duly sworn, hereby deposes and states as follows:

**INTRODUCTION**

1. I am an Investigator with the New York State Attorney General's Office currently assigned to the Organized Crime Task Force (hereinafter NYSAG-OCTF), Buffalo, NY and have been an Investigator with the NYSAG-OCTF since 1995. During my work with the NYSAG-OCTF, I have had the opportunity to conduct, coordinate and/or participate in investigations relating to the sexual exploitation of children. I have also had the opportunity to observe and review numerous examples of child pornography in all forms of media including computer media. I make this affidavit in support of an application for a search warrant of an apartment residence, located at 573 Grand Street, Apartment D 1204 in the City of New York, County of New York, State of New York. There is probable cause to believe that a search of this premises will result in the seizure of evidence relating to the possession, receipt and transmission of images depicting the sexual performance by a child less than sixteen years of

age in violation of New York State Penal Law, Article 263.00 et seq. A number of those computer graphic images were transmitted via the internet from that residence in New York City to a computer located in Erie County.

2. I have been assisted in this investigation by Special Agent (SA) Steven MacMartin of the United States Customs Service (USCS) who is currently assigned to the Office of the Special Agent in Charge, Buffalo, New York and who has been an officer of the USCS for approximately sixteen (16) years. SA MacMartin is currently acting as the Child Pornography Investigation Coordinator for the Special Agent-in-Charge, Buffalo, NY, and has had the opportunity to conduct, coordinate and participate in over thirty investigations relating to the sexual exploitation of children. He has also had the opportunity to observe and review numerous examples of child pornography in all forms of media including computer media, to discuss and review these materials with endocrinologists and pediatricians, and has received training and instruction from experts in the field of investigation of child pornography. I have also been assisted by Investigator Martin J. Harrington currently assigned to the Attorney General's Organized Crime Task Force. Inv. Harrington worked for the Buffalo Police Department for 24 years, including 17 years as a detective with the Vice and Narcotics Unit, during which time he had the opportunity to conduct, coordinate and/or participate in numerous investigations relating to the exploitation of children.

3. Your affiant, along with SA MacMartin, other USCS agents, Investigators with the NYSAG's OCTF and the New York State Police, are responsible for investigating violations of Customs and other federal laws as well violations of New York State Penal Law. This includes violations of federal law regarding the importation and knowing receipt of prohibited

and/or restricted merchandise, including child pornography and material related to the sexual exploitation of children as well as violations of New York State laws regarding the Sexual Performance by a Child. As an Investigator for the NYSAG-OCTF your affiant is authorized to investigate activities involving New York State Penal Law violations involving the Sexual Performance by a Child pursuant to New York State Penal Law, Article 263. Section 263.15 makes it a class D felony for any person, knowing the character and content thereof, to produce, direct or promote any performance which includes sexual conduct by a child less than sixteen years of age. In addition, since November 1, 1996, it has been a class E Felony to possess such materials (New York State Penal Law, Section 263.11).

4. Your affiant has fully discussed the facts and circumstances surrounding this investigation with Inv. Harrington and SA MacMartin who have overseen an undercover investigation out of the Buffalo Office of USCS. Your affiant has participated in the undercover operation with Customs since March, 1996. The investigation surrounds the transmission and receipt of child pornography across county, state and national boundaries through the use of electronic mail (e-mail). Furthermore, the suspects involved in such transmissions and/or receipts utilize an electronic communication service-provider known as "America Online" located in Vienna, Virginia. All such transmissions must go through America Online's server located in Vienna where such transmissions are temporarily stored by America Online. Furthermore, all of the persons who transmitted or received the e-mail hereinafter described have or had accounts with America Online. In order for transmissions to occur, each America Online customer has a "screen name" consisting of a combination of letters and/or numbers selected by the customer. The "suspect" subject to this investigation



has been identified as using the following "screen name": NateTSnake. This "suspect" has sent, from an apartment residence in the City of New York, computer graphic images of children less than 16 years of age engaged in a sexual performance, via America OnLine, to a computer located in Erie County, New York.

#### DEFINITIONS

5. New York State Penal Law, Section 263.00, et. seq. defines, for the purposes of Section 263.15, the following terms:

- (1) "Sexual Performance" means any performance or part thereof which includes sexual conduct by a child less than sixteen (16) years of age;
- (3) "Sexual Conduct" means actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sadomasochistic abuse, or lewd exhibition of the genitals
- (4) "Performance" means any play, motion picture, photograph or dance. Performance also means any other visual representation exhibited before an audience.
- (5) "Promote" means to procure, manufacture, issue, sell, give, provide, lend, mail, deliver, transfer, transmute, publish, distribute, circulate, disseminate, present, exhibit or advertise, or to offer or agree to do the same.

6. For purposes of this affidavit, unless otherwise specifically indicated, the term "computer" refers to the box that houses the central processing unit (CPU), along with any internal storage devices (such as internal hard drives) and internal communications devices (such as internal modems capable of sending/receiving electronic mail or FAX cards) along with any other hardware stored or housed internally. Thus, "computer" refers to hardware, software and data contained in the main unit. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as

peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package, the term "computer system" is used. Information refers to all the information on a computer system including both software applications and data.

7. The term "computer hardware" as used in this affidavit refers to all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices; peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

8. The term "computer software" as used in this affidavit refers to digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics , or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

9. The term "computer-related documentation" used in this affidavit refers to written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

10. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric, or other special, characters) usually operates as a "digital key" to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

#### **INTERNET SERVICE PROVIDERS (ISPs)**

11. Based upon your affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your affiant knows that the INTERNET is a world wide computer network which connects computers and allows communications and the transfer of data and information across county, state and national boundaries. Individuals that utilize the INTERNET can communicate by using electronic mail (hereinafter referred to as "E-mail"). E-mail is an electronic form of communication which can contain letter type correspondence and graphic images. E-mail is similar to conventional paper type mail in that it is addressed from one individual to another and is usually private. E-mail usually contains a message

header which gives information about the individual that originated a particular message or graphic, and importantly, the return address to respond to them.

12. The visual depictions referred to below are in the form of "computer graphic files". All of the E-mail described below contained computer graphic files and such files were photographs that have been digitized into computer binary format. Once in this format the graphic file can be viewed, copied, transmitted, and/or printed. Computer graphic files are differentiated by the type of format convention by which they were created. Two common types of computer graphic files encountered are those in JPEG (Joint Photographic Electronics Group) format having the "jpg" file extension, and the GIF (Graphic Interchange Format) format having the "gif" file extension. In addition, there are two primary video graphic files which can display motion picture graphics. The formats encountered are in AVI (Audio Visual Interleaved) format having the "AVI" file extension, and MPEG (Motion Picture Experts Group) format having the "MPG" file extension. There are also other formats.

13. Individuals that have an INTERNET E-mail address must have a subscription to, membership, or affiliation with, an organization or commercial service which provides access to the INTERNET computer network. A provider of INTERNET access is referred to as an INTERNET SERVICE PROVIDER or ISP. One such ISP is America Online.

### **THE UNDERCOVER INVESTIGATION**

14. On March 7, 1996, the USCS in Buffalo, NY began an undercover investigation into the transmission and receipt of child pornographic images involving the "INTERNET", under the direction of SA MacMartin. The INTERNET is a world wide computer network

which connects computers and allows communications and the transfer of data and information across county, state and national boundaries. Individuals that utilize the INTERNET can communicate by using electronic mail (hereinafter referred to as "E-mail"). On or about March 14, 1996, the NYSAG's office began working jointly with the U.S. Customs Service in this undercover operation. Since October 1, 1996, Investigators from the NYSP-SIU have also been assisting in the investigation. The experience of SA Steven MacMartin, your affiant, and other agents of the USCS, NYSAG-OCTF, and the NYSP-SIU is that the "INTERNET" is the newest and most popular medium by which child pornographic images are transmitted and/or traded.

15. In this undercover operation, agents of the USCS, investigators of the NYSAG's Organized Crime Task Force and the NYSP have actively participated in "chat room" conversations held on the INTERNET SERVICE PROVIDER known as America Online. As noted earlier, a ISP is an organization or commercial service which provides access to the INTERNET computer network; America Online (AOL) is such a provider.

16. During this investigation, the investigators would access AOL and enter specific "chat rooms"<sup>1</sup> within the AOL service. There are three (3) main chat areas on AOL which

---

<sup>1</sup> A "Chat Room" is a reference to an electronic address which because of its name draws users to its location (e.g. "Trekkie" might be an address where persons/fans interested in exchanging information about "Star Trek" would electronically congregate). When a person electronically enters such a "chat room", he/she may read all the messages being sent among other users who have gathered at that electronic address and participate in those electronic conversations simultaneously and instantaneously.

allow the user/member of the service to communicate with other members of the service simultaneously. The three (3) chat rooms are called

- 1) Public Rooms
- 2) Member Rooms
- 3) Private Rooms

Each chat area (except "Private Rooms") has a list of room names depicting the general content of the conversation occurring within that particular room. Each room can accommodate up to twenty-three (23) users/members at one time. To access a particular room in either the Public Room or Member Room areas, a user/member can scroll through a listing of room names and pick a room of interest. The Private Room chat area does not have a room listing option and can only be accessed by a user/member if the user/member knows the name of the room he/she wishes to enter. To that end Private rooms are most commonly used by a small group of members who wish to talk to each other privately and are usually prearranged by one or more members who wish to converse in a particular Private room. Thus the only way to access such a Private chat room is to have learned of its existence and its exact title from another user/member and then type that title in an option field in order to enter that room.

17. During the undercover operation, investigators who were physically located in Erie County, New York, were logged onto AOL and access would be made to a Private chat room named "PRETEEN." Our investigation indicates that the Private room designated "PRETEEN" is a room created by an organization or group of pedophiles for the purpose of trading child pornographic material among other pedophiles. I have been advised by SA

MacMartin, Investigator Harrington, and others that pedophiles often are members of an organization known as North America Man-Boy Love Association ("NAMBLA"). This organization is used by its members to buy, sell, and trade materials depicting children less than 16 years of age engaged in sexual conduct and to meet other individuals of similar social views and interests.

18. While in this Private room named "PRETEEN", investigators have conversed electronically with numerous suspects about trading child pornography. While conducting this undercover investigation in "PRETEEN", SA MacMartin and your affiant have received thousands of images, the vast majority of which, based on the training, experience and expertise of both SA MacMartin and your affiant, depict the sexual performance/sexual conduct by a child less than 16 years of age as defined in the New York State Penal Law.

19. Through this investigation, your affiant has come to learn that members/participants of the Private room "PRETEEN" usually ask other members/participants if they would like to be placed on a list in order to receive child pornography by e-mail. On many occasions, the originator of the list will ask that members/participants type a numeric number, such as "1" or type a short statement, such a "I will send 1 to get 1" so that the originator can record the names of the members that will be placed on the list and ultimately receive such child pornography.

20. On January 13, 1997, Investigators from the NYSAG-OCTF, while located at a computer terminal in Erie County, New York, were conducting visual surveillance of the conversations and activities occurring on-line while in the Private chat room called "PRETEEN", and NateTSnake expressed an interest in trading preteen materials with the

investigator who was "present" in the room. Specifically, at approximately 10:30 am on 01/13/97, the undercover personnel received an electronic e-mail message in the form of an Instant Message<sup>2</sup> ("IM") from NateTSnake who stated in the IM: "hi 20/m/NY<sup>3</sup>, how are you?" The undercover personnel respond by stating: "30f trading?" NateTSnake stated "yes, you?" The undercover investigators then stated: "sure, where in NY?" NateTSnake stated: "Manhattan, where are you from?, I go to school in Albany." The undercover investigators then stated: "Out west, near Buffalo." A short time later, the undercover investigators stated to NateTSnake: "I have many videos, what are you interests?" NateTSnake stated: "Almost anything." The undercover investigators then stated: " I can get my hands on just about all kinds of yng action vids." NateTSnake stated: "I like young girls, do you mean avi's<sup>4</sup> or videos?" The undercover investigators stated: "Videos,, many in my possession. Some are homemade, others are in my collection//." NateTSnake then responded by stating: "cool... I would Love to see an entire video." The undercover investigators then

---

<sup>2</sup> An Instant Message is a software option provided by America On Line which allows two members to communicate simultaneously and instantaneously in a private one-on-one setting.

<sup>3</sup> This phrase, 20/m/NY, is commonly used on the internet to tell another user/member of the AOL service the age/sex/location of the other member.

<sup>4</sup> AVI is a computer graphic file format extension which stands for Audio Visual Interleave. A computer graphic file formatted with an AVI extension while opened and viewed with the appropriate computer graphic software program will display a short motion picture quality movie on your computer monitor. (See paragraph 12 Supra.)



negotiate a "Trade" deal with NateTSnake whereby NateTSnake agreed to send ten (10) child pornographic electronic pictures in exchange for one (1) child pornographic VHS video tape.

During the course of their discussion, the undercover investigators asked NateTSnake what age of girls he is interested in. NateTSnake stated: "girls 13 and down, peeing, like that."

NateTSnake then give the undercover personnel a school address of:

Colonial Quad Box #1144,  
SUNY Albany, 1400 Washington Ave  
Albany, NY 12222.

(A copy of the IM transcript is attached as Exhibit A).

21. At approximately 10:54 am on 1/13/97, the undercover investigators began receiving e-mail messages, with computer graphic files attached, from NateTSnake. The e-mail message read " Subj: 1", and it had with it attachment file 09PEE.JPG. (A copy of the graphic file image is attached as Exhibit B).

22. On that same day between the hours of 10:56 am and 1:55 pm, the undercover received approximately twenty-seven (27) additional e-mail messages from NateTSnake containing the attached JPG/GIF files: !POPSUK.JPG, !!!!!13F.JPG, !10CUMFC.JPG, DADSUC.JPG, YG20.JPG, WHOLEFAM.JPG, !!10ETPS.JPG, !!06CUMM.JPG, \_\_\_DAD.JPG, OH1-11.JPG, DADDO019.JPG, GIRL&DAD.JPG, !8CUMFAC.JPG, !9FUCKME.JPG, 12INDIA2.JPG, YUNGGS.JPG, \_\_12\_MOM.JPG, 8FINGERD.JPG, 7DRINK\_1.JPG, 11DOSELF.JPG, !!!!!5.JPG, 04CUMFC.JPG, 05SUCKY.JPG, 06ONTOP.JPG, COOL4.JPG, and !!!!!08YRS.JPG. (A copy of the e-mail message with attached files are attached as Exhibit C.)

23. On 1/14/97 (the following day), at approximately 9:43 am, the undercover investigators AOL account began receiving additional e-mail messages, with computer graphic files attached, from NateTSnake.

24. Thereafter, on the same date (1/14/97), between approximately 9:45 and 10:55 am, the undercover AOL account received twenty-three (23) more e-mail messages with the following computer graphic files attached: !!!!!!!@.jpg, BRO-SIS.JPG, BRIELLE.GIF, \_\_3\_KIDS.JPG, !7-TASTY.JPG, !!10BLUE.JPG, \_7FKDAD.JPG, ZUJUNG\_4.JPG, DADDO019.JPG, DADDO029.JPG, \_13LICKR.JPG, \_1DADSGR.JPG, \_HPPYGRL.JPG, BETH&DAD.JPG, \_\_1st\_BJ.JPG, #1FAWN.JPG, \_\_\_\_\_10T.JPG, \_\_SUCDAD.JPG, BEWEIS.JPG, 10FUKDAD.JPG, !!!!6SUK.JPG, \_\_04DIL.JPG, 23SUCKY.JPG. (Copies of the graphic image files are attached as Exhibit D.)

25. On 1/14/97, at approximately 12:00 pm, the undercover investigators were logged on to AOL reviewing the e-mail transmissions sent by NateTSnake, and others, when NateTSnake engaged the undercover investigators in electronic Instant Message conversation ("IM"). During this IM conversation, NateTSnake stated to the undercover investigators: "...spent all night thinking about the videos." The undercover investigators replied: "i'll be sending them out Saturday for u." A short time later in the conversation, NateTSnake stated that he: "won't be able to send more pics when I get to school." NateTSnake stated that he has a laptop that is too slow and the modem freezes. NateTSnake further stated that the computer he is using: "is my dad's computer, the laptop is mine." The undercover investigators then asked: "does your dad like this stuff 2?" NateTSnake replies: "not little

kids, he likes smut though, I'm the only pedophile in the family :)<sup>5</sup>." 26. Your affiant states that based upon my experience in the undercover operation, as well as the training and experience of SA MacMartin and Investigator Harrington, the majority of the graphic images referred to in paragraphs 21-24 depict children under the age of sixteen engages in sexual conduct as defined by the New York Penal Law.

27. Through an analysis of the intelligence gathered throughout this investigation, your affiant states that during the evening of 12/19/96 and on 12/20/96, the undercover personnel, and NateTSnake received from various members of AOL, thirty-five (35) e-mail messages with computer graphic files attached. Specifically, on that date, between approximately 11:51 pm and on 12/20/96 at 10:19 pm, the following JPG files were received by NateTSnake: ISOH-~17.JPG, !ASIASUC.JPG, JOSALY~1.JPG,!ARKANSA.JPG, !!12BNNA.JPG,!16INCAR.JPG, 13NUDE.JPG, CUMNGET!.JPG, OREOSLU.JPG, MOMDAU.JPG, !!!!!10B.JPG, !\_TEEN97.JPG, !!!!!15.JPG, DSBG010.JPG, !12NEICE.JPG, BEAVER~1.JPG, !!!!!PET.JPG, !13TRY~1.JPG, ANDBEADS.JPG, !15SE.JPG, 18TEEN.JPG, !ASIASUC.JPG, #SISSUCK.JPG, !!!!!HAT.JPG, !!BJCNDY.JPG, !DEBSUKS.JPG, CHEERS.JPG, BUSH001.GIF, 8ROSEANN.JPG, !!BJCNDY.JPG, !!!!!PET.JPG, \_\_\_\_\_12Y.JPG.

---

<sup>5</sup> The symbols referred to above are commonly used by user/members on the internet to express various sideways faces or moods. For example, the symbol " :)" represents a smile face, " ;) " represents a wink, and " :( " represent a sad face.

28. Your affiant states that based upon my experience in the undercover operation, as well as the training and experience of SA MacMartin and Investigator Harrington, the majority of the graphic images referred to in paragraph 27 above depict children under the age of sixteen engaged in sexual conduct as defined by the New York Penal Law. These graphic images were received by NateTSnake and it is more likely than not that he has retained these graphic images.

29. America Online provides its users with the opportunity to list profile information on themselves. The information which the user chooses to provide, is then available for viewing by other users of America Online. NateTSnake provided as part of his profile that his name is Nathaniel "Nate to you" that he has a "Gateway something or other" computer, is a college "Stoodent" and lives in "New York, NY USA."

30. Based upon information obtained by Subpoena your affiant has determined from America Online that the subscriber for the screen name NateTSnake is Richard Levy, 573 Grand Street, Apartment D 1204, New York, New York 10002. America Online also listed day and evening telephone numbers as 212-228-6529, for the account of Richard Levy.

31. America On Line also provided your affiant with log on times for NateTSnake. The information provided by AOL reveals, upon information and belief, that NateTSnake was signed on to AOL on 1/13/97 from approximately 8:36 am until approximately 2:36 pm and on 1/14/97 from approximately 9:38 am until approximately 3:29 pm. Your affiant states that these log on times correspond with the times the undercover investigators were on line conducting the undercover investigation and received graphic computer images from NateTSnake.

32. Your affiant caused the SUNY/Albany records to be searched for information relating to Colonial Quad Box #1144. Information provided to your affiant indicates that such box is subscribed to by Nathaniel Levy, 573 Grand Street, Apartment D 1204, New York, NY 10002. Nathaniel Levy is also assigned to a SUNY dorm room located at Livingston Tower, 1302, Bedroom #3, Colonial Quad, SUNY Albany.

33. NYSPIN queries indicate that a New York State drivers license has been issued to Nathaniel A. Levy, DOB 01/18/76, 573 Grand Street, D1204, New York, NY 10002.

34. A check with U.S. Postal Service Inspectors indicates that Nathaniel A. Levy receives mail at 573 Grand Street, Apartment D 1204, New York, NY 10002.

35. Your affiant caused the Phone Disk telephone directory to be searched for telephone number 212- 228-6529. The information reveals that telephone number 212-228-6529 is subscribed to by R. Levy, 573 Grand Street, New York, NY 10002.

36. Your affiant states that based upon the facts set forth above that it is more likely that not that the computer utilized and the graphic image files referred to above, by NateTSnake, and/or Nathaniel A. Levy, to promote the sexual performance by a child less than 16 years of age are located at 573 Grand Street, Apartment D 1204, New York, New York. Even if NateTSnake has "deleted" the graphic images files, placed them on portable disks and transported them back to his school address, it is more likely than not, based upon my experience, and the training of our forensic computer experts, that the graphic images files will remain on the computers internal storage device (internal hard drive) for a period of time.

37. Investigators assigned to this matter have observed this location and described it as a multi-story apartment complex divided into three sections designated "D", "E", and "F".

Apartment 1204 is located on the 12th floor; the door is painted dark pink and is marked "D1204." The name on the mailbox and bell, in the lobby area, is "R.P.LEVY."

**CPL §690.35(4)(b) "NO KNOCK" REQUEST**

38. Based upon information developed during this investigation, it is possible that other individuals may have access to the computer which contains copies of the graphic image files maintained by the individual responsible for their transmission, receipt and storage.

39. Based upon my experience and training, as well as the experience and training of SA MacMartin and other investigators trained in the search, seizure, storage and retrieval of computer data, your affiant states that the "evidence" or property sought may be easily and quickly destroyed or disposed of by an individual utilizing a short series of key strokes or computer commands. In addition, an individual may be able to activate "booby-traps" or other forms of computer security programs which could render the data sought inaccessible or unusable, as well as reverse the process to restore it.

**CONDUCT OF INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY**

40. Pursuant to my training and experience, as well as the training and experience of other law enforcement personnel, I have learned that:

a) Child pornography is not readily available in retail establishments; accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contact with other individuals who have it available.

b) The use of computers to traffic in, trade, collect child pornography and obscenity has become one of the preferred methods of obtaining obscene and child pornographic materials. An individual familiar with a computer can use it, usually in the privacy of his own home or office, to interact with another individual or a business offering such materials in this country or elsewhere in the world. The use of a computer provides

individuals interested in obscenity or child pornography with a sense of privacy and secrecy not attainable by other media. It also permits the individuals to contact and interact with many more individuals than through the use of the mails.

c) Persons involved in sending or receiving child pornography tend to retain it for long periods of time. The images obtained, traded and/or sold are prized by those individuals interested in child pornography. In addition to their "emotional" value, the images are intrinsically valuable as trading/selling material and therefore are rarely destroyed or deleted by the individual collector. Graphic image files can be maintained on the computers built-in hard drive or on storage disks. This tendency is enhanced by the increased sense of security that a computer affords.

### CONCLUSION

41. Based upon your affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting.

42. Based upon the foregoing, there is probable cause to believe that the files, documents, and attachments identified in ¶¶ 22-27, and business records and related documents pertaining to the acquisition, purchase and distribution of graphic computer images depicting the sexual performance/sexual conduct of children less than 16 years of age in violation of Article 263 of the New York Penal Law are located on the premises at 573 Grand Street, Apartment D 1204, New York, NY 10002.

43. There is further probable cause to believe that these records are maintained in files, computer storage facilities or other data storage facilities, and that, within these files,

there are records--namely, correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles, documents, photographs, negatives, photographic slides or other visual depictions or equipment--used to depict child pornography materials.

44. Additionally, your affiant believes that evidence of violations of N.Y. Penal Law, Section 263.15 are contained or concealed in the tapes, cassettes, cartridges, streaming tape, commercial software and manuals, hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk applications programs, data disks, system disk operating systems, magnetic media-floppy disks, tape systems and hard drive and other computer related operating equipment, which depict or are used to depict child pornographic materials contrary to the laws of New York State.

45. Based on all the foregoing, there is probable cause to believe that child pornography, and other evidence of the use of computers to promote the sexual performance/sexual conduct by a child less than 16 years of age set forth in the attached search warrant, will be found on the premises located 573 Grand Street, Apartment D 1204, New York, NY, and under the control of the suspect identified in the attached sealed affidavit, and/or other individuals unknown, and that those items of child pornography constitute evidence of the sexual performance/sexual conduct by children under the age of sixteen (16) years of age contrary to the laws of New York State.

WHEREFORE, your affiant respectfully requests that a warrant be issued authorizing the New York State Attorney General's Organized Crime Task Force and the New York State Police, with the appropriate assistance from other law enforcement officers, to



enter the premises at 573 Grand Street, Apartment D 1204, New York, NY, and therein search and seize the following items:

1. Visual depictions !POPSUK.JPG, !!!!!13F.JPG, !10CUMFC.JPG, DADSUC.JPG, YG20.JPG, WHOLEFAM.JPG, !!10ETPS.JPG, !!06CUMM.JPG, \_\_\_\_\_DAD.JPG, OH1-11.JPG, DADDO019.JPG, GIRL&DAD.JPG, !8CUMFAC.JPG, !9FUCKME.JPG, 12INDIA2.JPG, YUNGGS.JPG, \_\_12\_MOM.JPG, 8FINGERD.JPG, 7DRINK\_1.JPG, 11DOSELF.JPG, !!!!!5.JPG, 04CUMFC.JPG, 05SUCKY.JPG, 06ONTOP.JPG, COOL4.JPG, !!!08YRS.JPG, 09PEE.JPG., !!!!!!!@.jpg, BRO-SIS.JPG, BRIELLE.GIF, \_\_3\_KIDS.JPG, !7-TASTY.JPG, !!10BLUE.JPG, \_7FKDAD.JPG, ZUJUNG\_4.JPG, DADDO019.JPG, DADDO029.JPG, \_13LICKR.JPG, \_1DADSGR.JPG, \_HPPYGRL.JPG, BETH&DAD.JPG, \_\_1st\_BJ.JPG, #1FAWN.JPG, \_\_\_\_\_10T.JPG, \_\_SUCDAD.JPG, BEWEIS.JPG, 10FUKDAD.JPG, !!!!!6SUK.JPG, \_\_04DIL.JPG, 23SUCKY.JPG, ISOH-~17.JPG, !ASIASUC.JPG, JOSALY~1.JPG,!ARKANSA.JPG, !!12BNNA.JPG, !16INCAR.JPG, 13NUDE.JPG, CUMNGET!.JPG, OREOSLU.JPG, MOMDAU.JPG, !!!!!10B.JPG, !\_TEEN97.JPG, !!!!!15.JPG, DSBG010.JPG, !12NEICE.JPG, BEAVER~1.JPG, !!!!!PET.JPG, !13TRY~1.JPG, ANDBEADS.JPG, !!15SE.JPG, 18TEEN.JPG, !ASIASUC.JPG, #SISSUCK.JPG, !!!!!HAT.JPG, !!BJCNDY.JPG, !DEBSUKS.JPG, CHEERS.JPG, BUSH001.GIF, 8ROSEANN.JPG, !!BJCNDY.JPG, !!!!!PET.JPG, \_\_\_\_\_12Y.JPG or other computer graphic files which depict children in a sexually explicit manner contrary to law.

2. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer

impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices such as computer disks, magnetic media-floppy disks, tape systems, hard drives, disk drives, tape drives, transistor-like binary devices, and other memory storage devices; and any external attachments peripheral input/output devices such as keyboards, printers, scanners, plotters, video display monitors, and optical readers; and related communications devices such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

3. Computer software, that is, digital information which can be interpreted by a computer and any of its related components, which may be stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs; computer related documentation, that is, written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

4. Business records, correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles, documents which reflect the receipt, purchase, transmission and/or distribution of materials depicting children in a sexually explicit manner.

5. Any, photographs, negatives, photographic slides or other visual depictions or equipment, used to depict child in a sexually explicit manner.

**SEALING OF THIS AFFIDAVIT**

46. It is respectfully requested that because this investigation is on-going and may be compromised by disclosure of this application that the Court issue an order pursuant to which this Application by Affidavit be filed and maintained under seal until further order of this Court.

\_\_\_\_\_  
MICHAEL G. McCARTNEY,  
Investigator  
N.Y. State Attorney General's  
Organized Crime Task Force

Sworn to and subscribed before  
me this \_\_\_\_\_ day of January, 1997.

\_\_\_\_\_  
JOSEPH S. FORMA, Justice  
Supreme Court, Erie County

STATE OF NEW YORK  
COUNTY COURT : COUNTY OF ERIE

---

In the Matter of the Application of  
Michael G. McCartney, for a Search  
Warrant Authorizing the Search of  
1 Hunington Quadrangle, Suite 2S12,  
Caraccia & Co, CPA, in the City  
of Melville, County of Suffolk, State of New York..

---

SEARCH WARRANT

**IN THE NAME OF THE PEOPLE OF THE STATE OF NEW YORK TO  
ANY POLICE OFFICER EMPLOYED BY THE STATE OF NEW YORK,  
ANY POLICE OFFICER OF THE JURISDICTION WHERE THE WARRANT  
IS TO BE EXECUTED AND ANY POLICE OFFICER ACTING UNDER  
THEIR DIRECTION.**

Proof by Affidavit having been made this day before me by Michael G. McCartney, an Investigator with the New York State Attorney General's Office, ("NYSAG"), that there is reasonable cause to believe that there is in the premises located at 1 Hunington Quadrangle, Suite 2S12, a Business known as Caraccia and CO, CPA's, located in the West corridor of building number 1, Hunington Quadrangle, Suite 2S12, County of Suffolk, State of New York, computer hardware, computer software, and computer related documentation, which constitutes evidence that the crime of Promoting the Sexual Performance by a Child, in violation of Article 263 of the Penal Law and Conspiracy to commit that crime has been committed.

YOU ARE THEREFORE COMMANDED, within ten (10) days of the date of the issuance of this warrant, in the daytime, to make an immediate search of the premises located at 1 Hunington Quadrangle, Suite 2S12, Caraccia and CO, CPA's, a Business, City of Melville, County of Suffolk, State of New York, above, to examine and/or seize the following property:

1. Computer graphic files: blosex55.jpg; blosex56.jpg; blosex58.jpg; joy02.jpg; joy03.jpg; joy03a.jpg; joy03b.jpg; ll-e1-15.jpg; ll-e1-29.jpg; ll-e1-af.jpg; ll-n1-08.jpg; ll-n1-11.jpg; ll-n3f22.jpg; ll-n3f23.jpg; ll-n3f25.jpg; ll-n4-40.jpg; ll-n3f24b.jpg; mt1a001.jpg; mt1a005.jpg; and mt1a025.jpg and/ or other computer graphic files which depict what appear to be children in a sexually explicit manner contrary to law.

2. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices such as computer disks, magnetic media-floppy disks, tape systems, hard drives, disk drives, tape drives, transistor-like binary devices, and other memory storage devices; and any external attachments peripheral input/output devices such as keyboards, printers, scanners, plotters, video display monitors, and optical readers; and related communications devices such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

3. Computer software, that is, digital information which can be interpreted by a computer and any of its related components, which may be stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as

word-processing, graphics , or spreadsheet programs), utilities, compilers, interpreters, and communications programs; computer related documentation, that is, written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

4. Any, photographs, negatives, photographic slides or other visual depictions or equipment, used to depict child in a sexually explicit manner.

YOU ARE FURTHER COMMANDED and authorized to enter said premises without giving notice of your authority and purpose pursuant to Section 690.35 of the CPL.

YOU ARE FURTHER COMMANDED to enter said premises and, if you find the same or any part thereof of the described property, and if you seize any of the described property, to bring it forthwith before me at this issuing court, and it is,

FURTHER ORDERED, that the Application and Affidavit for the search warrant shall remain sealed until further order of this Court.

Dated this \_\_\_ day of January, 1998, at \_\_\_\_\_ o'clock, City of Buffalo, County of Erie, New York.

---

HON.  
COUNTY COURT JUDGE

STATE OF NEW YORK  
SUPREME COURT : COUNTY OF ERIE

---

In the Matter of the Application of  
Michael G. McCartney, for a Search  
Warrant Authorizing the Search of an  
apartment residence, located at  
573 Grand Street, Apartment D 1204  
in the City of New York, County of  
New York, State of New York.

---

**SEARCH WARRANT**

**IN THE NAME OF THE PEOPLE OF THE STATE OF  
NEW YORK TO ANY SPECIAL INVESTIGATOR IN THE  
NEW YORK STATE ORGANIZED CRIME TASK FORCE,  
ANY POLICE OFFICER IN THE NEW YORK STATE  
POLICE AND ANY POLICE OFFICER ACTING UNDER  
THEIR DIRECTION.**

Proof by Affidavit having been made this day before me by Michael G. McCartney, an Investigator with the New York State Attorney General's Office, currently assigned to the Organized Crime Task Force, that there is reasonable cause to believe that there is in the apartment residence located at 573 Grand Street, Apartment D 1204, City of New York, County of New York, State of New York, computer hardware, computer software, and computer related documentation, which constitutes evidence that the crime of Promoting the Sexual Performance by a Child, in violation of Article 263 of the Penal Law and Conspiracy to commit that crime has been committed.

**YOU ARE THEREFORE COMMANDED**, within ten (10) days of the date of the issuance of this warrant, in the daytime, to make an immediate search of the apartment residence located at 573 Grand Street, Apartment D 1204, City of New York, County of New York,

State of New York, above, to examine and/or seize the following property:

1. Visual depictions !POPSUK.JPG, !!!!!13F.JPG, !10CUMFC.JPG, DADSUC.JPG, YG20.JPG, WHOLEFAM.JPG, !!10ETPS.JPG, !!06CUMM.JPG, \_\_\_\_\_DAD.JPG, OH1-11.JPG, DADDO019.JPG, GIRL&DAD.JPG, !8CUMFAC.JPG, !9FUCKME.JPG, 12INDIA2.JPG, YUNGGS.JPG, \_\_12\_MOM.JPG, 8FINGERD.JPG, 7DRINK\_1.JPG, 11DOSELF.JPG, !!!!!5.JPG, 04CUMFC.JPG, 05SUCKY.JPG, 06ONTOP.JPG, COOL4.JPG, !!!!!08YRS.JPG, 09PEE.JPG., !!!!!!!@.jpg, BRO-SIS.JPG, BRIELLE.GIF, \_\_3\_KIDS.JPG, !7-TASTY.JPG, !!10BLUE.JPG, \_7FKDAD.JPG, ZUJUNG\_4.JPG, DADDO019.JPG, DADDO029.JPG, \_13LICKR.JPG, \_1DADSGR.JPG, \_HPPYGRL.JPG, BETH&DAD.JPG, \_\_1st\_BJ.JPG, #1FAWN.JPG, \_\_\_\_\_10T.JPG, \_\_SUCDAD.JPG, BEWEIS.JPG, 10FUKDAD.JPG, !!!!!6SUK.JPG, \_\_04DIL.JPG, 23SUCKY.JPG, ISOH-~17.JPG, !ASIASUC.JPG, JOSALY~1.JPG,!ARKANSA.JPG, !!12BNNA.JPG, !16INCAR.JPG, 13NUDE.JPG, CUMNGET!.JPG, OREOSLU.JPG, MOMDAU.JPG, !!!!!10B.JPG, !\_TEEN97.JPG, !!!!!15.JPG, DSBG010.JPG, !12NEICE.JPG, BEAVER~1.JPG, !!!!!PET.JPG, !13TRY~1.JPG, ANDBEADS.JPG, !!15SE.JPG, 18TEEN.JPG, !ASIASUC.JPG, #SISSUCK.JPG, !!!!!HAT.JPG, !!BJCNDY.JPG, !DEBSUKS.JPG, CHEERS.JPG, BUSH001.GIF, 8ROSEANN.JPG, !!BJCNDY.JPG, !!!!!PET.JPG, \_\_\_\_\_12Y.JPG and any other GIF, JPG, AVI, MPG or other computer graphic files which depict children in a sexually explicit manner contrary to law.

2. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook"



computers); internal and peripheral storage devices such as computer disks, magnetic media-floppy disks, tape systems, hard drives, disk drives, tape drives, transistor-like binary devices, and other memory storage devices; and any external attachments peripheral input/output devices such as keyboards, printers, scanners, plotters, video display monitors, and optical readers; and related communications devices such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

3. Computer software, that is, digital information which can be interpreted by a computer and any of its related components, which may be stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics , or spreadsheet programs), utilities, compilers, interpreters, and communications programs; computer related documentation, that is, written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

4. Business records, correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles, documents which reflect the receipt, purchase, transmission and/or distribution of materials depicting children in a sexually explicit manner.

5. Any, photographs, negatives, photographic slides or other visual depictions or equipment, used to depict child in a sexually explicit manner.

STATE OF NEW YORK  
\*\*\*\*\* COURT : COUNTY OF NEW YORK

---

In the Matter of the Application  
for a Search Warrant Authorizing the  
Search of residence located at 253 Ramona  
Avenue, in the City of Staten Island,  
County of Richmond, State of New York.

---

**SEARCH WARRANT**

**IN THE NAME OF THE PEOPLE OF THE STATE OF  
NEW YORK TO ANY SPECIAL INVESTIGATOR IN THE  
NEW YORK STATE ATTORNEY GENERAL'S OFFICE,  
ANY POLICE OFFICER IN THE NEW YORK STATE  
POLICE AND ANY POLICE OFFICER ACTING UNDER  
THEIR DIRECTION.**

Proof by Affidavit having been made this day before me by Michael G. McCartney, an Investigator with the New York State Attorney General's Office, that there is reasonable cause to believe that there is in the premises located at 253 Ramona Avenue, a one story, one family ranch front front with an attached screen room area in Staten Island, New York, computer hardware, computer software, and computer related documentation, which constitutes evidence that the crime of Promoting the Sexual Performance by a Child, in violation of Article 263 of the Penal Law and Conspiracy to commit that crime has been committed.

**YOU ARE THEREFORE COMMANDED**, within ten (10) days of the date of the issuance of this warrant, in the daytime, to make an immediate search of the premises located at 253 Ramona Avenue, a One story one family ranch brick front residence in Staten Island, New York, above, to examine and/or seize the following property:

1. Computer graphic files: !!!11TAMM.JPG and 09PEE.JPG or other computer

graphic files which depict what appear to be children in a sexually explicit manner contrary to law.

2. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices such as computer disks, magnetic media-floppy disks, tape systems, hard drives, disk drives, tape drives, transistor-like binary devices, and other memory storage devices; and any external attachments peripheral input/output devices such as keyboards, printers, scanners, plotters, video display monitors, and optical readers; and related communications devices such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

3. Computer software, that is, digital information which can be interpreted by a computer and any of its related components, which may be stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs; computer related documentation, that is, written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

4. Any, photographs, negatives, photographic slides or other visual depictions or equipment, used to depict child in a sexually explicit manner.

YOU ARE FURTHER COMMANDED and authorized to enter said premises without giving notice of your authority and purpose pursuant to Section 690.35 of the CPL.

YOU ARE FURTHER COMMANDED to enter said premises and, if you find the same or any part thereof of the described property, and if you seize any of the described property, to bring it forthwith before me at this issuing court, and it is,

FURTHER ORDERED, that the Application and Affidavit for the search warrant shall remain sealed until further order of this Court.

Dated this \_\_\_ day of January, 1998, at \_\_\_\_\_ o'clock, City of New York, County of New York, New York.

---

HON.  
SUPREME COURT JUDGE

YOU ARE FURTHER COMMANDED and authorized to enter said premises without giving notice of your authority and purpose.

YOU ARE FURTHER COMMANDED to enter said premises and, if you find the same or any part thereof of the described property, and if you seize any of the described property, to bring it forthwith before me at this issuing court, and it is

FURTHER ORDERED that the Application by Affidavit for the search warrant shall remained sealed until further order of this Court.

Dated this \_\_\_ day of January, 1997, at \_\_\_\_\_ o'clock, County of Erie, New York.

---

JOSEPH S. FORMA, Justice  
Supreme Court, Erie County



## **Legal Issues**





- 1  **PROTECTING CHILDREN ONLINE**  
DANIEL ARMAGH  
APRI'S NATIONAL CENTER FOR PROSECUTION OF CHILD ABUSE
- 2  **PRIVACY ISSUES**
  - FEDERAL CONSTITUTIONAL PROTECTIONS
  - STATE CONSTITUTIONAL PROTECTIONS
  - STATUTORY PROTECTIONS
  - PRIVILEGES / CONFIDENTIAL COMMUNICATIONS - COURT DECISIONS
- 3  **FEDERAL PRIVACY STATUTES**
  - PRIVACY PROTECTION ACT
  - STORED WIRE AND ELECTRONIC COMMUNICATION AND TRANSACTIONAL RECORDS ACCESS ACT (ECPA)
  - VIDEO PRIVACY PROTECTION ACT
  - PROTECTING CHILDREN AND SEXUAL PREDATOR PUNISHMENT ACT OF 1998 (pending legislation)
- 4  **PRIVACY PROTECTION ACT**  
42 U.S.C. 2000aa  
*Provides protection against searches beyond what the fourth amendment affords for activities related to publishing. This law applies not only to traditional publishers, but also to anyone who may reasonably claim to be a publisher, including publishers of obscene material.*
- 5  **PPA**  
*YOU MUST BE EXTREMELY CAREFUL BEFORE USING A SEARCH WARRANT TO OBTAIN EVIDENCE FROM PERSONS WHO ARE ABLE TO CLAIM THAT THEY PUBLISH INFORMATION TO THE PUBLIC (e.g., bulletin board sysops).*
- 6  **PPA**
  - **ZURCHER v. STANFORD DAILY PRESS**, 436 U.S. 547 (1978).
  - PPA applies only to law enforcement
  - PPA provides for damages even where officers acted in good faith (no less than \$1000, plus attorneys fees and costs)
- 7  **PPA**
  - Regulates searches or seizures of work product materials or documentary materials which are intended to be published to the public.
  - Law enforcement may not search or seize wpm or dm (almost everything) from any person who intends to publish information to the public.

- 8  **PPA**
- Under PPA almost anyone is allowed to claim they are a publisher
  - Law enforcement must serve the target with a warrant or subpoena which the target may seek to have quashed by a court
  - Practical effect is to prohibit law enforcement from obtaining records from anyone that claims publisher status
- 9  **WORK PRODUCT MATERIALS**
- MENTAL IMPRESSIONS, THEORIES, OR CONCLUSIONS
- 10  **DOCUMENTARY MATERIALS**
- THE LANGUAGE OF THE PPA IS SUFFICIENTLY BROAD THAT VIRTUALLY ANY EVIDENCE WOULD BE INCLUDED IF PUBLISHER STATUS IS PROVEN
- 11  **ESMAY v. UNITED STATES, 1993 U.S. Dist. Lexis 20362**
- " Thus, for a valid claim to be stated under the PPA;  
(1) there must have been a search and seizure; and (2) there must be a showing of intent to publicly disseminate the information
- 12  **EXCEPTIONS TO PPA**
- CONGRESS EXCLUDED FROM DEFINITIONS OF WPM OR DM "ANY CONTRABAND O
- 13  **EXCEPTIONS WITHIN THE PPA**
- YOU MAY USE A **SEARCH WARRANT** WHERE;
  - Materials relate to a criminal offense( other than mere possession themselves);
  - immediate seizure of materials is necessary to save lives;
- 14  **EXCEPTIONS WITHIN THE PPA**
- **IN THE CASE OF DOCUMENTARY MATERIALS ONLY**,service of a subpoena would result in destruction, alteration, or concealment of evidence, **or**;
  - a court order was not complied with, and either appellate remedies are exhausted or delay would threaten the ends of justice.
- 15  **ANALYSIS UNDER PPA**
- REASONABLE THAT TARGET INTENDS TO PUBLISH?
  - IF **AFTER** YOU SEIZE MATERIALS YOU DISCOVER INTENT TO PUBLISH?
- 16  **ANALYSIS UNDER PPA**
- MIXED MATERIALS: CONSIDER SEIZURE BUT NOT EXAMINING UNTIL TARGET CONTESTS IN COURT
- 17  **ANALYSIS UNDER PPA**
- THE MATERIALS ARE ALMOST ALWAYS EITHER WPM OR DM IF YOU HAVE REASON TO BELIEVE THAT TARGET IS KEEPING MATERIALS

THAT RELATE TO HIS PUBLISHING ACTIVITY ON THE COMPUTER  
YOU INTEND TO SEIZE OR SEARCH

18  **EXCEPTIONS**

■ IF MATERIALS FALL INTO THE FOLLOWING CATEGORIES, YOU MAY  
USE A SEARCH WARRANT TO SEIZE THE MATERIALS:

1. *contraband, stolen property, property used to commit a crime*
2. *probable cause to believe target has committed, is committing a criminal offense to which the materials relate, **other than possession***

19  **EXCEPTIONS**

3. *Reasonable that immediate seizure of materials prevents sbi or death*

■ *If you are seizing **dm** which do not fall into the above cited exceptions, your may use a search warrant if your affidavit establishes that serving a subpoena would result in destruction, alteration, or concealment of **dm**.*

20  **PARADIGM SUMMARY- wpm**

21  **PARADIGM SUMMARY- dm**

22  **ANALYSIS SUMMARY**

■ *PPA prohibits search or seizure of protected materials; this means that law enforcement can not use a search warrant to obtain the materials. Law enforcement must use a subpoena for such materials on the person who possesses the materials, allowing for the target to challenge the subpoena before complying with it.*

23  **REASONABLE BELIEF STANDARD**

*FOR THE PPA TO APPLY TO EITHER WPM OR DM, THE PERSON POSSESSING SUCH MATERIALS MUST BE A PERSON **REASONABLY BELIEVED** TO HAVE A PURPOSE TO DISSEMINATE SUCH INFORMATION TO THE PUBLIC*

24  **SPECIAL PROBLEMS - PPA**

- *Poorly drafted language*
- *commingled materials - some of the material is protected and some is not: how do you proceed?*
- *what if you are unaware there is also protected material on computer until seized?*
- *Conflicts with the Omnibus Act*

25  **SPECIAL PROBLEMS - PPA**

- *COPY THE DISK OR THE CRIMINAL PORTION OF THE DISK?*
- *INSURING ACCURATE COPIES*
- *IS LAW ENFORCEMENT REQUIRED TO EXAMINE EVERY FILE ON SYSTEM BEFORE REMOVAL?*

- **LETTER TO THE EDITOR IN EVERY FILE OF THE TARGET'S COMPUTER**

26  **ANSWERS**

- *Courts are deciding these issues every month, with varying degrees of consistency*
- *So far, it appears if you don't know there is protected material at seizure, you may not be in violation unless, once you realize the material is protected, and it is requested, you are in violation if you fail to return materials*

27  **ANSWERS**

- *use a subpoena when possible*
- *get court approval on subpoena obtained records based on probable cause (may equal a warrant standard for purposes of the Omnibus Act)*
- **your job is to draft your affidavit to fit one of those exceptions to the search warrant prohibitions**

28  **PPA CASE HOLDINGS THROUGH APRIL, 1998**

- **CITICASTERS v. McCaskill**, 89 F.3d 1350 (1996) PPA does not require application for search warrant to describe exceptions to the PPA.
- **UNITED STATES v. MITTLEMAN**, 999 F.2d 440 (1993) PPA does not apply to criminal suspects and no greater showing of prob. cause for search warrant involving confidential relationships.

29  **CASES - PPA**

- **LAMBERT v. POLK COUNTY**, 723 F. Supp. 690 (1989) what constitutes "reasonably believed" to have a purpose to disseminate to the public a broadcast...
- **MINNEAPOLIS STAR & TRIBUNE CO. v. UNITED STATES**, 713 F.Supp.1308 (1989) attorney fees and costs under PPA

30  **CASES - PPA**

- **POWELL v. DEPUGH**, 911 F.Supp. 1184 (1995) statute of limitations for action under PPA is same as state's for tort or personal injury, not property or contract.
- **BENSON v. U.S.**, 1995 Lexis 31837, PPA did not apply because plaintiffs were suspects in criminal investigation and information seized not w/in PPA.

31  **CASES - PPA**

- **DEPUGH v. SUTTON**, 917 F. Supp. 690 (1996) plaintiff was within class of exceptions of criminal possessing materials relating to his criminal offense, namely poss. of child porn.
- **DAVIS v. GRACEY et.al.**, 111 F.3d 1472, (1997) sued police officers and

department for violations of PPA - lacked subject matter juris. Case has very pro-police analysis under ECPA.

32  *CASES - PPA*

- **STATE OF OKLAHOMA ex. rel. Robert Macy et.al. v. PIONEER CD-ROM...**, 891 P.2d 600 (1994) civil forfeiture of items seized under PPA- seizure upheld because the criminal verdict upheld- court gave no opinion on whether defendant had a viable civil suit under PPA.

33  *CASES - PPA*

- **STEVEN JACKSON GAMES v. U.S.**, 816 F. Supp. 432, affirmed 36 F.3d 457 (5th Cir. 1994) - court decided that immediate seizure did not violate PPA under reasonable belief standard, however once agent discovered materials were protected and failed to immediately return to plaintiff, PPA violated.

34  *CASES - PPA*

COMMINGLING PROTECTED AND NON-PROTECTED MATERIALS: in construing the fourth amendment protections, the court has held "that sometimes there is no viable alternative to seizing non-evidentiary items and sorting them out later." **Nat'l City Trading Corp. v. U.S.**, 635 F.2d 1020

35  *CASES - PPA*

- "If commingling prevents on site inspection, and no practical alternative exists, the entire property may be seizable, at least temporarily." **United States v. Tropp**, 725 F.Supp. 482 (1989). Obviously, these cases interpret the fourth amendment and not the PPA, but could be helpful as precedent on commingling issues.

36  *Electronic Communications Privacy Act (ECPA)*

- **Katz v. United States**, 389 U.S. 347 (1967) supreme court ruled that the fourth amendment does apply to wiretapping because people talking on the phone have an "expectation of privacy...Any attempt to capture that conversation is a search." Since **Katz**, a multitude of communication devices not in existence at the time fall under this rule.

37  *ECPA - HISTORY*

- In response to **Katz** Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which regulated interception of oral and wire communications. Congress eventually decided to regulate newer forms of communication- amending Title III in 1986 by enacting **ECPA**. Congress has amended some of **ECPA** last year.

38  *ECPA - a collection of statutes*

- Title 18 U.S.C. 2510 - 2521 deal with regulation of interception of electronic communications

- Sections 2701 - 2711 regulate *government access* to stored electronic communications
- Sections 3121 - 3127 regulate trap and trace devices and pen registers.

39  *ECPA - PPA*

- *The PPA protects a select group of communicators - media / publishers*
- *The ECPA protects communications based on their form - electric, wire, magnetic media...*
- *The ECPA applies not only to law enforcement as does the PPA; ECPA also applies to private parties*

40  *Cautions and Caveats*

- *These statutes do not replace the fourth amendment requirements, they supplement them*
- *State laws may have granted even greater protections than ECPA / PPA*
- *Laws are complex and many issues have not been resolved by the courts: Always consult a qualified attorney when faced with these statutes*

41  *ECPA - INTERCEPTION*

- *Protects electronic communication from interception while being transmitted.*
- *IN TRANSMISSION communication is speech, electrical impulses, radio waves...that constitute communication while moving from one party to another.*
- *Communication is not in transmission once it is 1. received 2. Stored*

42  *Communications in transmission*

- *fax transmissions in progress*
- *digital pager communications not received*
- *any data or commands traveling from one computer to another*
- Law enforcement rarely need to intercept communications in transmission*

43  *ECPA - INTERCEPTION*

- *exceptions: a party to a communication may "keystroke" monitor a communication in transmission and intercept same. 2511(2) (d)*
- *U.S. v. Seidlitz, 589 F.2d 152 (1978) owner of computer is party to comms.*
- *U.S. v. Merriweather, 917 F.2d 955 (1990) owner of pager or computer, or possessor of pager or computer is a party to communication.*

44  *ECPA - Interception*

- *Equipment furnished by the telephone company to any subscriber or user of such service may be used in the ordinary course of business to intercept communications. 2510 (4) (5)*
- *Providers of wire or electronic communication services may intercept*

where necessary to provide communication services or protect provider's rights or property. 2511 (2) (a)

45  *ECPA - Interception*

- *Provider of electronic communication services may provide to law enforcement any communication inadvertently obtained by provider which appears to be criminal activity. 2511 (3) (b) (iv)*
- *It is not an interception to examine a communications source or destination, as opposed to contents. 2510 (4)*

46  *ECPA- Interception - law enforcement*

- *ECPA mandates use of search warrant for law enforcement for interception*
- *ECPA distinguishes between federal and state court orders for interception*
- *state investigators are at a decidedly disadvantage in applying for intercept orders*

47  *State law enforcement - intercept*

- *If communications covered by the ECPA, help from feds is encouraged*
- *3 conditions for state investigators;*
  1. *authorized applicant under statute*
  2. *application meets state standards*
  3. *application demonstrates communication reveal enumerated crimes under state statute, >1yr.*

48  *Application for Court Order*

- *prob. cause specific offense will happen*
- *identity of suspect*
- *identity of sender of communication*
- *location of target equip. & facilities used*
- *period of time intercept. is maintained*
- *earlier applications? Course of invest.?*
- *less intrusive means inadequate?*

49  *Application for court order-intercept -2518 (1)*

- *must meet a higher standard than ordinary search warrant*
- *probable cause plus showing all less intrusive avenues have been used or considered and were not feasible - state reasons not possible.*
- *Be aware of stricter state requirements than that of ECPA*

50  *Congressional Notes - Judiciary Committee on Intercept Laws*

- *In monitoring wire transmissions, investigators must stop listening to innocent conversations. This concept is also desired in monitoring electronic communications as the committee "suggested" that all non-*

relevant material be deleted by initial law enforcement before being disseminated to others who would continue the investigation. Senate Rept. No. 99-541

51  *ECPA - Intercept- Suppression*

- Intercepting an **electronic communication** in violation of the ECPA can result in stiff penalties and possible criminal sanctions. It does not result in the suppression of the communication in a subsequent trial if no constitutional or state statutes were violated. (You loose your job, but the evidence is admissible!!)

52  *ECPA - Suppression- Intercept*

- Section 2515 omits electronic communication and only "wire or oral communication" remains as suppressible for violation of the ECPA.
- Section 2518 (10) © provides the exclusive remedies for violation of ECPA for non-constitutional grounds regarding electronic communications.

53  *Governmental Access to Stored Electronic Communications*

- ECPA sections 2701 - 2711
- Electronic service providers send and receive electronic messages and store them in "mailboxes". A message is not stored until it is received by the service provider / recipient.
- Generally there is a backup copy made for each message sent in case of system failure. Copy is with provider.

54  *Storage in different locations*

- ECPA protects only those communications in electronic storage in the possession of the provider. ECPA does not protect communications downloaded by the addressee to another computer not maintained by a provider.
- Provider = protected : Home computer downloaded message = not protected

55  *ECPA protects electronic communications maintained by:*

- electronic communication services (e-mail )
- remote computing services (data banks stored off - site)
- ECPA prohibits providers from disclosing the contents of communications to anyone, with certain exceptions

56  *Law Enforcement exceptions*

- law enforcement can compel disclosure from both types of providers by warrant or subpoena. The type of legal process required depends on the age of the communication and the pre-disposition of the government to inform the customer of the service about their request for contents.

57  *Law enforcement exceptions*



- ECPA also prohibits disclosure of information about their customers without legal process - identity of sender, location of origin of communication, identity of recipient.

- A communication obtained in violation of the Act does not result in suppression of the evidence (absent other constitutional violations)

58  *Electronic Communication Service*

- Usually an MCI mail service or CompuServe mail service

- ECPA defines the electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 2510 (15)

59  *Remote Computing Service*

- Includes anyone who provides "to the public...computer storage or processing services by means of an electronic communication system."

- This means that a bulletin board may serve as a remote computing service covered under ECPA.

60  *18 U.S.C. 2702 (1997) Disclosure of Contents*

- Prohibits disclosure to anyone except:

- addressee, recipient of communication or agent thereof

- as authorized under 2703

- consent of originator, addressee or recipient (public bulletin boards can be accessed by law enforcement)

- provider inadvertently obtains comm. which appears to be criminal - can disclose to law enforcement

61  *2703 - Requirements for Governmental Access*

- < 180 days requires a warrant

- 181 days or more gov. may use a warrant (no notice), administrative subpoena (notice), court order (delayed notice)

- (c) **records** - subscriber or customer (not contents of comm.) by warrant, court order or consent

62  *2703 (c)*

- **records** - include name, address, long distance telephone toll billing records, telephone numbers or other information about length and type of services utilized

- notice to customer not required under this section for administrative subpoena (2)

63  *2703 (d) Requirements for court order*

- any court of competent jurisdiction 3127 (2) (a)

- must offer specific and articulable facts that contents are relevant and

*material to an ongoing criminal investigation*

- *no state court may issue if prohibited under state law*
- *Service provider may move to quash if request voluminous or undue burden*

64  *2703 (e) Immunity for provider*

- *No cause of action against provider disclosing information under this chapter, nor employees, officers, agents or other specified persons if acting in accordance with the terms of court order, warrant, subpoena...*

65  *2703 (f) requirement to preserve evidence*

- *provider, upon request of gov. entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of court order or other process*
- *period of retention is for 90 days with option, on request of gov. for 90day extension*

66  *2704 Backup preservation*

- *may include in subpoena or order requirement to create backup of contents of communication*
- *without notice to customer*
- *ASAP w/in regular business (no later than 2 days after receipt of order)*
- *confirm to gov. backup created*

67  *2704 (a) (2)-(5)*

- *notice to customer by gov. in 3 days unless delayed under 2705*
- *provider shall not destroy backup until later of delivery or resolution of legal challenges*
- *provider releases no sooner than 14 days after no notice that customer has not challenged or challenge by customer not filed*

68  *2704 (a)(5)*

- *gov. entity may seek to create a backup copy in its sole discretion without notice to customer if there is reason to believe that notification may result in the destruction or tampering with evidence. This determination is not subject to challenge by provider or customer under 2703 (a).(search warrant)*

69  *2704 (b) Customer Challenges*

- *file within 14 days quash, vacate with written notice to gov. and provider.*
- *affidavit by customer shall state: they are a customer, contents have been requested, they are not relevant to investigation or no substantial compliance with the law.*
- *service*
- *sworn response (in camera) by gov.*

- 70  *2705 Delayed notification*
- *up to 90 days if court determines adverse result may be possible*
  - *adverse results*
  - *extension for 90 days*
  - *notice to customer after delay informing the date, agency, provision, and official in charge of action*
  - *may extend time of notification indefinitely if certain circumstances exist*
- 71  *2706 Cost Reimbursement*
- *fee for costs reasonably necessary and directly incurred, including disruptions in normal operations*
  - *Amount is mutually agreed upon or the court will decide*
  - *Records of common carrier are excluded, but court may consider case if unusually voluminous*
- 72  *2707 Civil Action*
- *except as provided in 2703 (e) a cause of action may be commenced against any entity that has violated ECPA*
  - *Damages - minimum \$1000, plus costs, punitive damages and attorney fees.*
  - *Disciplinary actions*
  - *good faith defense is complete*
  - *statute of limitations - 2 years from first discovery or reasonable opportunity*
- 73  *2708 Remedies*
- *Remedies described in this chapter are the exclusive remedies and sanctions for nonconstitutional violations of this chapter*
  - *Muskovich v. Crowell (1995, Iowa) 12 BNA IER Cas 647*
- 74  *2710 Wrongful disclosure of video tape rental or sale records*
- *not to disclose to law enforcement unless search warrant, state warrant, subpoena or court order used*
  - *court orders authorizing disclosure issue only with prior notice to customer and only if probable cause is shown that records are relevant to legitimate investigation.*
  - *Civil action-see liability*
- 75  *Liability - PPA*
- *Steven Jackson Games v. U.S., 816 F.Supp. 432 (1993) Secret Service ordered to pay \$50,000 in damages, \$195,000 in attorney fees, and \$57,000 in costs for violation of PPA*
  - *Minneapolis Star & Tribune Co. v. U.S., 713 F. Supp. 1308 (1989) violation*

of PPA, damages of \$750 per plaintiff, \$48,246.93 to one law firm, \$31,996.44 to a second firm, costs in excess of \$15,000

76  *Liability - ECPA*

- *Violations of ECPA may result in damages not less than \$1000. If damages are intentional or willful, punitive damages are authorized and costs, plus a reasonable attorney fee.*
- *Disciplinary action - if willful or intentional the court will order agency or department to investigate and a hearing to determine whether action is warranted against employee.*

77  *Liability - ECPA*

- *Good faith defense exists for law enforcement*
- *2 year statute of limitation*
- *Incidental seizure of e-mail on bulletin board by police officers did not violate ECPA because of good faith reliance on search warrant. Davis v. Gracey, 111 F.3d 1472 (1997)*

78  *Liability - ECPA*

- *Breaking or destroying equipment through negligence is actionable by victims*
- *Loss of business opportunity is actionable by victims, even if criminal activity is part of a wide sweep by law enforcement*
- *Failure to return equipment and comply with ECPA forms basis for liability*

79  *Liability - Searching and Seizing Computers*

- *Police officers must execute search warrants to avoid unnecessary destruction of property. Departments risk liability for failing to properly train officers proper procedures for searching and seizing computer evidence. Ginter v. Stallcup, 869 F. 2d 384 (1989)*
- *Tarpley v. Green, 684 F.2d 1 (1982)*

80  *Liability - Searching and Seizing*

- *Even perfectly reasonable search which destroys property may be a compensable taking... McGovern v. City of Minneapolis, 480 N.W.2d 121; Steele v. City of Houston, 603 S.W. 2d 786 (1986); but see Customer Co. v. City of Sacramento, 10 Cal 4th 369 (1995) holding that only innocent third parties would be eligible for compensation*

81  *ENTRAPMENT*

- *JACOBSON v. UNITED STATES*
- *112 S. Ct. 1535*
- *CHILD PORNOGRAPHY*
- *REVERSE STING*
- *SEVERAL AGENCIES OVER MANY YEARS*

- POLITICAL SPEECH ISSUE-1st amend

82  **ENTRAPMENT**

- UNITED STATES v. GENDRON, 18 F3d 955 (1994) - distinguished from Jacobson on predisposition issue. Grendon's correspondence sole desire was to view child pornography, not "launch a counter-attack against those who would curtail our freedoms."

83  **ENTRAPMENT**

- CHIN v. UNITED STATES, 833 F. SUPP. 154 (1993) - court distinguishes from Jacobson in that there is additional evidence of predisposition and that Chin demonstrated a predisposition to trade, loan, and order such material.

84  **SEARCH WARRANTS**

- STRONG PREFERENCE FOR SEARCH WARRANTS AND COURTS WILL SCRUTINIZE A WARRANTLESS SEARCH
- MOST COMPUTER SEARCHES WILL BE PURSUANT TO A WARRANT

85  **SEARCHING COMPUTERS**

- EXCEPTIONS APPLY
- PLAIN VIEW: LAWFUL POSITION TO OBSERVE THE EVIDENCE AND ITS INCRIMINATING CHARACTER IS IMMEDIATELY APPARENT.

86  **SEARCHING COMPUTERS**

- DETERMINE THE COMPUTER'S ROLE IN THE OFFENSE
- TOOL USED IN SENDING OUT PORNOGRAPHY
- REPOSITORY FOR STORING COMPUTER PORNOGRAPHY

87  **EXIGENT CIRCUMSTANCES**

- DEGREE OF URGENCY
- TIME FOR WARRANT
- EVIDENCE DESTROYED
- DANGER
- TARGET KNOWS YOUR COMING
- DESTRUCTIBILITY OF EVIDENCE
- MULTI - NETWORK INVOLVED

88  **BORDER SEARCHES**

- SOVEREIGN'S POWER TO EXCLUDE
- NO WARRANT REQUIRED
- NO PROBABLE CAUSE REQUIRED
- ONCE EVIDENCE IS IN COUNTRY AND CITIZEN DOWNLOADS

FROM BBS - DO YOU NEED A SEARCH WARRANT TO OBTAIN CHILD PORN?

- 89  *CONSENT SEARCHES*
- SPOUSES: DEF. MUST SHOW SPOUSE ACTUALLY DENIED ACCESS
  - PARENTS: MINOR CHILDREN
  - PARENTS: ADULT CHILDREN
  - EMPLOYEES: PUBLIC / PRIVATE
  - EXPECTATION OF PRIVACY
- 90  *CONSENT SEARCHES*
- OBJECTIVELY REASONABLE EXPECTATION OF PRIVACY
  - NETWORK SYSTEM ADMINISTRATORS
  - INFORMANTS AND UNDERCOVER AGENTS MUST GO NO FURTHER THAN PERMITTED BY DEF.
- 91  *CONSENT SEARCHES*
- SCOPE EXCEEDS CONSENT
  - PROPER PARTY CONSENTS BUT DATA IS ENCRYPTED
  - LIMITATIONS ON CONSENT EITHER IMPLIED OR EXPRESSED MUST BE HONORED
  - THIRD PARTY CONSENT TO COMMON AREA
- 92  *SEIZING HARDWARE*
- THREE THEORIES
  - CONTRABAND
  - INSTRUMENTALITY
  - EVIDENCE: PHYSICAL COMPONENTS- CENTRAL PROCESS. UNIT, KEYBOARD, MONITOR, MODEM AND PRINTER
  - PERIPHERALS
  - DOCUMENTS / DATA ONLY
- 93  *INDEPENDENT COMPONENT DOCTRINE*
- EACH COMPONENT IS ANALYZED INDEPENDENTLY
  - SEIZE ONLY COMPONENTS THAT ARE EVIDENCE OF A CRIME
  - OFFICERS MUST ARTICULATE A REASON FOR SEIZING THE ITEM
  - NOT JUST ANYTHING CONNECTED
- 94  *TRANSPORTING HARDWARE*
- HANDLING INFORMATION STORAGE DEVICES
  - CAREFUL PACKING

- TRADITIONAL EVIDENCE
  - INTEGRITY OF EVIDENCE
  - VIDEOTAPE / PHOTOGRAPH SCHEME
  - DRAW SCHEME
- 95  *WHERE EVIDENCE MIGHT BE*
- IDENTITY INVESTIGATION
  - FINGERPRINTS
  - HANDWRITTEN NOTES
  - LABELS
  - PASSWORD
  - TELEPHONE RECORDS
  - HARD COPY PRINT OUT
- 96  *SEIZING INFORMATION*
- INFORMATION AT THE SCENE
  - INFORMATION STORED OFF - SITE
  - CONTRABAND - SOFTWARE, ACCESS CODES, AND MANUALS
  - INSTRUMENTALITY - DIGITAL SOFTWARE USED IN FORMING COLLAGES OF CHILDREN FOR CHILD PORNOGRAPHY
- 97  *SEIZING INFORMATION*
- INFORMATION AS EVIDENCE
  - DOCUMENTS CONNECTING EVIDENCE TO CRIME
  - PATTERN OF MAILINGS
  - PORN EXCHANGE
  - HISTORY OF OPERATING CHATROOM OR BBS - PAPER OR ELECTRONIC IN FORM
- 98  *PROBABLE CAUSE TO SEIZE*
- HARDWARE
  - SOFTWARE
  - DATA
  - LOCATION OF SEARCH: SITE, FIELD OFFICE, OR LABORATORY
  - ULTIMATE GOAL
  - USE A SEARCH WARRANT
- 99  *DESCRIBING ITEMS TO BE SEIZED*
- WHAT ARE YOUR OBJECTIVES FOR SEARCH AND SEIZURE?
  - DOCUMENTATION, INSTRUMENT OR BOTH
  - BREADTH OF WARRANT DEPENDS ON SCOPE OF CRIMINALITY

- FOCUS ON CONTENTS OF RELEVANT DOCUMENTS, NOT DEVICES
- 100  *DRAFTING THE AFFIDAVIT AND WARRANT*
  - INDICATE WHETHER THERE IS ELECTRONIC MAIL ON TARGET COMPUTER
  - IDENTIFY MAIL TO BE READ
  - ESTABLISH RULE OF LAW THAT ALLOWS SEARCH
  - IF HARDWARE - FOCUS ON DETAILED DESCRIPTION OF COMPONENT
- 101  *WARRANT FOR INFORMATION SEIZURE*
  - DATA EXISTS IN ESSENCE, NOT IN FORM OR FACT
  - PHYSICAL LOCATION OF DATA UNKNOWN
  - LOCATION OF STORAGE: ON / OFF SITE
  - UNKNOWN LOCATION
- 102  *WARRANT - INFORMATION*
  - TELL MAGISTRATE ISSUING WARRANT NO WAY TO IDENTIFY SITE
  - INDICATE WHY THERE IS NO WAY TO IDENTIFY SITE AND DESCRIBE ALL ATTEMPTS TO LOCATE
  - DISCUSS THE NATURE OF STORAGE IN MULTI - NETWORK
- 103  *FOURTH AMENDMENT*
  - REQUIRES SPECIFICITY
  - PARTICULARITY
  - BREADTH/SCOPE
  - ASSUME THAT DETAILED AND CLEARLY DESCRIBED RECORDS ARE IN ELECTRONIC FORM AND SO PROVIDE IN YOUR WARRANT
  - GENERIC "ELECTRONIC" RECORDS ARE OVERBROAD
- 104  *NO - KNOCK WARRANT*
  - INJURY TO POLICE OFFICER
  - INDIVIDUAL
  - SUSPECT TO FLEE
  - DESTRUCTION OF EVIDENCE
  - COMPUTER CASES
  - PRESERVATION OF EVIDENCE
  - HOT KEYS, TIME DELAY, THESE PREMISES OR THESE PEOPLE
- 105  *SEARCHING TECHNIQUES*
  - UTILITIES SOFTWARE



- KEY WORD SEARCHES
- MODEM AND SOFTWARE EXPANDS SEARCH AND NEW WARRANTS
- RELY ON EXPERTS
- DISCOVERING THE UNEXPECTED NOT IN THE WARRANT - 4TH AMENDMENT

106 □ *DRAFTING THE WARRANT*

- COMPUTER CRIME UNIT, DEPT.. OF JUSTICE 202 - 514-1026
- ATF 301-217-5717
- FBI
- SEC.SERV. 202-435-7700
- DEA 703-557-8250
- IRS 202-535-9130

107 □ *NETWORKS AND BULLETIN BOARDS*

- ELECTRONIC BULLETIN BOARDS - MESSAGES ARE LEFT
- CHATROOMS ARE SUB - BOARDS
- PIRATE BULLETIN BOARDS = PORNOGRAPHY
- NOT PROTECTED BY THE FIRST AMENDMENT - NOT A LICENSE TO COMMIT CRIMES AGAINST CHILDREN

108 □ *ENCRYPTION*

- ENCRYPTED COMPUTER = LOCKED FILE CABINET
- WARRANT TO SEARCH AND SEIZE ENCRYPTED INFORMATION
- DOES THAT WARRANT AUTHORIZE BREAKING THE ENCRYPTION?
- LOOKING OVER SHOULDER?
- CASE SPECIFIC

156 ☐ *UNITED STATES v. KNOX*

- 32 F. 3D 733 ( 1994)
- KNOX KNEW THE CONTENTS
- KNEW TRAVELED INTERSTATE
- NO NUDITY WAS INVOLVED
- LASCIVIOUS CONDUCT WAS NOT FOCAL POINT - WAS THERE AN EXHIBITION, NOT CHARACTER OF EXHIBITION (DOST)

157 ☐ *JURISDICTIONAL ISSUES*

- *Searching a single personal computer is certainly different that searching a network of computers that reach around the world. Investigators must have intelligence that forms the basis of charging crimes and where those crimes occurred. Intelligence is crucial. Vendor/providers loyalty to the customer usually far outweighs any sense of obligation to police.*

158 ☐ *Jurisdictional Issues*

- *Multiple sites in same district - (several targets in the same building)*
- *Multiple sites in same district - different buildings*
- *There is some precedent for allowing connected computers within the same district to be covered under one warrant, provided no violations of 4th amendment*

159 ☐ *Jurisdictional Issues*

- *Multiple sites in different districts*
- *Did law enforcement know evidence was in a different district before executing a search warrant?*
- *United States v. Rodriguez, 968 F.2d 130 (1992)*

160 ☐ *Jurisdictional Issues*

- *Information at an Unknown Site*
- *Evidence at an off-site storage that law enforcement knew prior to execution of warrant, but does not know where the off-site storage is located*
- *Show a clear relationship between the target computer and connected computers*
- *Information/Devices which have been moved*

161 ☐ *Jurisdictional Issues*

- *Forum and jurisdiction is driven factually first and most importantly. In multiple jurisdictional crimes, prosecutors have options under most facts as to where to bring criminal charges.*
- *Resources*
- *Judges*

- *Prosecutor*
- *double jeopardy*

162  *Jurisdictional Issues*

- *If you are going to search off-site computers located in the same jurisdiction, include that authorization in your application for search warrant.*
- *If you are going to search or access a computer off-site in another jurisdiction, it is unclear whether you need a judge in that other jurisdiction to authorize that search.*

163  *Partnering for investigating and prosecuting computer crimes*

- *Sexual exploitation of children by using computers involve many jurisdictions, agencies and laws.*
- *How do we involve the prosecutors, law enforcement agencies and other professionals in coordinating resources, talents and time to investigate and prosecute these cases.*

164  *Partnering*

- *Identify resources in your jurisdiction*
- *Identify federal and state resources which are available*
- *Developing a relationship with the prosecutors in your jurisdiction*
- *Developing and maintaining a multi-agency team and protocol*

165  *Partnering*

- *Civil forfeiture - what is in it for me*
- *Community prosecution*
- *Innocent Images and the FBI policy regarding co-investigations with local, state and other federal agencies: why you need a separate protocol for dealing with the FBI policy*
- *Developing your own investigation resources and abilities*

166  *Partnering*

- *Computer Analysis Response Team*
- *Training Online Techniques*
- *Undercover and Sting Policy Guidelines*
- *Task Force Concepts*
- *Victim/Witness Coordination*

167  *THANK YOU FOR YOUR ATTENTION*  
*HAVE A GREAT DAY!*



# Resources





The National Center for Missing and Exploited Children

---

---

---

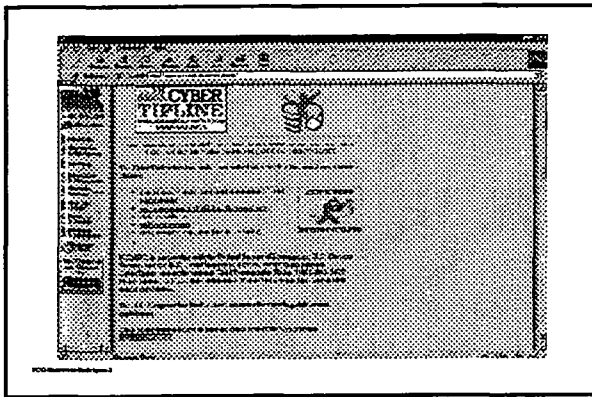
---

---

---

---

---



---

---

---

---

---

---

---

---

**CYBERTIPLINE REPORTING FORM**

**Exploited Child Unit**

How did you see this?

Child's Name: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

Phone: \_\_\_\_\_

Age: \_\_\_\_\_

Sex: \_\_\_\_\_

Reporting Person's Name: \_\_\_\_\_

---

---

---

---

---

---

---

---

Address

City State ZIP Postal Code

Country

Country or Area Code/Telephone #

City and State for return

Business or Home

Full Address

---

---

---

---

---

---

---

---

Business Information

Website URL

Internet //

Physical Street Address

Business Service Number of Telephone # with  
for AOL, CompuServe, INTERNET, etc.

Business Name of Company

Business Location (e.g. Street, P.O., etc.)

Business Telephone Number

---

---

---

---

---

---

---

---

Customer Information

Child's Name

Age

Address

City State ZIP Postal Code

Country

Business Customer

---

---

---

---

---

---

---

---



**SEARCH** **Help**  
 Request Name: \_\_\_\_\_  
 Date of Birth (FORMAT: mm/dd/yyyy)        
 Address: \_\_\_\_\_  
 City: \_\_\_\_\_ State: \_\_\_\_\_ Postal Code: \_\_\_\_\_  
 Country: \_\_\_\_\_  
 **Clear Request**

---

---

---

---

---

---

---

---

**Additional Information** **Help**  
 Please provide additional information or description (be specific).  
 \*The values entered should be typed in the screen.  
 Kill Rick Binicucci

---

---

---

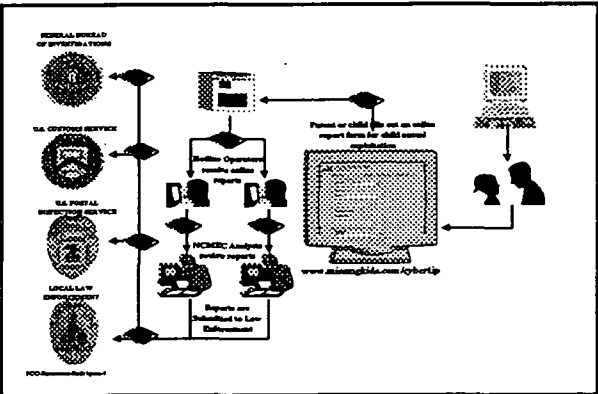
---

---

---

---

---




---

---

---

---

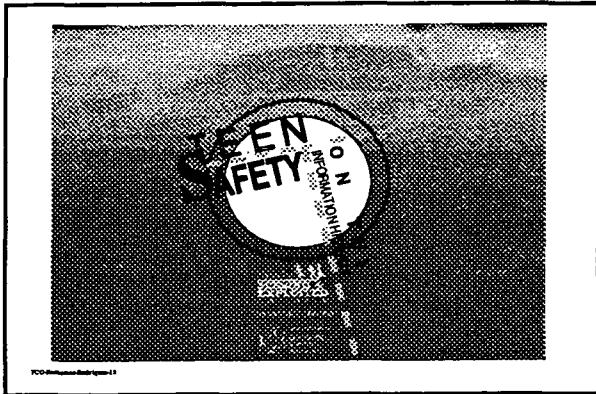
---

---

---

---





---

---

---

---

---

---

---

---

**Publication focusing on the review and analysis of laws dealing with child pornography both domestic and international**

**Child Pornography**

*Work In Progress*

*Domestic and International*

---

---

---

---

---

---

---

---

**ABA Children and the Law Study addressing the laws and issues dealing with Child Prostitution and Sexual Tourism**

**Child Prostitution and Sex Tourism**

*Work In Progress*

---

---

---

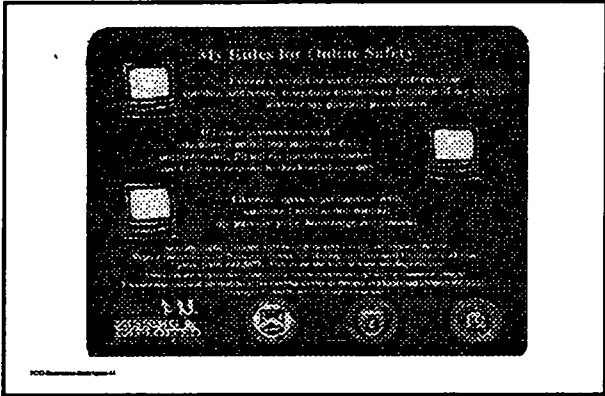
---

---

---

---

---



---

---

---

---

---

---

---

---



---

---

---

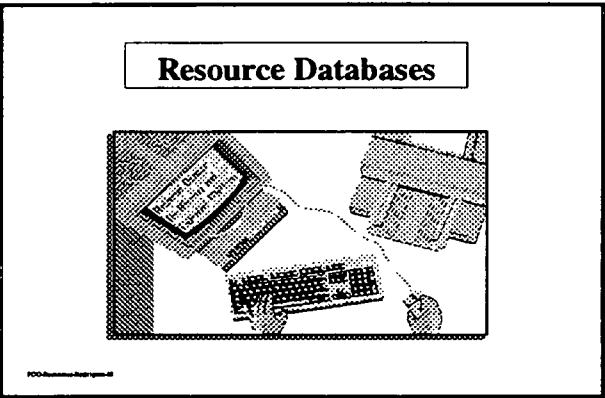
---

---

---

---

---



---

---

---

---

---

---

---

---

## Law Enforcement Contacts Database

Individual Contacts  
Worldwide that Deal  
with the Issues of  
Crimes against  
Children.



100-888888-888888-11

---

---

---

---

---

---

---

---

## State and Federal Task Forces

A database of federal,  
State, and local agencies  
and task forces that deal  
with crimes against  
children.



100-888888-888888-11

---

---

---

---

---

---

---

---

## Private Sector Resources

A database of private  
companies and organizations  
that deal with education and  
additional resources to law  
enforcement.

SEARCH  
HTCIA  
National White Collar Crimes  
FACCI



100-888888-888888-11

---

---

---

---

---

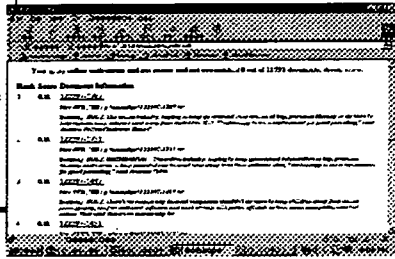
---

---

---

## News Article Archive Database

A database of new articles, available for research and analysis on the subjects of child sexual victimization issues.



---

---

---

---

---

---

---

---

## Additional Resources



---

---

---

---

---

---

---

---

## Public Records Database



Availability to search public records databases (CDB, Infotek, Autotrak, Lexis-Nexis) on leads pertaining to crimes against children.

---

---

---

---

---

---

---

---

## Secret Service Resources

### Forensic Services Division

Forensic Services Division (FSD) plans, directs, and coordinates forensic science activities within the Secret Service.

- Fingerprint and Handwriting Analysis
- Polygraph Examinations
- Audio and Video Enhancement



FOIA Exemption - Rule 6(e)(3)(C)

---

---

---

---

---

---

---

---

## Mapping Software



Geographic Information System software for street level plotting and analysis of leads.



FOIA Exemption - Rule 6(e)(3)(C)

---

---

---

---

---

---

---

---

## Training Programs

Training Programs for law enforcement on the issues of child sexual exploitation and missing children.

Investigating crimes on the Internet as it relates to sexual exploitation of children and missing and abducted children.



FOIA Exemption - Rule 6(e)(3)(C)

---

---

---

---

---

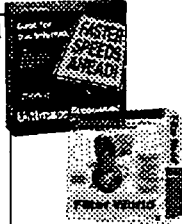
---

---

---

## Applications and Software Evaluation

Identifying Software and other applications (spiders, webcrawlers, intelligent agents) that may be of assistance to law enforcement officers investigating crimes against children via the Internet.



FOO Research and Systems

---

---

---

---

---

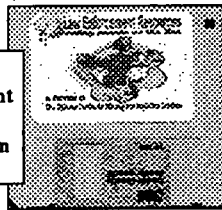
---

---

---

## Applications and Software Development

Developing programs that aid law enforcement officers obtain information available on the Internet.



FOO Research and Systems

---

---

---

---

---

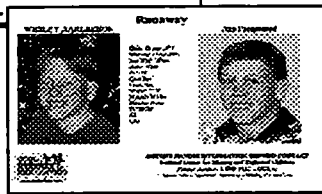
---

---

---

## Age Progression and Imaging

Specialists using advanced technology can assist in facial image enhancement or reconstruction.



FOO Research and Systems

---

---

---

---

---

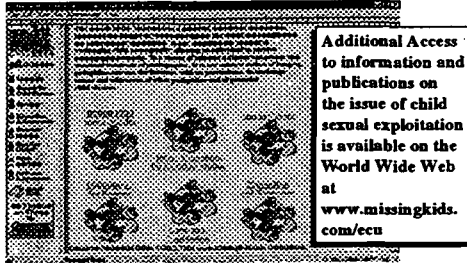
---

---

---



## ECU Web Site



---

---

---

---

---

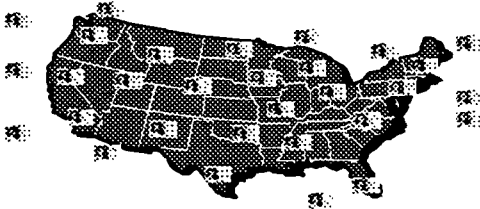
---

---

---

## Distribution of Images

Extensive network enables the transfer and posting of child posters worldwide in a matter of minutes utilizing the Internet or being sent via broadcast fax.



---

---

---

---

---

---

---

---

*For Assistance contact:*

**Ruben D. Rodriguez**  
Director

**Kathy Free**  
Program Manager

**Exploited Child Unit**  
1 800 843-5678

e-mail- [rrodriguez@ncmec.org](mailto:rrodriguez@ncmec.org)  
[kfree@ncmec.org](mailto:kfree@ncmec.org)

---

---

---

---

---

---

---

---

# A GUIDE FOR INTERNET SERVICE PROVIDERS TO ASSIST LAW ENFORCEMENT IN COMBATING CHILD EXPLOITATION

In recent years, some of the individuals in our society who prey upon children have discovered cyberspace. Some of these individuals are sex offenders and are using cyberspace to exploit and victimize children.

A computer sex offender is someone who uses online computer services or the Internet to prey upon children or other individuals they have discovered in cyberspace. These offenders sometimes collect and trade child pornography online and use their online access to locate and attempt to sexually exploit and victimize children.

The following guidelines are intended to show how Internet Service Providers (ISPs) can assist law enforcement in reducing child victimization in cyberspace. ISPs are cautioned, however, to consult with their legal counsel to determine how the laws of their state may apply.

## HOW CAN ISPs HELP FIGHT CHILD EXPLOITATION?

- 1) Require a positive means of identification when a customer opens an account. Verify that the credit card number, telephone number, and other information that is provided are accurate.

Computer sex offenders, as well as others interested in the commission of various types of online crimes, may provide false information when opening an online account. This can stymie investigative efforts. Requiring subscribers to provide addresses that match their credit card billing information can be effective in reducing subscription fraud and assisting in investigative efforts. Requiring a copy of their driver's license is a further step in fraud reduction.

- 2) Report any evidence of child exploitation to your local or state law-enforcement agency or the Federal Bureau of Investigation (telephone numbers for these agencies can be found under the "Government" section of your local telephone book), as well as to the National Center for Missing and Exploited Children (NCMEC) by calling 1-800-843-5678 or online at [www.missingkids.com/cybertip](http://www.missingkids.com/cybertip).
- 3) If you discover child exploitation being perpetrated by one of your subscribers, report it immediately to law enforcement and NCMEC. **Do not terminate the account nor take any other action that might alert the subscriber, until the appropriate law-enforcement agency has asked you to do so.**
- 4) If you believe that your system has been utilized for the commission of a crime, immediately contact a local, state, or federal law-enforcement agency. The law-enforcement agency may request that you preserve the information that your company has inadvertently obtained or was provided to your company through another party such as another customer.

An offender may seek to destroy evidence of his or her crime. Preserving the information that your company has obtained ensures that the law-enforcement agency, using the appropriate court process, may use this as evidence against the individual(s) in any future legal proceedings.

- 5) Remove news groups, bulletin boards, and/or forums that are used for the posting of child pornography, or delete the attached child pornography from postings.

While there is only a handful of such sources, they are responsible for a large quantity of the child pornography found in cyberspace. These sources are located in the "alt.sex" and

"alt.binaries" areas and are usually obvious. Just as a bookstore is not required to carry books that they do not desire, ISPs are under no obligation to provide any specific groups.

- 6) Educate your customers. Advise them of the software available to limit a child's net-surfing abilities. Place a link to the National Center for Missing and Exploited Children's web site ([www.missingkids.com](http://www.missingkids.com)) on your home page and suggest to new users that they visit the site.
- 7) Educate law enforcement. If your company conducts Internet training classes, consider inviting officers from local, state, and federal law-enforcement agencies in your area.

### WHAT IS REQUIRED FROM A LAW-ENFORCEMENT AGENCY FOR AN ISP TO TURN OVER INFORMATION?

**A**n ISP may freely report child exploitation or any other offense of which it is aware. Under federal law, a law-enforcement officer may obtain subscriber information from an ISP by issuing a subpoena. In some instances, a court order or search warrant may be required. The type of information that will be of interest to law enforcement includes

- \* name of the account holder
- \* status of the account (active, canceled by subscriber, terminated by ISP, etc.)
- \* address(es) of the account holder
- \* date the account was established
- \* account usage history
- \* E-mail address(es) belonging to the account holder
- \* billing method (includes credit card or bank account information, address, etc.)
- \* similar information on other accounts belonging to the same person or address
- \* electronic communications that have been in storage for more than 180 days

Under federal law, a law-enforcement officer may obtain electronic communications that have been in storage for fewer than 180 days by obtaining a search warrant. This would apply to files that may be stored on the ISP's server and in E-mail. Typically the search warrant is served on the ISP; then the ISP copies all of the files and E-mail onto disks and provides the disks to the requesting law-enforcement agency.

This brochure was written by D. Douglas Rehman, a former local, law-enforcement officer who was assigned to the Federal Bureau of Investigation's Innocent Images Task Force, and is distributed in partnership with the National Center for Missing and Exploited Children (NCMEC).

NCMEC was established in 1984 as a private, nonprofit organization and serves as a clearinghouse of information on missing and exploited children per federal statutes 42 USC § 5771 and 42 USC § 5780. The 24-hour, toll-free Hotline and CyberTipline are open for those who have information on missing and exploited children at 1-800-THE-LOST (1-800-843-5678)/[www.missingkids.com/cybertip](http://www.missingkids.com/cybertip). NCMEC is located at Suite 550, 2101 Wilson Boulevard, Arlington, Virginia 22201-3077.

NCMEC is the national clearinghouse and resource center funded under cooperative agreement 98-MC-CX-K002 from the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice.

Points of view or opinions in this work are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Copyright © 1998 National Center for Missing and Exploited Children. All rights reserved.





# “VICTIMS OF INNOCENCE”

Child Pornography and the Sexual  
Exploitation of Children: A Perspective  
From The United States of America



*Prepared By: Raymond C. Smith  
U.S. Postal Inspector - Program Manager  
U.S. Postal Inspection Service  
Office of Criminal Investigations  
475 L'Enfant Plaza West, SW  
Washington, DC 20260-2166*

INTRODUCTION TO  
CHILD PORNOGRAPHY

The sexual exploitation of children through pornography is a continuing tragedy that crisscrosses all social and economic classes, with little regard for the enduring grief and trauma it brings to its victims. We have come to realize that child pornography is not simply an "art form." It is, rather, the end product of deviant behavior resulting in the sexual molestation and abuse of children.

During the past several years, the public has become increasingly more aware of the proliferation of sexually oriented materials involving the abuse of children. These materials graphically depict children, sometimes as young as two years of age, engaged in a variety of explicit homosexual and heterosexual activities appearing in full-color magazines, slides, photographs, movie films, video tapes, and now, picture quality computer images.

Due to public outcry, and a series of well-publicized incidents involving child exploitation and abuse, state and local law enforcement efforts in the United States have all but eliminated the over-the-counter sale and viewing of child pornography throughout the country. Child pornographers and pedophiles now use the United States Mail and computers to traffic in this insidious material because they can buy, sell, trade, and remain somewhat anonymous. It is this cloak of anonymity and the compulsive nature of the pedophiles need to not only amass greater quantities of child pornography, but also to validate their behavior with others that has given the child pornographer the drive to engage in this criminal activity.

Child pornography is a permanent record of the sexual abuse and exploitation of children. The dangers of child sexual exploitation cannot and should not be minimized. This most despicable of crimes -- a crime against children -- results in physical and emotional suffering, ruined lives, and shattered dreams. Only through public awareness, vigorous investigation, certain prosecution and just sentencing can we hope to reduce this horrible crime.

THE U.S. POSTAL INSPECTION SERVICE

The U.S. Postal Inspection Service is the law enforcement arm of the United States Postal Service responsible for investigating crimes involving the U.S. Mail, including all child pornography and child sexual exploitation offenses. Postal Inspectors specially trained to conduct these investigations are assigned to each of its 30 field divisions nationwide. U.S. Postal Inspectors, as federal law enforcement agents, carry firearms, serve warrants and subpoenas, and possess the power of arrest.

Recognizing that preferential child molesters and child pornographers<sup>1</sup> often seek to communicate with one another through what they perceive as the security and anonymity provided by the U.S. Mail, Postal Inspectors have been involved extensively in child sexual exploitation and pornography investigations since 1977. Since the enactment of the federal Child Protection Act of 1984, Postal Inspectors have conducted over 2,500 child pornography investigations, resulting in the arrests and convictions of more than 2,200 child pornographers and preferential child molesters.

Postal Inspectors in the United States utilize an established, nationwide network of intelligence in implementing a wide variety of undercover programs designed to uncover suspects and develop prosecutable cases. These undercover operations recognize the clandestine nature of the targets and the inherent need of many offenders to validate their behavior. The techniques utilized in these programs include placement of contact advertisements in both national and local publications, written contacts and correspondence with the subject, and more recently, contact via computer bulletin boards. Postal Inspectors are ready to assist in any related investigation involving child sexual exploitation.

---

1. Child pornographers are not always active child molesters. Conversely, many child molesters are not involved in child pornography. Both types of offenders may use the U.S. Mail to correspond with others who share their interests.

The Postal Inspection Service has had specific responsibility for investigating the mailing of obscene matter for over a century (Title 18 U.S. Code, Section 1461). While over the years child pornography was, as a matter of course, investigated along with the obscenity matters, increased public concern over this material resulted in the United States Congress enacting the Sexual Exploitation of Children Act in 1977 (Title 18 U.S. Code, Section 2251-2253). The Child Protection Act of 1984 (18 USC 2251-2255) amended the 1977 Act by:

1. Eliminating the obscenity requirement.
2. Eliminating the commercial transaction requirement.
3. Changing the definition of a minor from a person under age 16 to one under age 18.
4. Adding provisions for criminal and civil forfeiture.
5. Amending the federal wiretap statute to include the Child Protection Act.
6. Raising the potential maximum fines from \$10,000 to \$100,000 for an individual and to \$250,000 for organizations.

On November 7, 1986, Congress enacted the Child Sexual Abuse and Pornography Act of 1986 (18 USC 2251-2256) which amended the two previous acts by:

1. Banning the production and use of advertisements for child pornography.
2. Adding a provision of civil remedies for personal injuries suffered by a minor who is a victim.
3. Raising the minimum sentences for repeat offenders from imprisonment of not less than two years to imprisonment of not less than five years.



On November 18, 1988, the United States Congress enacted the Child Protection and Obscenity Enforcement Act of 1988 (18 USC 2251-2256). These amendments:

1. Make it unlawful to use a computer to transmit advertisements for, or visual depictions of, child pornography.
2. Prohibit the buying, selling, or otherwise obtaining temporary custody or control of children for the purpose of producing child pornography.

More recently, on November 29, 1990, Congress enacted an additional amendment (18 USC 2252), making it a Federal crime to possess three or more pieces of child pornography.

#### THE U.S. CUSTOMS SERVICE

The U.S. Customs Service, Office of Enforcement, has Special Agents in every field office responsible for conducting child exploitation investigations. In addition, the Customs Service has foreign mail facilities in 22 U.S. cities that intercept illegal mailings. Every port of entry to the United States is staffed by Customs Inspectors whose responsibilities include interdicting child pornographic contraband and related articles. Customs Agents are currently involved in pro-active, undercover investigations to identify and infiltrate computer bulletin boards used for exchanging child pornography where border crossings are involved.

The Customs Service is authorized to award up to \$250,000 to any individual who can provide information leading to a significant seizure or arrest in a child exploitation investigation.

**Special Resources:**

The Treasury Enforcement Communication Systems (T.E.C.S.) is a computer system that contains reports of investigations, arrests and seizures, and information on border-crossing from around the world. The T.E.C.S. is utilized by Customs' Special Agents on a daily basis to assist in the investigation of sexual exploitation cases.

The U.S. Customs Service also maintains a seizure list containing information about prohibited pornographic materials which have been seized at the border.

Data bases maintained by the U.S. Customs Service are accessible by other federal investigative agencies and by state and local law enforcement agencies with permission.

THE FEDERAL BUREAU OF INVESTIGATION

The Federal Bureau of Investigation (FBI) is responsible for investigating suspected cases of child sexual exploitation involving interstate commerce.

The FBI assigns particular attention and priority to investigations indicating organized criminal activity, commercialized prostitution, and the manufacture or distribution of child pornography. FBI investigations have also identified computer networks and bulletin boards, both national and international in scope, in which child pornography is transmitted to clients or other members of the network.

Within the FBI there are agents who are specially trained to investigate cases of child sexual exploitation. There is also extensive technology to enhance investigations, including lab testing of fingerprints and body fluids, video enhancement, and technology targeted to computer crimes. The Bureau also has special expertise in behavioral analysis, such as offender profiling.

CHILD PORNOGRAPHERS AND THEIR COLLECTIONS

Unlike commercial adult obscenity dealers, domestic child pornographers rarely, if ever, openly advertise or solicit new business. Their operations are underground and restricted, in many instances, to dealing with known pedophile customers. In fact, child pornography exists only for the the pedophile. A pedophile is defined as one whose erotic imagery and fantasy are focused on children. Pedophiles have an abnormal sexual desire for children; and, as a group, they are the major producers, distributors, and consumers of child pornography. Reduced to its simplest form: no pedophiles -- no child pornography.

Child pornographers and pedophiles come from all walks of life. The occupations of some of the offenders arrested in the United States include: doctors, teachers, lawyers, law enforcement officers, clergymen, and businessmen. Some have occupations bringing them into frequent contact with children. Many hold respected positions in their community and have concealed their interest in child pornography for years. The hobbies of offenders include little league baseball and football coaching, dance instructing, scout leading, baby-sitting, volunteer firemen, and amateur photography.

When, during the course of an investigation, sufficient probable cause has been developed to indicate that a suspect has violated the child pornography statutes, a federal search warrant may be sought for the suspect's residence. Execution of search warrants usually leads to the recovery of child pornography, sexually oriented correspondence, and, quite often, the identification of child victims.

To the child pornographer, his collection is one of the most important things in his life. Why else would he risk fines, disgrace, and jail? The child pornographer's collection is never complete; he must always add to it. To acquire it, he usually

uses the United States Mail, computer systems, or produces it himself. As he acquires it, he organizes his collection carefully, for he will keep it as long as he can. In most cases, because he knows what he does is illegal, the child pornographer carefully conceals his collection. Although the pedophile's collection of child pornography is oftentimes "hidden" from the casual observer, it is almost always readily accessible to him, for it is from this collection of child pornography that the pedophile derives his own sexual gratification.

More recently, over the past several years, we have seen a significant increase in computer usage by these child pornographers through computer bulletin board networks and commercially available telecommunication systems. Today's computer technology allows for the electronic transfer of picture quality images at the touch of a button and makes "letter writing" much easier. Even though the computer, in some cases, is replacing traditional correspondence, our experience has shown these computer literate child pornographers still rely heavily on the mails to exchange video tapes and computer diskettes containing the child pornography.

Of late, it has not been uncommon for law enforcement authorities to seize personal computers and related materials that have been used to store data bearing on the identities of other pedophiles with whom the offenders have been in contact. Recent investigations, however, have revealed that pedophiles employ personal computers for purposes extending far beyond the mere storage of data. They are using them to carry out "private" conversation with persons of similar proclivities in communicating their sexual interest in and activities with children. Even more alarming today, many pedophiles are now using the computer to carry out these "private" conversations directly with children and, oftentimes, are successful in persuading the child to engage in sexual conduct with them.

Use of the mails and computers in the distribution of child pornography perpetuates the sexual abuse and exploitation of the children involved. Pedophiles believe there is nothing wrong with what they are doing, so naturally they are looking for other individuals who support their thinking. A pedophile will use "kiddie porn," both private, original material and commercial material, to seduce other children into participating in sexual activity with them. Once the pedophile seduces the child, he uses the pornography to blackmail the child into continuing the relationship or keeping their "secret" from others. The pornographer also exchanges the material with other pedophiles.

Who are the victims? Despite a popular notion that runaways and children from broken homes are the main targets of pedophiles, that is not the total answer. In most cases, the victim is the child "down the street" who has been seduced into a relationship by a trusted adult and then hides the fact because of guilt, shame, blackmail, or, in some instances, because, for the first time in their life, they have received attention and what is interpreted to be affection from an adult.

Few crimes, if any, are more heinous and detrimental to our society than the sexual exploitation of children. Governments and their respective law enforcement agencies should not have a "blind eye" toward individuals trafficking in child pornography. Through years of investigating this unlawful activity, it has become clearly evident, the most effective means to identify these individuals is through the development and implementation of pro-active undercover investigations. Generally speaking, this crime does not come "knocking at your door." It can be said, the easiest way to convince yourself that this criminal activity isn't occurring in your community is quite simple, don't look for it. In case after case, had it not been for the work of law enforcement agencies in the United States and our pro-active undercover investigative efforts, these offenders, arrested for violating U.S. laws and sexually abusing children, in all likelihood, would have never been identified and would still be abusing and exploiting children today and well into the future.

It is now time for all international governments and law enforcement agencies to unite and work together in a cooperative spirit. Our goal should be to eradicate child pornography, and in so doing, we will reduce the far too many incidents of child sexual exploitation. Only by combining our efforts, resources, and knowledge in a team approach to this hideous crime can we make a difference.

# Child Sexual Abuse Kills:

# The story of Justin and Matthew Wilke

In May 1985, Justin Wilke and his brother Matthew attended Camp Puh'Tok in Monkton, MD. There they met 23-year-old camp counselor Peter Dudley Albertsen II. Albertsen, ponytailed and mustachioed, befriended the youngsters, aged 9 and 11. The boys looked up to Albertsen, a seven-year veteran of the camp, who was studying to become a teacher. Pete played the dulcimer and taught arts and crafts.

Albertsen continued his friendship with Justin and Matt after camp was over. He became friends with the boys' parents, who thought of him as a wonderful "older brother" and "role model" for their boys. Albertsen began spending a large amount of time, sometimes even staying overnight, at the Wilke's residence in Upperco, MD. The parents began entrusting the boys to Albertsen's care for overnight visits at his home in Baltimore.

"This was the life," Justin would later write. "This was any kid's dream. I wanted to be as mature as Pete. And in my mind I was. I would do anything to keep the relationship. I knew that he was the best friend any kid could ever have ... so I thought."



During one of the weekend visits to Baltimore, Albertsen began to sexually abuse the boys.

#### Justin's story

It started with tickling and play wrestling. That went on for about a year. Then Albertsen began to separate the boys and play games with them in private.

One hot summer evening in 1987, Pete persuaded Justin to play a new game — Pete would be the photographer and Justin would be the model. Albertsen, who had already painted a picture of 11-year-old Justin, told the boy he wanted to do a series of pictures: one with Justin wearing jeans, then wearing just his underwear, and





He was ordered to undergo therapy and have no contact with Justin or Matt.

### The stalking begins

The Wilke family enrolled in counseling sessions, but quit after six visits. They weren't comfortable talking about Pete. They decided to bury the problem and keep it a secret. Mental health experts say this is the worst possible way to handle trauma.

Despite the restriction placed by the courts, Albertsen continued to pursue Justin. He began a writing campaign, mailing dozens of cards and letters to Justin, unsigned and postmarked from different places to throw off Justin's parents. He left love letters, poems and notes on Justin's car and on the cars of Justin's friends. Albertsen began secretly watching Justin and showing up at events he knew Justin would be attending.

In May 1994, Pete called Justin and told him he had watched his high school graduation from a hidden spot in the trees. He mailed Justin a letter every day for a month before his eighteenth

birthday and said he would be standing in Justin's driveway that day. Included in one letter was a refrigerator magnet that spelled "Happy Birthday, Justin."

On the weekend of his birthday, Justin and a girlfriend left town. Justin was afraid that Pete would be watching him. He believed Pete would kill him if he couldn't have him.

Shortly after Justin's birthday, Albertsen left the United States for Germany on a student visa.

### Coping with the damage

When Matthew and Justin attended Loyola High School in Baltimore, they were required to perform volunteer work in the community. First Matt, and later Justin, decided to volunteer at St. Vincent's Center for abused and neglected children in Baltimore County.

At St. Vincent's, the boys met and worked with children who had been sexually abused. Matt and Justin worked under the direction of Father Ray Chase, who became their friend. They told Father Ray about their abuse at the hands of Peter Albertsen.

close and nurturing relationships. While the boys never discussed specifics about their own stories, Matt let Father Ray know he had told Albertsen to stay away from his brother.

Father Ray knew that Matt's chief concern was to protect Justin from Albertsen. Matt often told Father Ray he felt he had failed to protect Albertsen from abusing Justin when they were young.

In the fall of 1993, after graduating from Loyola and enrolling in college, Matt attempted suicide, but was unsuccessful. He told Father Ray, who visited him in the hospital, that he felt that the world "would be better off with him gone."

Matt feared that, because he had been abused, he would either be perceived as, or actually become, a pedophile — just as Albertsen had predicted.

Father Ray assured Matthew that this was not an automatic consequence of child abuse, but Matt didn't seem to believe him.

### Painting his pain

Like his older brother, Justin never discussed specifics about his abuse by Albertsen, but he did tell Father Ray that Albertsen was stalking him and that he was afraid that Pete would kill him.

After graduating from Loyola, Justin enrolled at the Maryland Institute, College of Art. He began to develop into a skilled artist and started expressing himself in writing. Father Ray suggested a project for Justin: to create a series of paintings and writings that would depict his abuse as a child and the effect it had on him and his family. It would be a way to help others heal their wounds from sexual abuse.



**Matt Wilke in 1992. He was an avid mountain biker and photographer.**



**Justin Wilke in 1994. He was a skilled painter, music fan and car mechanic.**

According to Father Ray, Matt's work with one of the children at St. Vincent's, helping the child cope with the emotional consequences of his history, was wonderful. Justin worked for a year with two small girls, with whom he developed

Justin's first painting dealt with the pain and vulnerability of being abused. A second painting depicted Justin's dehumanizing experiences with Albertsen. A third revealed the effect of Peter Albertsen's abuse on the Wilke family. The fourth painting was intended to express to others his current state of mind, years after the abuse.

Justin finished the paintings in October 1994. He wrote three pieces to accompany his artwork, and dedicated the series to Matthew:

"This story is dedicated to my brother, two years my elder. May this help you understand me, for you are the one with whom I silently endured this trail of emotion. May these writings and artwork open a door through which we can both reflect on what has happened to us and what will happen in the future. Please try to understand me, and help me lift this wall of silence between us ... I love you, bro."

The first painting was accompanied by a short story he titled "Solitude." It revealed that Justin still viewed Albertsen as his best friend — a best friend who had betrayed him:

"I remember confusion. I remember emptiness and the sickening feeling of helplessness. I can remember the way I felt when he looked at me with that glassy stare. I can picture it. I can remember trying to imagine why Pete would want to take videotapes of me undressing. It may seem like that is an obvious sign of someone that is not mentally stable, but to an eleven-year-old, it is a bit more confusing.

I can remember how I felt physically ill after he touched me. I still remember him taking me out for hot dogs and burritos afterward as if nothing had ever happened. I can still remember him saying he loved me. I can remember hating him.

I still hate him ...."

In Justin's second painting and poem, he describes Pete's calculated actions, lies and deception. Justin's third piece, accompanied by a letter in which he prays to God to help him, describes



Father Ray Chase and Matt Wilke in April 1996.

Albertsen's impact on the Wilke family: Albertsen is depicted as Satan clutching the neck of Justin's mother, Susan, and Albertsen's house is shown with a red light in the window. In the letter, Justin speaks of Albertsen's impact on his life and the life of Justin's family.

Justin's fourth painting was completed in the fall of 1995, and portrayed the theft of his youth at Albertsen's hands. The event had reduced his childhood to a vague memory. The writing accompanying the painting revealed the devastating impact the abuse had on Justin's self-esteem.

"I cannot pinpoint the demise of my self-esteem or the fading of my concentration on life ....

I sometimes try to think of what I was or where I was before Pete. I want to know if I was happy then, but for some reason, before I was 13. I cannot remember much. Maybe I can remember smatterings of things, but nothing very solid ....

Short-term memory and attention deficit haunts me every day. The hazy image of what I once was lingers over me like a tattered tent, full of vague holes and cold drafts of unpleasant childhood memories ....

My brother, father and I do share at least one thing in common. We all hate Pete and we would give up everything we had to turn back time and avoid the hell that seemed to create the paths of the rest of our lives for us."

About one year later, St. Vincent's Center began exhibiting Justin's paintings to professionals and others in the field of child sexual abuse. It was intended to be part of a process to help people explore and understand, through Justin's art, the emotional devastation caused by child sexual abuse from the perspective of an abused child.

In 1993, Matt tried, unsuccessfully, to kill himself again, using a gun he took from a neighbor's house. When he came home from the hospital 10 days later, he found out his mother and father were separating.

#### A prohibited mailing

Although Pete Albertsen was in Germany on a student visa, he continued to "stalk" Justin Wilke — this time by mail.

In May 1995, Justin received a package from Germany. It was timed to coincide with his birthday.

Justin recognized the handwriting and the postmark and knew instantly who had mailed it.

In the package was a birthday card; two sealed letters, marked "A" and "B"; two photographs of Albertsen; and a videotape. The video was in a format that could not be viewed on American equipment.

Justin panicked. He was afraid the videotape contained sexually explicit scenes Albertsen had taped of him years earlier.

In the "A" letter, Albertsen told Justin the "proverbial ball is in your court," and he asked him to respond to his letter. "No answer is an answer, and in this case I will define it as 'no.' So if I don't hear 'Wait for me, I don't know, or f— off, (silence = go to hell),' next year around your birthday, I will send one last birthday card and say good-bye."

Letter "B" was 22 pages long. Albertsen went into great detail describing their relationship, including the sexual acts he had performed on Justin. Albertsen knew the letter would cause problems and wrote, "If you are still in the middle of school exams it may be better to wait until you have finished the semester before you deal with this letter."

Albertsen asked in the letter:

"Did I injure you? What is the extent and nature of the injury? Did I destroy you? What was the mechanism of the destruction? Were my actions careless? Were they criminal?"

Justin never viewed the videotape. He gave the package to Father Ray, who surrendered it to an attorney employed by the Maryland Department of Social Services. The attorney interviewed Justin and

Matthew, who hired him to handle their claim against Peter Albertsen as a result of harassment and other objectionable actions.

The attorney viewed the tape and was relieved to find Justin was not on it.

**"The tape contained images of children under the age of 18 engaged in sexually explicit conduct. Its mailing constituted a federal crime."**

The tape contained images of children under the age of 18 engaged in sexually explicit conduct. Its mailing constituted a federal crime.

The attorney contacted the U.S. Postal Inspection Service and U.S. Customs Service.



**Pete Albertsen at the time of his second arrest, the day after Christmas, 1996.**

#### **Child abuse kills**

In the months following receipt of the package, Justin became anxious and depressed. Justin's father, Donald Wilke, wanted to

pay for any costs associated with stopping Albertsen from stalking his son. He felt he had failed to protect his sons.

Donald was depressed about his sons' problems and his own failed marriage. On November 30, 1995, Justin found his father's body in the family car. Donald had taken his life by carbon monoxide poisoning.

Justin and Matt were traumatized by their father's suicide. Matt became quiet and kept to himself. Justin, normally an easy-going kid, was agitated and withdrawn, and he stopped talking to friends.

Justin blamed Pete Albertsen for the death of his father, at least in part, and felt he had lost his last line of defense against Albertsen's stalking. He spoke of feeling trapped.

Within a month of his father's death, Justin created a fifth painting, his last artwork. There was no writing to accompany the piece. The painting depicted his father dead in the car, just as Justin had found him. It included a photo of a pair of outstretched hands holding a baby rabbit. Justin told Father Ray that he wanted people to know that child abuse kills.

#### **I hate you Pete**

On February 8, 1996, Justin Wilke was found dead in a car behind a service station in Cockeysville, MD. The station was next to the funeral home that had handled his father's funeral. Justin had died at his own hands, by carbon monoxide poisoning. On the passenger seat next to his body was a note that read:

"Sell everything I have and donate the money to St. Vincent's. I love you all — Justin.

I hate you Pete! F— off."

Matthew Wilke was destroyed by the suicides of his brother and father. He felt he had failed miserably to protect his brother from the abuse and continued stalking by Peter Albertsen.

Matt wanted to see Albertsen brought to justice. He met and agreed to cooperate with Postal Inspectors and agents from the U.S. Customs Service to lure Albertsen back into the country. But he could not fight his sadness, his loneliness and his fear of being left alone.

On August 15, 1996, a farmer working in his field found Matt's body in a car. Like his father and brother, he had committed suicide by carbon monoxide poisoning.

Matt left a note saying that he hoped everyone would forgive him, but he could not go through a fall or winter without his father and brother. Along with the note was a teddy bear he had received as a child, a gift from his father.

Five days later, Peter Albertsen was officially charged with trafficking in child pornography via the U.S. Mail.

On December 21, 1996, U.S. Customs received information that Albertsen might have re-entered the country. Postal Inspectors and Customs agents conducted a surveillance of Albertsen's mother's home during the Christmas holidays. On December 26, 1996, Albertsen was arrested.

In an interview with Inspectors and Customs agents, Albertsen admitted that he knew Justin and Matt had

committed suicide. He was sad, but did not feel responsible for the deaths.

#### **The tragedy comes full circle**

On March 21, 1997, Peter Albertsen pleaded guilty to one count of mailing child pornography to the United States.

Sentencing was set for July 11. In an emotional four-and-a-half-hour hearing, the government called only two witnesses. Postal Inspector Tom Boyle testified to the overall investigation, arrest and post-arrest interview of Peter Albertsen. Father Ray took the stand and spoke about the victims and the terrible impact Peter Albertsen had on their lives. He dimmed the lights in the courtroom, illuminated Justin's paintings and read aloud the dead boy's words. There were sobs in the audience.

The tragedy had come full circle. The one positive thing Justin had gained from his relationship with Peter Albertsen — his art — was the very thing Justin was able to use to show others his abuse and damage.

Peter Albertsen offered a few words, too, but they were not what anyone had expected. Rather than express remorse, Albertsen offended the judge and the courtroom, declaring that he had loved Justin and Matt. He said he was the only one who would remember them in 10 years' time.

U.S. District Judge William Nickerson sentenced Peter Albertsen to 10 years in prison, the statutory limit. The judge stated that the sentence was inadequate for the crime.

The unconscionable actions of Peter Albertsen had triggered the suicides of Donald, Justin and Matthew Wilke. But Albertsen's actions also sealed his own fate: If Pete had never mailed Justin the videotape of child pornography, he might never have been brought to justice.

Postal Inspectors have heard too many tales like this one. It's why the U.S. Postal Inspection Service remains committed to aggressively pursuing those who use the mail to exploit children.

#### **Postscript**

In October 1997, Albertsen admitted he had violated the terms of his original, suspended three-year sentence by mailing Justin the letters and the child pornography videotape in 1995. The three-year sentence was therefore reinstated, and added on to the ten-year sentence Albertsen is already serving.

### **Preventing Child Abuse**

**If you are interested in securing Justin's artwork for a presentation or training session for professionals in the field of child abuse, or would like to contribute to a fund Justin established to nurture the use of art with abused children and for programs related to the prevention of child sexual abuse, please call Father Ray at St. Vincent's Center in Baltimore, MD, at (410) 252-4000, ext. 1607.**

This article was a joint collaboration of Special Agent Lisa Ward, U.S. Customs Service, Baltimore, MD; Assistant U.S. Attorney Andrew C. White, Baltimore, MD; Assistant U.S. Attorney Christain Manuelian, Baltimore, MD; and Postal Inspector Thomas E. Boyle, Baltimore Domicile, Washington Division.



### **The first painting**

Justin represented himself as a young girl in this pen-and-ink work. His strongest reason for using this image was his concern that people would be less sensitive to a man's pain, as society does not "allow" men to be victims without also being accomplices in their victimization or deficient as men.

Nearly hidden in the lower folds of the girl's skirt, a child screams as a hand closes around her throat — sexual abuse is experienced as an attempt to murder, or kill. The girl's legs are drawn close to her body, self-protectively, but her hand is deformed, revealing Justin's sense of vulnerability and his inability to protect himself from Pete and further victimization. In this bleak image, Justin shows that most people are in the darkness about child sexual abuse: They are rarely aware when it occurs, so its young victims are left defenseless and in pain.

**Father Ray, of St. Vincent's Center, exhibits Justin's paintings and writings to educate professionals and others in the field of child sexual abuse about the experience of abuse from a child's perspective.**



### **The second painting**

At left, Justin lies awake, unable to sleep. His thoughts are trapped in the prison-like hurt of his abuse. Both the heart and its rhythms are reversed in the picture: Justin is confused about himself and his feelings for Pete. The words below, "Keep the secret until I die," reveal the internal and external messages that caused Justin to continue to be terrorized. He depicts himself as a young girl, surrounded by the golden glow of innocence as she looks at a book with a picture of a jester crying. The jester weeps for the child, who is dressed in harlequin colors, indicating she will play the fool. Her spread legs indicate the vulnerability of childhood. One hand is held behind her in a gesture of helplessness, and the other rests in the flowing red of the evil that is child sexual abuse.

The white figure being pulled by its limbs may indicate how Justin felt torn apart by Pete, who sometimes felt like his best friend and other times his worst enemy. The man behind the camera is Pete, who took pictures of Justin, making him feel exposed. Pete is painted without ears; he wasn't interested in what Justin had to say and wouldn't or couldn't listen to how his actions affected Justin. The figures that appear at the side of Pete's head are math calculations — Pete's actions were well planned. The rectangle at the upper left is an actual postcard Justin received from Pete before he went to Germany. It contains lines from a haiku verse written by a Japanese poet, Issa.

The painting is expressed as a strip of film: Pete "exposed" Justin to abuse, and Justin is exposing Pete's abuse through his art. In the lens of the camera, which Justin fashioned to jut out of the painting in 3-D, is a photo of a half-nude boy.



### The third painting

Pete is depicted as the devil, clutching the boys' mother by the neck, indicative of how Susan Wilke was victimized by her trust in Pete. She is painted as a pale figure, without hands, powerless. The building in the background was Pete's home in Baltimore, and the room with the red shade is where Justin and Matt were abused. A girl, who is meant to be a composite of the brothers, is staring away from a photo album of a childhood the boys never had. The ghostly man, seated and holding his head in his hands, is Donald Wilke, the father. The image projects his sense of helplessness and inadequacy in protecting his sons. No one in the picture is on the same linear plane; the family members are isolated from one another.



### The fourth painting

Justin painted this picture in response to a question about how he was doing, years after the abuse. The old woman is Justin, who felt old when he looked back at his lost youth. Justin attached a photo of a young woman just above the figure of the older one, as if the girl is an image in the older woman's thoughts. Justin didn't want to find himself an old man still grieving over his lost youth. He painted this picture on a bed linen primarily with his fingers, possibly intending that the black paint would gradually fade, as indeed it has. At the left side of the painting is an image of Christ. Oddly, although the rest of the picture is fading, the image of Christ has retained its brightness.

Justin wanted this painting to be illuminated from the front when shown. He intended it to be more hopeful than the others. The golden light, which covers more than half of the painting, is a positive image: Christ watches over the woman in the light that washes across her. Even the young woman is painted in gold, indicating that Justin was beginning to come out of the "darkness" and his lost childhood was beginning to shine through.



### The last painting

Justin painted this picture less than a month after finding his father dead in the family car; the painting duplicates the exact scene of the death. Justin worked in a frame shop and framed all of his artwork. He used non-glare glass to frame this picture, which meant that, to see it clearly, the viewer is forced to stand directly in front of it, just as Justin was forced to see his father's death. An actual photograph, which was left on the dashboard of the car where Justin found his father, is mounted on the painting and shows a pair of outstretched arms holding a baby rabbit. Justin said that if people showed the same compassion for abused children as shown towards this rabbit, these terrible events would never have happened.

Justin never wrote anything about this painting, although he wrote about all the other paintings in the series. When asked what he wanted people to "take" from the painting, he said: "I would say that child abuse can kill."

# PROJECT SPECIAL DELIVERY

*Postal Inspectors Bust Child Porn Ring — and its Patrons*



It's hard to believe that Postal Inspector Dave Austrum's response to a postal customer's complaint in December 1993 would lead Inspectors to shut down the largest commercial child pornography ring ever encountered by U.S. law enforcement. Project Special Delivery, a pro-active, undercover investigation conducted by the U.S. Postal Inspection Service, not only shattered an international cartel of child pornographers, it went after its customers as well. It's the customers' demand for this illicit material that creates a market for child pornography, a crime that victimizes children around the world.

Project Special Delivery began when Inspector Dave Austrum

learned that a Minneapolis man received an unsolicited videotape of child pornography from a mail-order company called Overseas Male (OSM). The video was actually a promotional tape, referred to by OSM as a "video catalog," featuring short previews of young, underage boys engaged in various sexual acts, and ordering information for full-length features. The return address placed the business in San Diego, so Dave forwarded the tape and some OSM advertising brochures to Postal Inspector Don Trutna of the former San Diego Division.

Inspector Trutna tracked down OSM's business address to a mail drop (commercial mail receiving agency) in San Ysidro, CA, a

community on the U.S.-Mexican border; you can see the Tijuana International Airport from the street in front of the mail drop. The owners of the mail drop company told Inspector Trutna that OSM received high volumes of mail, which they forwarded several times a week to another mail drop in Mexico. OSM was using a fake return address on its videotape mailings.

Using the undercover mail drop of Postal Inspector Karen Cassatt from the Phoenix Division as a return address, we ordered some of the OSM videos. Inspector Cassatt soon sent us our purchases. All of the material was graphic child pornography, with

obviously underage children holding starring roles.

Inspector Trutna called OSM in Mexico, using one of the numbers listed in its literature. The man who answered called himself "Jose." Jose assured us that some models in the videos were under 18. He said that was why OSM was in Mexico.

#### The real work begins

On June 29, 1994, Inspectors from U.S. Customs arrested James Kemmish for currency violations upon his re-entry to the United States from Mexico. Customs Inspectors found over \$16,000 in undeclared cash and money orders in Kemmish's possession. They also found videotapes, disguised as audiotapes, containing child pornography. And business records for Overseas Male.

U.S. Customs Special Agent Shirley Harris, a member of an interagency child exploitation task force in San Diego, remembered that Inspector Don Trutna was working a case involving Overseas Male and called him for help. The two spent the next day with Assistant U.S. Attorney Barbara Major drafting a search warrant for Kemmish's San Diego apartment. They executed the warrant with members of the San Diego Police Department and Sheriff's Office. What they found at Kemmish's place stunned them.

From the outside, Kemmish's home looked like any other beach area apartment. Inside, however, was a state-of-the-art production facility used to duplicate videotapes. There were tapes of children having sex with other children and with adults, children as young as seven years old. High-end Super VHS recorders, Hi-8

decks and 20 industrial duplicating machines flanked stacks of high-quality, master videotapes of child pornography. And more than 2,000 solicitations from Overseas Male ready to mail to addresses across the United States.

Inspectors noted the quality of the images and sophisticated effects used in their production. These were not old copies of tapes transferred to video, but state-of-the-art productions from around the world. There weren't many business records in the apartment, but there was a fax machine with

business practices of Overseas Male. Using intelligence gathered from the investigation, we would target OSM customers who had been relying on the U.S. Postal Service to deliver child pornography. Our company would be called "Island Male."

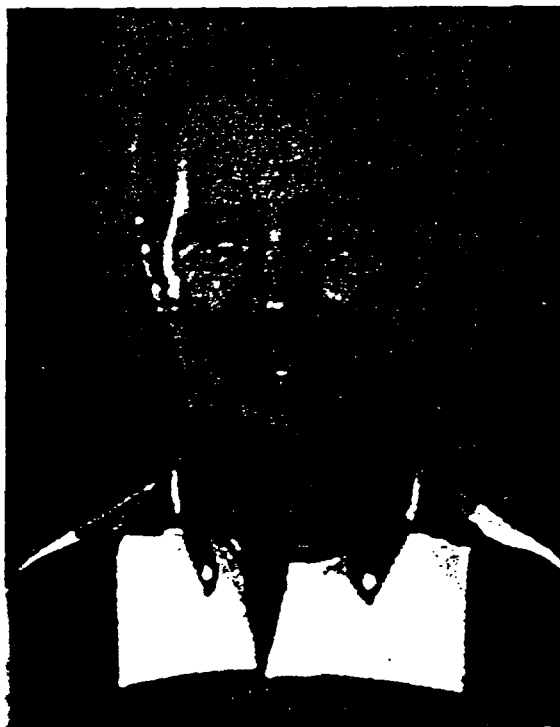
Inspector Ray Smith began meeting regularly with members of the Child Exploitation and Obscenity Section (CEOS) at the Department of Justice (DOJ) in Washington, DC, a group that specializes in child exploitation investigations. We worked hand-in-hand with DOJ attorneys to develop an investigative strategy that would be legally sound and withstand any claims of entrapment or outrageous government conduct. Even Attorney General Janet Reno was personally briefed on the initiative, and gave her department's full support.

We were able to expand our customer base when Inspector Smith received additional names of suspects in the United States from a Belgian colleague at a meeting of Interpol's Standing Working Party of Offenses Against Minors in Lyon, France. The names were found after John Stamford was charged in Brussels with depravity of youth and child prostitution.

Stamford founded Spartacus International, Ltd., a worldwide organization which distributed publications such as *PAN (Paedo Alert News)*, a magazine about sexual relations between men and boys.

#### Building the case

Within weeks of the takedown, Inspectors called Jose to complain about an unfilled order. We learned



James Leroy Kemmish

printouts of the latest orders from Mexico.

The ink had barely dried on the search warrant when Don and Team Leader Andy Thomas called Program Manager Ray Smith at National Headquarters and briefed him on the results of the search. Their decision was unanimous: It was an ideal opportunity to set up an undercover operation — a "reverse sting" — following the



OSM was in trouble due to "a major catastrophe" (meaning Kemmish, his distributor, was out of commission). But we received brochures again a few weeks later from other companies offering tapes from OSM's catalog. Our undercover purchases confirmed this.

We fine-tuned Project Special Delivery with CEOS at the Department of Justice throughout the fall and into the winter of 1995. Inspector Trutna left the group when he was transferred to work with the Revenue and Asset Protection Program (RAPP) Team. The San Diego portion

of Special Delivery and the Kemmish-Jose investigation was passed on to me.

We added more customers to our Island Male mailing list, this time compliments of the Vancouver Police Department in British Columbia. The Vancouver police found that a number of U.S. citizens were buying child pornography through the mail from "Out in the West Productions," a commercial distributor they had recently shut down. We also knew that two companies based in California were distributing OSM's material.

It was now evident that if Project Special Delivery was to succeed we had to close down these satellite businesses and neutralize Jose; otherwise, OSM's customers — now our customers — would know something was up.

As we continued building our case against Jose and OSM, we got a crucial lead: "Jose" was Troy Anthony Frank. The investigation suddenly became far more disturbing.

**An evil man**

Troy Frank began his career in child pornography in

Greeley, CO, where he was arrested by local police and later convicted for child molestation. He was sentenced to probation on state charges. Frank moved on to San Diego and continued producing his videos, meeting James Kemmish there in the late 1980s.

Just as the San Diego police were about to shut down Frank's operation, he fled to the Netherlands via Mexico. Frank again eluded authorities in Amsterdam, when they shut down a major child pornography operation in the area with ties to Frank. He returned to Mexico using the alias of a deceased Colorado police officer.

Meanwhile, Colorado police issued a state arrest warrant against Frank for child molestation, and the Department of State obtained a federal arrest warrant against him for passport fraud. U.S. Customs officials began working with high-level Mexican authorities in 1994 and 1995 to track down Troy Frank, without success.

**Full speed ahead**

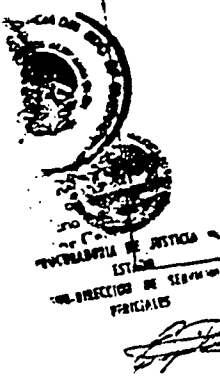
On July 10, 1995, Inspectors led by Ron Higa of the Los Angeles Division and Fred Renfro of the San Francisco Division executed nearly simultaneous federal search warrants at businesses we believed were involved with OSM. Inspectors Andy Thomas and Karen Cassatt initiated actions to stop mail being delivered to Frank's mail drops in San Ysidro, CA, and Phoenix, AZ. With the full approval of the Department of Justice, Project Special Delivery was cleared to go.

The next day we mailed our first "Island Male" solicitations to suspects from the Kemmish, Spartacus and Out in the West Productions investigations. Only days later I received requests for information. I mailed this group a second letter, graphically



Suicide note believed to have been left by Troy Anthony Frank for his mother.

*Mother,  
I am truly sorry that it had to  
end this way. I know the pain and  
suffering this will put you through. Please  
forgive me. Always be comforted that  
I will always be near you. I have  
tremendously missed being near you for  
the last few years. You are always  
in my thoughts and heart.  
Circumstances finally got out of control and  
I had no choice. It is definitely a  
terrible state that this has led to.  
Please hang on to all treasure the  
many happy moments that we shared together.  
I love you all.  
Your son  
Troy*



describing Island Male's products and enclosing order forms. Some of the orders for child porn came back faster than requests for information, but the child pornographers would have to wait until we were fully ready to deliver our product.

Project Special Delivery was running at full speed. On some days I received over 150 responses. The only problem was Frank, still at large in Mexico. On the evening of July 18, 1995, we played our last card.

We called Jose. "We know who you are," we told Troy Frank. "and we know where you are in Acapulco. We have federal and state arrest warrants ready for you."

We offered Frank three options: He could surrender himself to Special Agent Ed Lennon at the Embassy in Mexico City, he could surrender himself to us at the border or he could take his chances with the Mexican authorities. Frank said he'd think about it and call us back.

That was the last we heard from Frank. No one answered his phone, and the service was finally disconnected.

#### **A pauper's grave**

Acapulco police burst into Frank's bedroom on August 3, 1995. Besides a rotting body slumped in a chair, they found Frank's video equipment, OSM business records, child pornography tapes, a passport and a suicide note.

Servants identified the body as Frank's based on the gold Rolex watch on its wrist and other clothing, and the American

Consulate identified him based on documents found at the scene, including a passport and birth certificate. By the time Agent Lennon and Mexican federal authorities arrived, the medical examiner had ruled the death a suicide, and the body was placed in a pauper's grave.

But Mexican officials carried the



*A Postal Inspector makes a controlled delivery of child pornography videotapes to an Island Male customer.*

case as an open homicide. The body was placed face down in the grave, following local superstition that it would induce the murderer to return to the site.

Ed Lennon, however, believed that Frank had committed suicide. He was also fairly certain the body was Frank's, as there weren't many Anglo bodies to be found in Acapulco. Trial Attorney Georgiann Ceresse at the Department of Justice's Child Exploitation and Obscenity Section and Assistant U.S. Attorney Barbara Major in San Diego wanted to indict Frank. We just didn't know for sure if the body found at the Acapulco villa was truly his.

#### **The sting continues**

On September 6, 1995, Postal Inspectors conducted the first five

controlled deliveries of child pornography videotapes to Island Male customers.

One of our first arrests was Robert LaFond, a San Diego businessman who greeted us at his front door with a loaded semi-automatic pistol after accepting an Island Male package from Postal Inspector Yvonne Gurrero. We

secured LaFond and his residence and then found his stash of child pornography. LaFond told us he had cultivated a sexual interest in children for over 20 years and admitted he had purchased child pornography through the mail, but he claimed he never hurt a child.

I spoke with AUSA Barb Major on my cellular phone during the search. After uncovering Polaroids of a young boy in a sexual act, I told her I

had more questions for LaFond and I'd call her back. When confronted with the photos, LaFond admitted he had molested the boy, who lived in the neighborhood, as well as others. AUSA Major said, "Bring him in."

We dropped off LaFond at the Metropolitan Correctional Center and called San Diego Police Child Abuse detectives; they located and interviewed a young victim that day. LaFond was convicted of child molestation. He'll have to wait to go to state prison until he finishes up his time in the federal penitentiary for receiving child pornography through the mail.

### Is he or isn't he?

Inspector Pat Carr of the Denver Division was also briefed on the investigation, and he interviewed Frank's mother, who broke the news of his death to her other son, Keith. Keith was troubled when he heard about the medical examiner's report.

Troy Frank was found dead wearing a pair of shorts, and he had used his right hand to shoot himself. But Troy was left-handed, said Keith, and he absolutely never wore shorts; it could be 100 degrees in the shade and Troy would wear slacks and a shirt. Keith also told Inspector Carr that Troy's business partner bore a striking resemblance to his brother. Recent photos and a family video, both taken in Mexico, confirmed Keith's statements.

I decided to run the case by my old mentor, Detective J.B. Eoyd of the San Diego Police Department's homicide team. What he and fellow homicide detectives told me wasn't reassuring. Two extra bullet holes were found in Frank's bedroom, besides the one which had killed him. One of the bullet holes could be written off as a ricochet, but the other one?

"Test shots" were not unheard of, but were uncommon in suicides, said Boyd. He postulated that an inexperienced medical examiner could misdiagnose a contact wound as being an exit wound; exit wounds are usually larger than entry wounds due to muzzle blast. The detectives had other questions which made me uneasy.

Trial Attorney Georgiann Cerese and AUSA Barb Major were itching to indict Frank — if he was still alive. We realized we'd have to confirm the identity of the body now buried, face down, in an Acapulco grave.

### A steady stream of orders

More bad news came in early fall 1995 from Inspector Tom Kochman of the Philadelphia Division: Project Special Delivery had been "outed" in the *North American Man Boy Love Association (NAMBLA) Bulletin*. NAMBLA advocates consensual sexual relations between adults and children. The group had printed an altered version of one of our Island Male letters, along with an inaccurate and damaging article.

November brought better news. We received over 50 new orders from Island Male customers and even more repeat business, despite the NAMBLA article and the continuing arrests and indictments of Special Delivery subjects. AUSA Major indicted Kemmish on additional charges related to using the mail to distribute child pornography. Postal Inspectors across the country were working significant cases from the operation.

Inspector Karen Cassatt's suspect, Ray Opfer, was a prime example.

Opfer ordered tapes from Island Male. A background check revealed that Opfer, a scout leader, had a previous child molestation conviction hidden in his past and was on probation. Inspector Cassatt traveled to Reno, NV, to make a controlled delivery to Opfer with Inspector Kerry Fisher of the Phoenix Division.

Ray Opfer had a large collection of child pornography. Photographs found during the search revealed he was molesting young neighborhood boys. Opfer pleaded guilty to crimes related to child sexual abuse. After an emotionally charged hearing in which the victim's mother was allowed to speak on the witness stand, the judge sentenced Opfer to three consecutive terms of life imprisonment.

In January 1996, days before his

*Troy Frank's grave site just before the exhumation, Acapulco, Mexico.*



trial, Schwartz agreed to the government's final offer. Schwartz pleaded guilty to all charges, accepting even the prospect of an upward departure from the sentencing guidelines.

### Getting the green light

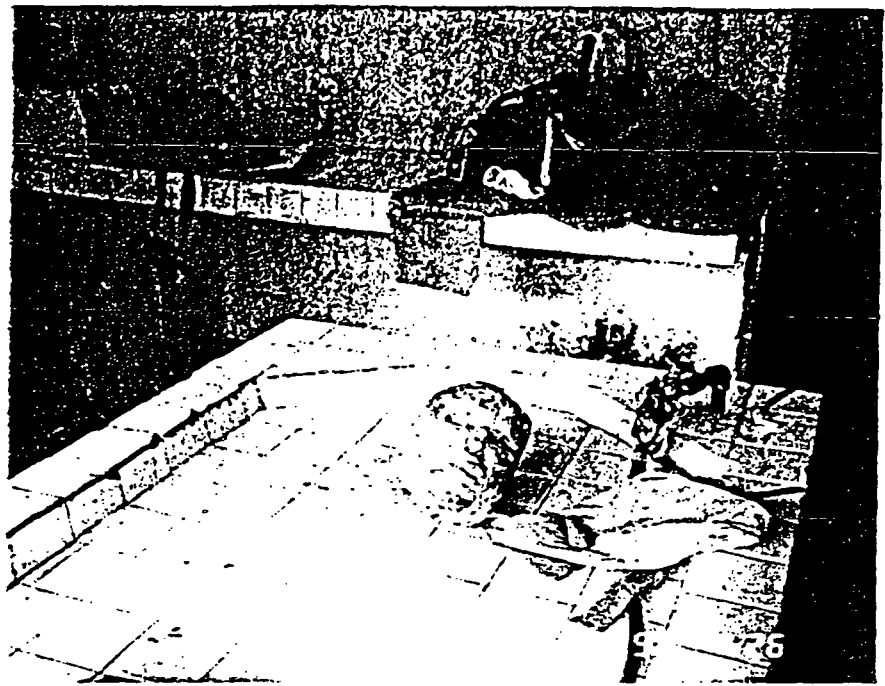
Meanwhile, the "Frank mystery" remained open. My job was to work with the Mexican authorities and the U.S. Embassy in Mexico City to coordinate an exhumation of the body found in Acapulco. When Frank gave us permission to have his brother's remains exhumed and identified, Inspector Carr tracked down Frank's dental X-rays, as we didn't expect to find the body in good condition after months underground.

Postal Inspector Ron Higa of the Los Angeles Division obtained Frank's dental records for the exhumation and had them transferred to me. My team comprised Detective Miguel Penaicosa, from the homicide team at the San Diego Police Department, and Dr. Norman "Skip" Sperber, a world-renowned forensic specialist and a pioneer in forensic dentistry. Dr. Sperber developed a dental identification system for the state of California after the crash of a PSA jet in San Diego, a system now used nationally. Both Miguel and Skip had previously worked on homicide investigations in Mexico.

Just before leaving, Ed Lennon set me up with the fourth member of our team and his right-hand man, Senior Foreign Service National Investigator Mario Gonzales. Mario worked for the American Embassy in Mexico for over 20 years as a criminal investigator; he knew how to get things done in that country.

### The Mexican way

We were met at the airport in Acapulco by a delegation of prosecutors from the State Attorney



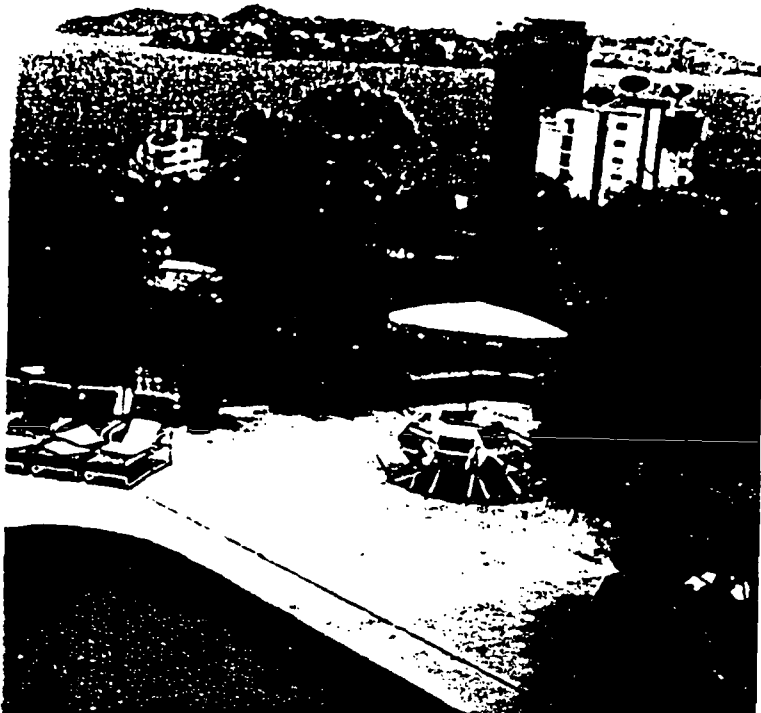
A Mexican doctor and dentist prepare Troy Frank's skull and teeth for further examination.

General's office, and traveled by motorcade to the main police station.

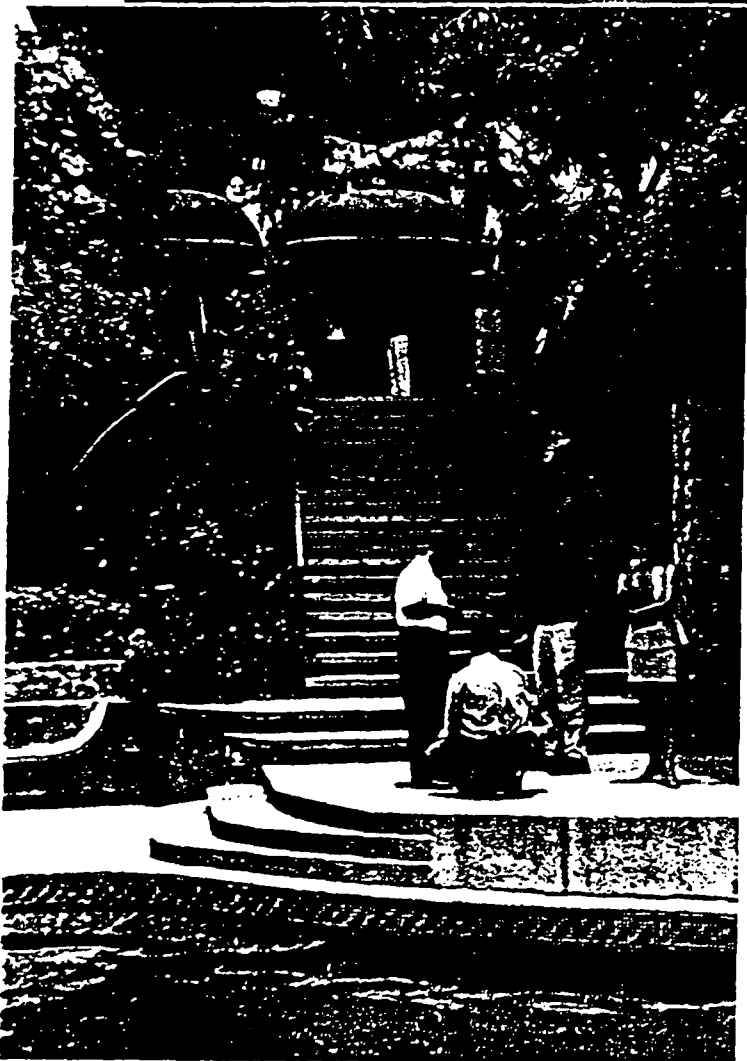
Prosecutors at the station trotted out voluminous evidence of a worldwide child pornography operation. Working late into the night, we pored over business records showing sales of over \$50,000 a month; customer lists,

with familiar names from the OSM investigation and Project Special Delivery; reams of false identification documents; and photographs of hundreds of young victims of child exploitation.

The next day, the prosecutors took my team to Troy Frank's magnificent villa overlooking Acapulco Bay. They guided us through the



*The view from the garden level of Frank's residence overlooking Acapulco Bay in Mexico.*



*Inspector Garn, Attorney Alexander Richards, and another prosecutor tour the villa in Acapulco where Troy Frank lived at the time of his death.*

multilevel mansion, from the four-car, iron-gated garage and pool with deck, to the video production room and bedroom on the fourth level. They pointed out the bullet holes and the fractured door frame of the bedroom, where in August 1995 detectives found the decomposed body, two weeks old, with a solid gold Rolex on its wrist. That night we worked with a team of doctors, dentists, prosecutors and even anthropologists preparing for the exhumation.

We exhumed the body just as the mercury passed the 90-degree mark, removing the head and right thumb at the grave site and returning to the medical examiner's office via our now-familiar motorcade. A ceiling fan whirred overhead, flies buzzed and the temperature climbed as a doctor and dentist removed remaining flesh from the skull in preparation for the X-rays. Some of the teeth had fallen out and were stuck back in place with a hot glue gun from the Acapulco Wal-Mart. Using his bare hands, the medical examiner rolled the lone thumb on index cards for prints.

Unfortunately, one of the front teeth, which had a unique filling, was missing. Dr. Sperber told me the tooth was probably lost during the first autopsy in August 1995. He said that Frank had a lot of dental work done since the X-rays taken during the 1980s, so he was unable to positively identify the body without an X-ray of the skull.

We moved on to the medical lab for new X-rays. By comparing the orientation of the teeth and other features of the jaw in the new X-rays to the older set from Colorado, Dr. Sperber positively identified the remains. The body that had been buried in a pauper's



*Inspector Phil Gam (left) presents Ramon Almonre-Borja, a prosecutor from the State Attorney General's office, with a Los Angeles Division cap and pin. Alexander Richards, a Mexican attorney, (right) translates.*

grave was indeed that of Troy Anthony Frank.

#### **The sanctity of the seal**

Orders for Island Male videos waited to be filled back in San Diego. Even after eight months and over 120 searches nationwide, customers were still eager for our product. We continued receiving orders the same week Chief Hunter held a press conference in Washington, DC, announcing the results and huge success of Project Special Delivery.

Island Male still hasn't quite closed its doors — quite a few cases await final resolution. As of August 1996, after 133 searches, 57 subjects have been prosecuted and many more are waiting in the wings as Inspectors waded through

mountains of evidence. Postal Inspector Steve Sadowitz of the Detroit Division claims he has reviewed more videos than Siskel and Ebert this year.

Child pornographers from all walks of life were identified through Project Special Delivery: four members of the clergy, six NAMBLA devotees, two Boy Scout leaders, one Big Brother, seven school teachers, a retired Army Lieutenant Colonel, several active and former police officers, an attorney, a history professor, a medical doctor, an electrical engineer, a computer programmer and a school counselor. Many were regarded as upstanding citizens in their communities— but they were secretly abusing children.

And there were other, unforeseen, benefits of our work. Robert H.

Ellison, another customer of Island Male investigated by Postal Inspector Bob Williams of the Chicago Division, was found to have sexually abused a number of young children in his neighborhood some 35 years earlier. Now adults, these victims came forward, encouraged by the media attention we generated, to tell Postal Inspectors about the man's terrible deeds. Ellison will be spending the next several years behind bars in federal prison and will be registered with the state of Illinois as a sex offender for the rest of his life.

As a result of outstanding work by Postal Inspectors across the nation, from new students like Inspector Rey Santiago at the Ft. Worth Division and Inspector Rhonda Bowie at the Phoenix Division, to "old hands" like Inspector John Dunn in Boston and Inspector Beryl Hedrick in Alabama, Project Special Delivery was a huge success.

We struck a major blow against those who believed they could use the U.S. Postal Service as an unwitting accomplice to sexually exploit and victimize our nation's children. To those who abused the "sanctity of the seal," we proved once again the value of our work: For over 200 years, Postal Inspectors have protected the mail and the citizens of this country, ensuring that confidence in the U.S. Mail is not undermined. ■



#### **ABOUT THE AUTHOR**

*Postal Inspector Phil Gam earned his B.A. in Psychology from the University of Virginia. He served as an officer in the Naval Reserve until 1990, and entered the Postal Service as a letter carrier in 1985, later supervising mail processing, delivery and finance operations. Inspector Gam was appointed as a Postal Inspector in 1990, and was assigned to the External Crimes Team of the former San Diego Division. Since 1994, he has worked in the areas of prohibited mailings-narcotics, internal crimes-narcotics and prohibited mailings-obscenity. Inspector Gam currently is assigned to the Los Angeles Division's Fraud and Prohibited Mailings Team based in San Diego. ■*

# USPS PROCEDURES

---

## MAIL COVER REQUESTS



**RESTRICTED INFORMATION**

**No portion of this document may be reproduced**

**Publication 55, July 1995**

Publication 55  
USPS Procedures: Mail Cover Requests [DATE]

### 1. EXPLANATION

This publication provides instructions to law enforcement agencies requesting a mail cover as part of a criminal investigation. All conditions and procedures contained in these instructions must be met before a mail cover can be authorized.

### 2. DISTRIBUTION

- a. Initial. Headquarters, Inspection Service Operation Support Group (ISOSG) Managers and Inspectors in Charge (INC) receive initial copies.
- b. Additional Copies. Only those receiving initial distribution may order extra copies from the Material Distribution Centers (MDCs) on Form 7380, MDC Supply Requisition. Only the Inspection Service may issue copies to law enforcement agencies on a case-by-case basis.

### 3. PROTECTION

Publication 55 is a "Restricted Use" publication. All persons in possession of this document must ensure that it is secured at all times. Its reproduction is prohibited.

### 4. COMMENTS

Address comments and questions to:

**COUNSEL  
OFFICE OF THE CHIEF INSPECTOR  
US POSTAL INSPECTION SERVICE  
WASHINGTON DC 20260-2181**

This publication is effective upon receipt.

Kenneth J. Hunter  
Chief Postal Inspector



**Exhibits:**

**1. Title 39, Code of Federal Regulations, Section 233.3 ..... 10**

**2. Inspection Service Operations Support Group Managers ..... 16**

**3. Sample Request (Letter/Memo) - Criminal Violation ..... 18**

**4. Sample Request (Letter/Memo) - Forfeiture ..... 21**

**5. Sample Request (Letter/Memo) - Fugitive ..... 24**

**6. Form 2009, Information Concerning Mail Matter ..... 27**

requester prior to the receipt of the written request

#### **D. Authority**

The United States Postal Inspection Service (Inspection Service) has sole regulatory authority to authorize mail covers. Title 39 of the Code of Federal Regulations, Section 233.3, authorizes and prescribes the manner in which mail covers are conducted (see Exhibit 1).

Requests are approved by the Chief Postal Inspector and, by delegation, to each of the five ISOSG Managers. In emergencies, local Inspectors in Charge may also approve cover requests.

### III. Preparation

#### **A. Mailing Instructions**

Request the mail cover on agency letterhead addressed to the ISOSG Manager, Attn.: Mail Cover Specialist, and send to the Inspection Service Operational Support Group (ISOSG) which has jurisdiction over the postal facility where the information will be recorded. A list of ISOSGs and the geographical area they cover is provided as Exhibit 2. Endorse the request and envelope RESTRICTED INFORMATION. Seal the request in the envelope, place it in a second envelope, and mail to the ISOSG.

#### **B. Mandatory Information**

There is certain information which must be furnished to determine if a mail cover can be approved. The items in this section are numbered to correspond to those shown in parentheses on the sample mail cover requests provided as Exhibits 3, 4 and 5. These sample requests identify the information required for a mail cover in a criminal case (Exhibit 3), a forfeiture case (Exhibit 4) and a fugitive case (Exhibit 5).

**1. Cover Justification.** State your purpose for requesting a mail cover and explain how the cover will provide evidence of a crime. A mail cover should not be used as merely a routine "investigative tool." Specify how information from the mail cover will assist the criminal investigation. Provide reasonable grounds that demonstrate the basis of the criminal investigation and the need to obtain this information from the mail. (For example, reasonable grounds might be based on information from a confidential informant, public complaint, previous investigation, etc.) Be specific and concise in outlining the reasonable grounds element.

#### **Reminders:**

- a. Mail covers are not authorized for exploratory purposes or for crimes punishable by less than one year imprisonment (misdemeanors).
- b. Requests referencing federal grand jury material covered by Rule 6(e) of Federal Rules of Criminal Procedure are returned without action.
- c. The request is a permanent part of the mail cover file and will be made available through proper disclosure procedures, including criminal or civil discovery actions.

**2. Subject Identity.** Identify each person or business to be covered by full name, address, and ZIP Code. If the request specifies "all other names at the subject address," it must justify the broader scope. Examples of such justification could include the known use of aliases by the subject, agency experience in similar cases which indicate that different names are normally used, or information that a spouse, family member, or roommate is involved in the suspected criminal activity.

In those cases where information is being sought in furtherance of a forfeiture, specify both the legal basis of the forfeiture (facts which describe the forfeiture investigation) and applicable statutes which authorize the forfeiture by the requesting agency (forfeiture statute and the agency's forfeiture authority).

If the subject is formally charged by indictment or information while the mail cover is in effect, notify the ISOSG Manager immediately to terminate the cover. Except in fugitive and forfeiture cases, mail covers are not continued if the person is indicted for the crime upon which the mail cover was requested. In these instances, a new mail cover request must be submitted which states as its basis the identification of assets for forfeiture purposes or the location of the suspect as a fugitive.

**6. Legal Representation.** Give the name and address of the subject's attorney or state if the attorney is unknown to you. If the purpose of the cover is to locate a fugitive, identify known legal counsel for both the subject of the cover and the fugitive. Mail covers exclude any mail between subjects and their attorneys.

**7. Daily Documentation.** Cover information is documented daily on Forms 2009 and sent to you at the end of the authorized time frame. If you need these forms during the course of the cover period, specify in your request that the forms are to be submitted on a weekly basis. Return all Forms 2009 to the ISOSG Manager within 60 days of the mail cover termination date (see Exhibit 6).

**Reminders:**

- a. All Forms 2009 are USPS property.
- b. Reproduction of forms is prohibited.
- c. Use of forms as evidence, or reference to mail covers in criminal, civil or administrative proceedings, should be avoided to the extent possible.
- d. Requesting official must ensure security of forms and their return.

**8. Special Instructions.** Note any additional circumstances relevant to your investigation, such as particular mail the subject receives or name of the local Postal Inspector if liaison has been established.

**C. Signature Block**

Provide your name, title, department, and commercial phone number. Sign above typed name.

- (4) **"Unsealed mail"** is mail on which appropriate postage for sealed mail has not been paid and which under postal laws or regulations is not included within a class of mail maintained by the Postal Service for the transmission of mail sealed against inspection. Unsealed mail includes second-, third-, and fourth-class mail, and international parcel post mail.
- (5) **"Fugitive"** is any person who has fled from the United States or any State, the District of Columbia, territory or possession of the United States, to avoid prosecution for a crime, to avoid punishment for a crime, or to avoid giving testimony in a criminal proceeding.
- (6) **"Crime"**, for the purposes of this section, is any commission of an act or the attempted commission of an act that is punishable by law by imprisonment for a term exceeding one year.
- (7) **"Postal statute"** refers to a statute describing criminal activity, regardless of the term of imprisonment, for which the Postal Service has investigative authority, or which is directed against the Postal Service, its operations, programs, or revenues. —
- (8) **"Law enforcement agency"** is any authority of the Federal Government or any authority of a State or local government, one of whose functions is to: (i) Investigate the commission or attempted commission of acts constituting a crime, or (ii) Protect the national security.
- (9) **"Protection of the national security"** means to protect the United States from any of the following actual or potential threats to its security by a foreign power or its agents: (i) An attack or other grave, hostile act; (ii) Sabotage, or international terrorism; or (iii) Clandestine intelligence activities, including commercial espionage.
- (10) **"Emergency situation"** refers to circumstances which require the immediate release of information to prevent the loss of evidence or in which there is a potential for immediate physical harm to persons or property.

(f) (1) **Exceptions.** A postal inspector, or a postal employee acting at the direction of a postal inspector, may record the information appearing on the envelope or outer wrapping, of mail without obtaining a mail cover order, only under the circumstances in paragraph (f)(2) of this section.

(2) The mail must be: (i) Undelivered mail found abandoned or in the possession of a person reasonably believed to have stolen or embezzled such mail; (ii) Damaged or rifled, undelivered mail, or (iii) An immediate threat to persons or property.

(g) **Limitations.**

(1) No person in the Postal Service, except those employed for that purpose in dead-mail offices, may open, or inspect the contents of, or permit the opening or inspection of sealed mail without a federal search warrant, even though it may contain criminal or otherwise Non-mailable matter, or furnish evidence of the commission of a crime, or the violation of a postal statute.

(2) No employee of the Postal Service shall open or inspect the contents of any unsealed mail; except for the purpose of determining: (i) Payment of proper postage, or (ii) Mailability.

(3) No mail cover shall include matter mailed between the mail cover subject and the subject's known attorney.

(4) No officer or employee of the Postal Service other than the Chief Postal Inspector, Manager, Inspection Service Operations Support Group, and their designees, are authorized to order mail covers. Under no circumstances may a postmaster or postal employee furnish information as defined in Title 39, Code of Federal Regulations, Section 233.3(c)(1) to any person, except as authorized by a mail cover order issued by the Chief Postal Inspector or designee, or as directed by a postal inspector under the circumstances described in Title 39, Code of Federal Regulations, Section 233.3(f).

(5) Except for mail covers ordered upon fugitives or subjects engaged, or suspected to be engaged, in any activity against the national security, no mail cover order shall remain in effect for more than 30 days, unless adequate justification is provided by the requesting authority. At the expiration of the

(4) The retention period for files and records pertaining to mail covers shall be 8 years.

(i) **Reporting to requesting authority.** Once a mail cover has been duly ordered, authorization may be delegated to any employee in the Postal Inspection Service to transmit mail cover reports directly to the requesting authority.

(j) **Review.**

(1) The Chief Postal Inspector, or his designee at Inspection Service Headquarters shall periodically review mail cover orders issued by the Manager, Inspection Service Operations Support Group or their designees to ensure compliance with these regulations and procedures.

(2) The Chief Postal Inspector shall select and appoint a designee to conduct a periodic review of national security mail cover orders.

(3) The Chief Postal Inspector's determination in all matters concerning mail covers shall be final and conclusive and not subject to further administrative review.

(k) **Military postal system.** Title 39, Code of Federal Regulations, Section 233.3 does not apply to the military postal system overseas or to persons performing military postal duties overseas. Information about regulations prescribed by the Department of Defense for the military postal system overseas may be obtained from the Department of Defense.

**Memphis ISOSG:** INSPECTION SERVICE OPERATIONS SUPPORT GROUP

225 N. Humphreys Blvd., 4th Floor South

Memphis TN 38161-0009

**Jurisdiction:** AL, AR, FL, GA, LA, MS, OK, TN, TX

---

**San Bruno ISOSG:** INSPECTION SERVICE OPERATIONS SUPPORT GROUP

PO Box 9000

South San Francisco CA 94083-9000

AK, AZ, CA, HI, ID, MT, NV, NM, OR, WA



**JOHN DOE (AND ALL OTHER NAMES)**

**1234 MAIN STREET**

**SAN FRANCISCO CA 12345-6789**

The subject of this request was convicted in 1988 and again in 1992 for drug trafficking, and our informant has personally made two buys from him.

All other names should be covered because recidivists often use aliases. Mail delivered to this address is intended for John Doe and, to our knowledge, no one else receives mail at the same address.

**(3-Mail Class)**

The mail cover should include information from both sealed and unsealed mail since past experience indicates that drugs are transported by both of these mail categories.

**(4-Time Frame)**

Cover is requested for 30 days, to begin as soon as possible.

**(5-Violation)**

Our investigation concerns a possible violation of 21 USC, 841(a), Possession of a Controlled Substance, punishable by up to 15 years in prison. Doe has not been indicted, but if he is formally charged during the 30 days requested, you will be promptly notified to terminate the mail cover.

**Exhibit 4. Sample Request - Forfeiture**

**Department of Treasury**

**Internal Revenue Service**

**[DATE]**

**ISOSG MANAGER**

**US POSTAL INSPECTION SERVICE**

**PO BOX 9000**

**SOUTH SAN FRANCISCO CA 94083-9000**

**ATTN: MAIL COVER SPECIALIST**

**Restricted Information**

**(1-Justification)**

This is a request for a mail cover to assist in the identification of property, proceeds or assets forfeitable under law. Our investigation has developed evidence that the subject J. Doe, 123 Main Street, San Francisco, CA 12345-6789 is engaged in money laundering.

**(2-Subject)**

The cover subject is:

J. Doe (AND ALL OTHER NAMES)

123 MAIN STREET

SAN FRANCISCO CA 12345-6789

**(8-Special Instructions)**

Information concerning accounts with banks or other financial institutions will be especially helpful.

(Provide complete name, address and phone number for case agent if different than requester.)

(Signature)

T. Smith, Director

Criminal Division

Internal Revenue Service

Phone: (000)123-1234

Cover request because it is believed that the fugitive may be communicating with his mother by mail. A mail cover is necessary to attempt to locate the fugitive.

The cover subject is:

JANE DOE

123 BROADWAY

ANYTOWN, USA 12345-6789

**(3-Mail Class)**

The mail cover should include information from sealed mail.

**(4-Time Frame)**

Cover is requested for 30 days, to begin as soon as possible.

**(5-Violation)**

R. Doe was originally charged with distribution of narcotics. A warrant for R. Doe's arrest has been issued by the authority of Oregon Statute 3146 (A2), Penalty for failure to appear. This offense is a felony punishable by imprisonment for a term of 15 years or more. The subject, Jane Doe, has not been indicted, but if she is formally charged during the 30 days requested, you will be promptly notified to terminate the mail cover.

**(6-Attorney)**

It is unknown if the fugitive R. Doe or the subject Jane Doe are represented by counsel at this time. However, if this information becomes available, the name of the attorney will be relayed to you at once.

Exhibit 6. Form 2009

**Information Concerning Mail Matter**

▶ **RESTRICTED INFORMATION** ◀

|                                                                             |  |                                                                                      |                      |
|-----------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------|----------------------|
| U.S. POSTAL SERVICE<br>INFORMATION CONCERNING MAIL MATTER                   |  | YOUR FILE NO.<br>951249                                                              | FILE DATE<br>5/27/95 |
| TO (Name of Postal Inspector)<br>INSPECTION SERVICE OPERATION SUPPORT GROUP |  | FROM (Post Office)<br>MEMPHIS, TN                                                    | DATE<br>5/27/95      |
| ADDRESS (City, State and ZIP Code)<br>PO BOX 6667<br>MEMPHIS TN 38161-0011  |  | The delivery of mail was not delayed while obtaining this information.<br><br>POSTER |                      |

THE FOLLOWING INFORMATION IS FURNISHED IN COMPLIANCE WITH YOUR REQUEST

| ADDRESSEE | SENDER    | RETURN ADDRESS                                | PLACE AND DATE OF POSTMARK | METER NUMBER | CLASS OF MAIL |
|-----------|-----------|-----------------------------------------------|----------------------------|--------------|---------------|
| JOHN DOE  | JANE TREE | 123 N. FRONT ST.<br>MEMPHIS, TN<br>38166-1234 | 3RD STREET PO<br>5-9-95    | 7231154      | FIRST CLASS   |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |
|           |           |                                               |                            |              |               |

**RECEIVED**

MAIL THIS FORM IN TWO, OPAQUE ENVELOPES. DO NOT USE WINDOW ENVELOPES.  
THE INNER ENVELOPE MUST BE MARKED "RESTRICTED INFORMATION."

PS Form 2009  
June 1981

▶ **RESTRICTED INFORMATION** ◀



A Glossary of  
Internet and Internet  
Related Terms

NATIONAL  
CENTER FOR   
**MISSING &  
EXPLOITED**  
CHILDREN

**CYBER  
TIPLINE**

[www.missingkids.com/cybertip](http://www.missingkids.com/cybertip)  
**1-800-843-5678**

# **THE INTERNET**

---

The Internet is a communication network that is second in size only to the telephone network. Like the telephone network, it matters less to the end user how the technology works, and more how to use the technology. We usually approach the Internet with a goal in mind. That goal is to use the Internet to locate information. Thus the "researcher", often without giving the technology a second thought, uses the Internet to communicate with other computers to find desired information. On any given day there are roughly 40 million people using the Internet throughout the world.

The Internet traditionally encompasses several tools, some of which are electronic mail (e-mail), file transfer protocol (FTP), Gopher, Telnet and the World Wide Web (WWW). The advent of graphical web browsers has brought the World Wide Web to the forefront and pushed some of the other tools to the background. Exploring these Internet tools is much like checking under the hood of a car. You know the engine is there, but you don't necessarily need (or sometimes even want) to know how it works. In most instances, modern Internet technology makes knowledge of these tools unnecessary, but at the National Center for Missing and Exploited Children it is crucial that we grasp a sound understanding of the basics of this medium.

The quickest way to get on the Internet is to get an account on one of the commercial online services. Some of the major national commercial online services are Prodigy, CompuServe, America Online, Genie, Erols, Delphi and Microsoft. All of these services offer Internet e-mail, and several offer other Internet tools. Also, many offer free trial periods and home-access software. For about \$10-20 per month, you can ask questions and electronically look over peoples shoulders to learn about the Internet.

## **Revisions / February 9, 1998**

I have revised the Internet Glossary to include more relevant terms and have withdrew some words that were not needed. The previous version contained 123 terms, this glossary contains 288 terms. I have tried to shorten the definitions and have included a few tables to help explain a few of the terms. In addition I have included a new list of commonly used email and chat room symbols.

Again, it is important to understand that the Internet is constantly growing and thus the language that is associated with it will grow. These lists will continue to be reviewed and updated on a regular basis.

**Section 1**  
**Section 2**  
**Section 3**

**Quick Reference List**  
**Internet Glossary**  
**Chat Room and Email Acronyms and Symbols**



# INTERNET QUICK REFERENCE LIST

---

**Applet** A small Java program that can be embedded in an HTML page. Applets differ from full-fledged Java applications in that they are allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, etc.), and are prohibited from communicating with most other computers across a network. The current rule is that an applet can only make an Internet connection to the computer from which the applet was sent.

**Baud** In common usage the baud rate of a modem is how many bits it can send or receive per second. Technically, baud is the number of times per second that the carrier signal shifts value - for example a 1200 bit-per-second modem actually runs at 300 baud, but it moves 4 bits per baud ( $4 \times 300 = 1200$  bits per second).

**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 1 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.

**Cookie** The most common meaning of "Cookie" on the Internet refers to a piece of information sent by a Web Server to a Web Browser that the Browser software is expected to save and to send back to the Server whenever the browser makes additional requests from the Server. Depending on the type of Cookie used, and the Browser's settings, the Browser may accept or not accept the Cookie, and may save the Cookie for either a short time or a long time. Cookies might contain information such as login or registration information, online "shopping cart" information, user preferences, etc. When a Server receives a request from a Browser that includes a Cookie, the Server is able to use the information stored in the Cookie. For example, the Server might customize what is sent back to the user, or keep a log of particular user's requests. Cookies are usually set to expire after a predetermined amount of time and are usually saved in memory until the Browser software is closed down, at which time they may be saved to disk if their "expire time" has not been reached. Cookies do not read your hard drive and send your life story to the CIA, but they can be used to gather more information about a user than would be possible without them.

**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.

**Gopher** A widely successful method of making menus of material available over the Internet. Gopher is a Client and Server style program which requires that the user have a Gopher Client program. Although Gopher spread rapidly across the globe in only a couple of years, it has been largely supplanted by Hypertext, also known as WWW (World Wide Web). There are still thousands of Gopher Servers on the Internet and we can expect they will remain for a while.

**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 server; thus in order for a web browser to display a page that contains 3 graphics, 4 "hits" would occur at the server: 1 for the HTML page, and one for each of the 3 graphics. "hits" are often used as a very rough measure of load on a server, e.g. "Our server has been getting 300,000 hits per month." Because each "hit" can represent anything from a request for a tiny document (or even a request for a missing document) all the way to a request that requires some significant extra processing (such as a complex search request), the actual load on a machine from 1 hit is almost impossible to define.

**Home Page (or Homepage)** Several meanings. Originally, the web page that your browser is set to use when it starts up. The most common meaning refers to the main web page for a business, organization, person or simply the main page out of a collection of web pages.

e.g. "Check out so-and-so's new Home Page." Another sloppier use of the term refers to practically any web page as a "homepage," e.g. "The web site has 65 homepages and none of them are interesting."

**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.

**Hypergraphic:** A graphic image link to other documents containing more information on the same or a related topic. To retrieve the related document, click on the hypergraphic. Similar to an icon in the Mac world.

**Hypertext:** A text link to other documents containing more information on the same or a related topic. Hypertext links are identified as different coloured text with an underline. To retrieve the related document, or move to the related link, click on the hypertext.

**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.

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

**Java** Java is a network-oriented programming language invented by Sun Microsystems that is specifically designed for writing programs that can be safely downloaded to your computer through the Internet and immediately run without fear of viruses or other harm to your computer or files. Using small Java programs (called "Applets"), Web pages can include functions such as animations, calculators, and other fancy tricks. We can expect to see a huge variety of features added to the Web using Java, since you can write a Java program to do almost anything a regular computer program can do, and then include that Java program in a Web page.

**Listserv** The most common kind of maillist, 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 the WELL and then go to the GBN conference.

**Maillist** (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 World Wide Web.

**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

**Server** A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running, e.g. Our mail server is down today, that's why e-mail isn't getting out. A single server machine could have several different server software packages running on it, thus providing many different servers to clients on the network.

**Terminal** A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry. Usually you will use terminal software in a personal computer - the software pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

**URL (Uniform Resource Locator)** -- The standard way to give the address of any resource on the Internet that is part of the World Wide Web (WWW). A URL looks like this: <http://www.matisse.net/seminars.html> or <telnet://well.sf.ca.us> or <news:new.newusers.questions> etc. The most common way to use a URL is to enter into a WWW browser program, such as Netscape, or Lynx.

**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.

# INTERNET RELATED TERMS

---

## A

### **ac**

If a Domain Name includes the characters "ac" then the site is associated with an academic institution  
e.g www.collegename.ac

### **Access Provider**

A company which provides its customers a service whereby they can access the Internet. The user normally connects to the Access providers computer via a modem using a dial up connection.

### **Access Time**

A standard measure which indicates the level of performance of the Hard Disk. The measure is the actual time that it takes for a piece of Data to be located on the Hard Disk.

### **AI**

Artificial Intelligence.

### **Alias**

An alias is an alternate name used to refer to something or someone.

### **Animated GIF File**

A special type of GIF File. They give the impression of a video. A collection of GIFS, presented one after the other each picture slightly different from the previous. Same principle as a film.

### **Anonymous FTP**

The mechanism of actually connecting to a remote computer, as an anonymous user, normally to transfer files back to your own PC.

### **Anonymous FTP Site**

If an FTP site does not require the user to have their own specific User ID & password the site is called an Anonymous FTP Site. Basically they can be accessed by anybody.

### **Anorak**

A rather unkind reference to somebody whose life revolves around computers & computer technology.

These people are also stereotyped as being into trainspotting (the real thing not the movie). Someone who spends a lot of time putting together a Glossary of PC & Internet Terminology is not necessarily an Anorak.

## **ANSI**

American National Standards Institute. It is a US business group which sets the standards - it is a voluntary organisation. ANSI is frequently seen in 3 areas:-

- Programming Languages - FORTRAN, COBOL & C conform to ANSI
- SCSI
- ANSI.SYS Device Driver. Available in DOS - it enables the use of ANSI defined commands (using the escape key) to control the screen & the keyboard

## **Anti Virus Software**

A program which is written specifically to locate & remove harmful viruses from your PC. These programs constantly have to be updated to cater for new viruses as they become known.

## **Applet**

An applet is a very small program written in the Java programming Language which can only be used as part of a Web Page. The Browser you are using must be capable of running Java Applets. They are used to bring a Web page to Life.

## **Application Program**

A Program which has been created to perform a specific task which is useful to the user - unlike the operating system which is a program that controls the PC. Most people buy PC's so that they can run application programs. Examples include :-

- Wordprocessor
- Spreadsheet
- Home Finance Package
- Drawing Package

## **Archie**

A Program which enables you to find Files on the Internet which you can transfer to your own PC. Archie searches the internet & provides you with a list of all the locations of the type or name of file that you are looking for. You can then transfer the file that you require using FTP.

The name Archie is derived from the word Archive

## **Archive**

A backup copy of data designed to be kept long term - often for security or audit reasons. The verb for doing this is also archive.

## Artificial Intelligence

A computer science which involves making a computer imitate human intelligence - learning as it goes along.

## ASCII

American Standard Code for Information Interchange. It is a standard way of representing ordinary text as a stream of binary numbers. A code set of 128 characters. The first 32 characters are control codes & the remaining 96 are upper & lower case letters, numbers, punctuation marks & special characters.

## ASCII Text File

The most common File Format found on PC's. They are basically text files which contain no formatting information at all. They do not require special programs to access them

## AUTOEXEC.BAT

This is one of the two special Batch Files which Automatically Execute when the PC is started up - the other being CONFIG.SYS. This File is normally located in the Root Directory. An example AUTOEXEC.BAT is :-

```
@ECHO OFF
```

```
CLS
```

```
PROMPT $p$g
```

```
PATH=C:\DOS;C:\WINDOWS
```

```
SET TEMP=C:\DOS
```

"@ECHO OFF" stops DOS from displaying each command on screen rather than just its results. "CLS" clears the screen. "PROMPT \$p\$g" determines what appears before the flashing cursor, p specifies show the path and g specifies show the ">" sign. "PATH=C:\DOS;C:\WINDOWS" tells DOS where to look for a File if it can't find it in the Current Directory. If a version of the file happened to exist in more than one of the Directories in the Path the file in the first directory listed would be the one that was selected. "SET TEMP=C:\DOS" tells programs which directory to place any Temporary Files which may be produced.

*B*

## BABT Approval

Any Modem used in the UK must be approved by the British Approval Board for Telecommunications. A green circle means approval, a red triangle means it has not been approved.

## **Back Up**

A Back up is a duplicate copy of some data or a disk or some software that is made by the user as a safeguard against the loss of the original information. Should this happen then the information can be recovered by restoring or copying the information back from the backup.

## **Band Width**

The Band Width is basically the maximum speed at which data can be transmitted between computers in a network.

## **Basic**

Beginner's All-purpose Symbolic Instruction Code. A very popular programming language developed by John Kemeny and Thomas Kurtz at Dartmouth College in the 1960's. There have been a number of implementations of basic over the years including :-

- Tiny Basic
- Microsoft Basic
- CBasic
- Integer Basic
- Applesoft Basic
- GW Basic
- Turbo Basic
- Microsoft QuickBasic

Historically, basic has been the programming language with which most people have got their first experience of programming.

## **Batch File**

A Batch File is a set of DOS commands contained within a single Text File. If this text File has a File Suffix of .BAT then by entering the File name at the DOS Prompt, the DOS commands will be executed one after the other. AUTOEXEC.BAT is an example of a Batch File.

## **Baud**

In common usage the baud rate of a modem is how many bits it can send or receive per second. Technically, baud is the number of times per second that the carrier signal shifts value - for example a 1200 bit-per-second modem actually runs at 300 baud, but it moves 4 bits per baud ( $4 \times 300 = 1200$  bits per second).

## **BBS**

Bulletin Board System - a computer which allows the people who subscribe to it to :-

- Copy files to it from their own PC's
- Copy files from it to their own PC's
- Send messages to other users of the Bulletin board
- Play multi-player games.

BBS's are still around in abundance but have generally been superseded by the Internet

## Beta Version

Beta Version refers to a version of an Application Program which is available for use but is not the definitive version that the company who developed the product will be releasing as the final product - it carries a warning that it is not 100% reliable - the idea of this is to iron out any unidentified problems before releasing it to the whole world.

## Binary

The Base 2 numbering system which has a very high use in PC technology. 10 in Binary is equivalent to 2 in decimal.

## BIOS

The PC's Basic Input/Output System stores a set of instructions which tells your PC how to handle input from the keyboard or the mouse & output to the printer or monitor.

## Bay

An opening at the front of the PC's Case which is designed to hold a data storage device such as a hard disk or a CDROM

## Bit

A bit is the smallest unit of information understood by a computer. A bit can take a value of 0 or 1. A byte is made up of 8 bits which is large enough to contain a single character. For example the character 2 would be equivalent to "00000010" when represented in bits. A Kilobyte is equivalent to 1024 bytes. A Megabyte is equivalent to 1024 Kilobytes. A Gigabyte is equivalent to 1024 Megabytes.

A Megabit is 1048576 bits.

| Bit           | Byte          | Kilobyte  | Megabyte | Gigabyte |
|---------------|---------------|-----------|----------|----------|
| 8             | 1             | -         | -        | -        |
| 8,192         | 1,024         | 1         | -        | -        |
| 8,388,608     | 1,048,576     | 1,024     | 1        | -        |
| 8,589,934,592 | 1,073,741,824 | 1,048,576 | 1,024    | 1        |



## 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

An application program which interprets HTML & presents the final Web Page. Used to "Surf the WWW". Examples include:-

- Internet Explorer
- Netscape Navigator
- Mosaic

## Bus

Data is transmitted to & from the different components of a PC via a bus. Different types of BUS are :-

- CPU/Memory bus
- I/O Bus
- Local Bus

The CPU/Memory bus runs at the same speed as the Processor but the I/O Bus runs at about 8MHz.

## Bus Clock Speed

The speed in Megahertz at which the I/O bus runs.

## Byte

A Byte is a unit of measure for Data Storage. 1 Byte is equivalent to 8 Bits.

| Bit           | Byte          | Kilobyte  | Megabyte | Gigabyte |
|---------------|---------------|-----------|----------|----------|
| 8             | 1             | -         | -        | -        |
| 8,192         | 1,024         | 1         | -        | -        |
| 8,388,608     | 1,048,576     | 1,024     | 1        | -        |
| 8,589,934,592 | 1,073,741,824 | 1,048,576 | 1,024    | 1        |

*C*

## Cache

A Cache Memory is a small but very fast memory used to store frequently used Data or instructions. It

tries to "guess" what data is going to be needed next by the Processor. The Cache can be:-

- Level 1 (Primary) Cache - part of the processor itself - fast & expensive
- Level 2 (Secondary) Cache - Mounted on the Motherboard slower than Level 1

## **CCITT**

Consultative Committee on International Telegraphy and Telephony is an international committee based in Geneva that sets standards for the whole world on Telecommunications

## **CD ROM**

A CD ROM (Compact Disk - Read only Media) can contain vast amounts of information (over 600Mb) which is accessible via a PC providing it contains a CD ROM Drive. As the name suggests you can only read information from a CD ROM.

## **CD ROM Drive**

A CD ROM Drive is required to enable the PC to read CD ROM's. The power of the CD ROM Drive is determined by its speed. Available on the market nowadays are:-

- Two Speed
- Four Speed (Quad)
- Six Speed
- Eight Speed
- Ten Speed
- Twelve Speed
- Sixteen Speed
- Twenty Speed
- Twenty Four Speed

## **Central Processing Unit**

Refers to the Microprocessor & the Memory of the PC.

## **CGA**

Colour Graphics Adapter Video Apapter introduced by IBM in 1981. A CGA Monitor can display 640 X 200 pixels using 2 different colours or 320 X 200 pixels using 4 colours.

## **CGI**

Common Gateway Interface Scripts are used by Internet Programmers to perform basic functions such as counting the number of times a Web Page is accessed

## **Client Server**

Client/Server distributes the processing of a Computer Application between 2 computers the Client & the Server - the principle being to exploit the power of each. The Client is normally a PC. The

Application Program will access Data & perform processing on the Server & using the data obtained via the server more processing tasks will be performed on the Client. The Application can be used by more than one user.

### **Clock Speed**

The speed at which the PC works measured in Megahertz

### **CMOS**

CMOS stands for Complimentary Metal-Oxide Semiconductor. It is a special RAM Chip which stores vital settings about your PC - such as the size of the Hard Disk & the amount & type of Memory. This information is stored even when the PC is switched off.

### **Command Interpreter**

The command interpreter is a DOS program which executes commands entered at the DOS prompt.

### **Com Port**

1 of up to 4 serial ports on your PC - normally used for a mouse or a modem

### **Compression**

A technique used to considerably reduce the size of a file without loosing any of the original information. The compression process alters the content of the file but this can & is completely recovered by reversing the process.

### **CONFIG.SYS**

This is one of the two special Batch Files which Automatically Execute when the PC is started up - the other being AUTOEXEC.BAT. This File serves the purpose of giving you the opportunity to Configure your System to you own requirements. Commands in your CONFIG.SYS commonly set up your PC to work with other Peripherals such as a CD ROM Drive. This file is normally located in the Root Directory. An example CONFIG.SYS is :-

```
DEVICE=C:\DOS\SETVER.EXE
```

```
DEVICE=C:\DOS\HIMEM.EXE
```

```
DEVICE=HIGH
```

```
FILES=30
```

```
SHELL=C:\DOS\COMMAND.COM C:\DOS/P
```

"DEVICE=C:\DOS\SETVER.EXE" fools Software into thinking it is running under an older version of DOS (i.e. upgrading to a new version of DOS does not mean that your old programs can no longer be used - good in theory but does not always work in practice. "DEVICE=C:\DOS\HIMEM.EXE" loads the Extended Memory Manager. "DEVICE=HIGH" saves Conventional Memory by loading Parts of DOS into the High

Memory area above 1Mb. "FILES=30" is the number of Files that can be open at any one time.  
"SHELL=C:\DOS\COMMAND.COM C:\DOS/P" points to the Command Interpreter. The /P telling it to stay permanently in Memory

### **Controller**

A circuit board which links the Hard Disk & the Motherboard. When access to information on the hard disk is requested by the Operating System, the controller tells the Hard Disk to get to work. With IDE Hard Disks, the controller is built into the Hard Disk itself.

### **Conventional Memory**

The first 640 Kilobytes of Memory. All DOS programs run in Conventional Memory.

### **Cookie**

A file that is written to your Hard Disk when you access certain Web Pages. The file contains certain information, often information that you entered when you displayed the page. The next time you access this page a check is done to see if the Cookie exists. The information within the cookie may well influence what happens next.

### **CPU**

Central Processing Unit.

### **CPU/Memory Bus**

The CPU/Memory bus, also referred to as the System Bus, transmits data between the CPU, Cache & RAM. The CPU/Memory Bus runs at the same speed as the Processor.

### **Current Directory**

The current directory is the DOS Directory at which the user is currently positioned. The current directory can be changed using the "CD" command. For more information type "help" at the DOS prompt

### **Cursor**

A flashing rectangle or line on the screen which shows exactly where the user is working. For example, when using a Word Processor the cursor indicates the point at which the characters being typed by the user will be inserted.

### **Cyberpunk**

Cyberpunk was originally a cultural sub-genre of science fiction taking place in a not-so-distant, dystopian, overindustrialized society. The term grew out of the work of William Gibson and Bruce Sterling and has evolved into a cultural label encompassing many different kinds of human, machine, and punk attitudes. It includes clothing and lifestyle choices as well.

## **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.



## **Daisy Chain**

A Daisy Chain, is when a number of PC's and or Peripherals are connected to each other in a series. When devices are daisy-chained to a PC, the first device is connected to the PC, the second device is connected to the first etc.

## **Data**

The content of a File, e.g. the information contained within a Spreadsheet, the contents of the Records on a Database

## **Database**

A collection of Data organised & designed for easy access. A collection of customer names & addresses may form the content of a database.

## **Databits**

When you send an Email to a friend or colleague the information will be sent (probably using a modem) across a network. As well as sending the content of the Email, information telling the system where it has come from, where it is going to, how much data should be sent e.t.c will also be sent as part of the transmission. Databits refers to the bits of information in this transmission which contain the content of the Email message.

## **Data Transfer Rate**

The speed at which data can be read from the hard disk & delivered to the processor

## **DDE**

**Dynamic Data Exchange.** When 2 or more programs that support DDE are running simultaneously, they can exchange information and commands. For example, a spreadsheet with a DDE link to a communications program might be capable of keeping stock prices that are displayed in the spreadsheet current with trading information received over the communications channel.

## **Default Value**

A number of programs will require the user to provide information. In some cases if the user chooses not to enter a value a "default value" will be taken. If for instance you have a Database in which you record the names & addresses of all your customers & nearly all of them are based in the UK you can set the database up such that if a country is not entered then it will be defaulted to the UK.

## **DES**

**Data Encryption Standard.** A commonly used standard method used for Encrypting & Decrypting Data. Encryption is necessary as valuable & sensitive information is often sent from one computer to another via a network which technically can be accessed by anybody. It provides a degree of security should the information fall into the wrong hands. DES was developed by the U.S National Institute of Standards & Technology.

## **Desk Top Publishing**

Using your PC to produce professional publications which can be used to market your products or present useful information to your customers. Software packages which are specifically designed for this purpose include :-

- Microsoft Publisher
- Corel print House

## **Device Driver**

Software that allows the PC to talk to hardware devices such as the printer & the Mouse. If you buy a new Printer it will come complete with a Disk containing the necessary Device Drivers.

## **Dialog Box**

A box displayed on your PC screen by a program including a message normally indicating that something is about to happen or has just happened. The dialog box requires the user to respond to the message before continuing with what it is about to do - normally the response is in the form of a Yes or No & based on the answer the program will carry out the next step or stop what it is doing. An example of this could be within an Email program - you read a message that has been sent to you & you decide to delete the message. After clicking on the delete button a dialog box containing the message "Are you sure you want to remove this message from your PC ? Yes or No" may be displayed.

## **Dial Up Connection**

A temporary connection between two computers via a telephone line normally using a modem - the most common method used to access the internet

A to Z index

---

## **Digital camera**

A digital Camera is basically a camera which produces photographs which can be saved as files on your PC. These cameras do not require a film to be processed. This is an ideal way to get a picture of anything that you need to include in a web page. The alternative is to take an ordinary photograph & use a scanner to scan the image into a file on your PC.

## Digital Video Disk

New Disk Technology. Digital Video Disks can hold over 4 Gigabytes of information - these are predicted to eventually supercede CD's.

## DIMMs

Dual In-line Memory Modules. Memory chips which are soldered onto plugs which slot into sockets on the Motherboard of the PC - makes fitting memory much easier than it use to be.

They have 168 pins in two rows. See SIMMs

## Directory

A directory is catalog for files stored on the Hard disk of a PC; a mechanism to group the files so that the user is not overwhelmed by a one huge long list of all the files stored on the hard disk. All the filenames belonging to a particular project, for example, might be kept together in one directory. The topmost directory is called the root directory; the directories within a directory are called sub directories.

Example

```
C:\WINDOWS\SYSTEM
```

In this Example "C:\" is the Root Directory, "C:\WINDOWS" is referred to as the WINDOWS directory & "C:\WINDOWS\SYSTEM" is referred to as the SYSTEM directory. This directory is a subdirectory of "C:\WINDOWS".

Windows 95 refers to directories as Folders

## Diskette

Another name for a 3.5 inch Floppy Disk.

## DLL

Dynamic Link Library - A library of program subroutines which can be shared amongst several different Application Programs - a concept which is extensively used under Windows. Windows programmers do not have to re-invent the wheel each time they want to do something common such as undo the last command or highlight a line of text.

## DNS

The Domain Name System is how the Internet links together the thousands of Networks which it is comprised of. The DNS is utilised whenever you send an Email or access a particular Web Page. Each computer on the Internet has a one of more Domain Names such as "fredblogs.co.uk". The .co indicates a commercial organisation & the .uk indicates that the computer is in the United Kingdom. Standard conventions used in Domain Names include:-

- ac - Educational institution
- co - Commercial organisation

- com - Commercial organisation
- edu - Educational institution
- gov - Non military government organisations
- int - International Organisations
- mil - Military government organisations
- net - Networks
- org - non profit organisation

You will also see these codes in URL's such as "homepages.enterprise.net/jenko/Glossary/G.htm".

These DNS converts the Domain Names to a unique number known as an IP address (the IP stands for Internet Protocol). You will often see the IP address displayed by your Web Browser when you are connecting to a particular computer.

## **Domain Name**

The Domain Name is a unique name which represents each computer on the Internet. (Some machines do have more than one Domain Name. The DNS converts the Domain Name requested by an Internet User into an IP Address. The location of the machine with this IP address is known & the information being requested can then be found. "www.yahoo.com" is an example of a Domain Name. The "com" indicates that Yahoo is a commercial Organisation. Other codes include:-

- ac - Educational institution
- co - Commercial organisation
- com - Commercial organisation
- edu - Educational institution
- gov - Non military government organisations
- int - International Organisations
- mil - Military government organisations
- net - Networks
- org - non profit organisation

You will also see these codes in URL's such as "homepages.enterprise.net/jenko/Glossary/G.htm".

These Domain Names are converted to a unique number known as an IP address (the IP stands for Internet Protocol). You will often see the IP address displayed by your Web Browser when you are connecting to a particular computer.

## **DOS**

Disk Operating System. oversees such operations as disk input and output, video support, keyboard control, and many internal functions related to program execution and file maintenance.

## **Download**

To copy files from another computer to your own PC via a network or using a modem.

## **DPI**

Dots Per Inch - A measure of the quality of the output from a printer - the greater the number of DPI the better the printer.



## **DRAM**

Dynamic Random Access Memory. It is a type of RAM capable of speeds of about 40MHz. Superseded by EDO RAM.

## **DTP**

Acronym for Desk Top Publishing.

## **DVD**

Digital Video Disk, New Disk Technology. Digital Video Disks can hold over 4 Gigabytes of information - these are predicted to eventually supersede CD's.

## **DVDROM**

Digital Video Disk Read Only Media, Digital Video Disks which can only be read.



## **EDO RAM**

Extended Data Out Random Access Memory. It is a type of RAM capable of speeds of about 50MHz. It holds its last requested data in a cache after releasing it. Superseded by SDRAM.

## **edu**

If a Domain Name includes the characters "edu" then the site is associated with an academic institution e.g www.collegename.edu

## **EGA**

Enhanced Graphics Adapter Video Adapter introduced by IBM in 1984. A EGA Monitor can display 640 X 350 pixels using 16 different colours from a table of 64 colours.

## **EIDE**

Enhanced Integrated Drive Electronics - protocol which allows for faster data transfer rates & the connection of up to 4 hard disks to a PC - supersedes IDE.

## **Email**

ElectronicMail - a way of sending other people messages from your PC. Widely used facility on the Internet which basically sends addressed messages over a Network. The message normally gets there in a couple of minutes. Internet users refer to the conventional Mail system as "Snail Mail". Who says Anoraks don't have a sense of humour.

## **Encryption**

Encryption is the process of converting data into "unreadable code" so that prying eyes cannot understand the content. Encryption is necessary as valuable & sensitive information is often sent from one computer to another via a network which technically can be accessed by anybody. It provides a degree of security should the information fall into the wrong hands.

## **Ethernet**

Ethernet is a LAN which was developed by Xerox in 1976. The different Nodes on the Network are connected by Coaxial Cable. This cable can be thin (which can connect 2 Nodes up to a distance of about 1000 feet) or thick (which can connect 2 Nodes up to a distance of about 3300 feet). The Ethernet standard has a provision to transmit data at a rate of 10 megabits per second.

## **Expanded Memory**

Physical Memory above 1 Megabyte for PC's with an 8086 or 8088 microprocessor (or simulating these microprocessors). This memory can be accessed using an Expanded Memory Manager.

## **Expanded Memory Manager**

A program which allows DOS to utilise the Expanded Memory.

## **Expansion Card**

A printed circuit card such as a video card that plugs into an expansion slot and adds functionality to the PC.

## **Expansion Slot**

Compartments in a PC into which you can plug expansion cards such as a video or sound card & connect them to the system bus. Most PC's have from 3 to 8 expansion slots.

## **Extended Memory**

Physical Memory above 1 Megabyte for PC's with an 286 or above microprocessor (or simulating these microprocessors).

## **Extranet**

Very similar to an Intranet with the added feature that the information contained can be accessed externally by business partners.



## **FAQ**

Frequently Asksed Questions - a term used in magazines & by Software companies to provide users with answers to those questions that we all have to ask.

## **Fiber Optics**

A technology by which data is transmitted using light through glass fibre cable

## **Finger**

An Internet software tool for locating people on other Internet sites. Finger is also sometimes used to give access to non-personal information, but the most common use is to see if a person has an account at a particular Internet site. Many sites do not allow incoming Finger requests, but many do.

## **File**

Data is stored in the form of a file. Files can be program files - contain instructions which allow the PC to perform various tasks under the control of the user or data files which contain information only.

## **File Format**

Defines or categorises files based on the way that the data is stored & presented. Examples include :-

- ASCII Text
- TIFF
- GIF

The format of a file governs which programs can process the file for either update & or display purposes.

## **Firewall**

A combination of specialised hardware & software designed to keep unauthorised users from accessing information within a networked computer system.

## **Floating Point Calculation**

A mathematical method which the processor uses to perform calculations which need a very high degree of accuracy

## **Floppy Disk**

A magnetic disk which is used to store data. They come in 3.5 & 5.25 inch diameter variants. Floppy disks are often used to transfer files from one PC to another or to backup important files.

## **Flowchart**

A Flowchart is a diagram which is produced to show the steps in a particular process. The flowchart will show what are the inputs & outputs in each of the steps. Flowcharts are frequently used to show diagrammatically what processes certain computer programs perform.

## **FTP**

File Transmission Protocol - a standard for moving Files from one computer to another. Predominant use on the Internet. This master copy of this document resides on my (Steve Jenkins) home computer. When I make a change to it I use FTP to transfer the updated files to the computer of my Internet Service Provider. I can also use FTP on certain computers on the internet to transfer files to my home computer.

A computer on the Internet which specifically stores files for users to FTP to there own computers is called an FTP Site.

If the FTP site does not require the user to have your own specific User ID & password is called an Anonymous FTP Site.

## **Function**

A Function is similar to a subroutine in that it is part of a program which can be performed a number of times. The difference is that a function has input parameters & output parameters. For example I have developed a function which you pass in the date of your birthday - the function then calculates how many days there are until your next birthday & passes the result of this back to the program - I use this function in a Web Page which displays the number of days until the next birthdays of all the members of my family (except uncle Bert who likes to keep his birthday a secret).



## **General Protection Fault**

A Windows term - Each program running under windows is given its own exclusive area of memory which is protected from other applications & a general protection fault occurs if this exclusive memory is accessed by another program.

## **Gateway**

The technical meaning is a hardware or software set-up that translates between two dissimilar protocols, for example Prodigy has a gateway that translates between its internal, proprietary e-mail format and Internet e-mail format. Another, sloppier meaning of gateway is to describe any mechanism for providing access to another system, e.g. AOL might be called a gateway to the Internet.

## **GIF File**

The most common type of image file used on the Internet. These files are compressed so they take up the minimum amount of space & can therefore be downloaded a lot quicker than other graphics file.

GIF files are typically used for:-

- Backgrounds
- Displaying banners
- Advertisements
- Buttons

The files unlike other graphical file types are limited to 256 colours.

GIF Files are stored in a number of different formats such as:-

- 87a
- Interlaced 87a
- 89a
- Interlaced 89a

The interlaced versions are designed to allow the image to be gradually revealed as it is downloaded.

## **Gopher**

An application whose purpose is to locate, retrieve & record information from the Internet. Developed at the University of Minnesota in 1991.

## **Gopherspace**

The information that is available via the Gopher tool set.

## **Graphic**

A picture or non text item within a document. Most Web pages will contain a number of Graphics

## **GUI**

GUI stands for Graphical User Interface. A Graphical User Interface is designed so that the user can perform tasks by using a mouse to point & click on an icon. The user can perform any task with either the mouse or the keyboard.

GIF Files can also be:-



## **Hacker**

Somebody who deliberately Logs on to other computers by somehow bypassing the Log on security system - this is sometimes done to steal valuable information or to cause irreparable damage.

## **Hard Disk**

The Hard Disk is where the data is stored within the PC. Hard Disks have the capacity to contain several megabytes or even a few gigabytes of data.

## **Hardware**

The physical components of a PC including Peripherals.

## **Head**

The part of the harddisk mechanism which actually reads & writes data to the disk.

## **Hexadecimal**

The Base 16 numbering system which has a very high use in PC technology. The decimal numbers 10 to 15 are represented by the letters A to F. 10 in hexadecimal is equivalent to 16 in decimal.

## **High Memory Area**

The first 64 Kilobytes of Extended Memory.

## **Hit**

This occurs when a web page is accessed by a user or a program accesses the page. A hit was registered on this particular web page (the Letter "H" in the Glossary) when you requested to look at the information contained within it.

## **Home Page**

The page by which a user normally enters a web site. If you click on the "A to Z index" below you will display the Home Page of this Glossary Web Site.

## **Host Computer**

A Host Computer is one which provides a particular service to a user. This includes Information or communications.

## **Hot Java**

Hot Java is a Web Browser which can display "executable content" written in the Java Programming Language

## **HTML**

HyperText Markup Language - the text based language used to construct WWW pages. Interpreted by Web Browsers. This delightful masterpiece is a collection of HTML instructions which you can see using the View HTML Source option from your Browsers menu.

## **HTTP**

HyperText Transmission Protocol is a Protocol that Computers on the Internet use to communicate with each other.

## **Hypermedia**

Basically, Hypertext which also contains Multimedia components.

## **Hypertext**

Text which contains links which can be clicked with a mouse. When the user "clicks" the link they are taken to another document or a different section of the current document. This Glossary is a good example of Hypertext.

- Animated - gives the impression of a video. A collection of GIFS, each picture slightly different from the previous. Same principle as a film
- Transparent - Blends in with the background



## **IAB**

Internet Architecture Board - a group of people which makes decisions regarding Internet Standards. IETF & IRTF are subordinate to the IAB.

## **ICE**

Intelligence Concept Extraction - technique used by Search Engines to relate words to ideas, so if you do a search for "camping equipment" you may well find articles specifically about tents.

## **Icon**

An Icon is a small picture which is displayed on the screen. It is intended to depict pictorially a task. By clicking the icon with the mouse will invoke the task. It is an essential component of a Graphical User Interface.

Examples include:-

- A folder with a magnifying glass to depict Windows Explorer
- A book with a question mark to depict a help file
- A blue notepad to depict, believe it or not, Windows Notepad

## **IDE**

Integrated Drive Electronics. Most PC's contain IDE Hard Drives. They normally contain built in controllers.



## **IEEE**

Institute of Electrical & Electronic Engineers. This organization is responsible for many of the accepted communication standards

## **IETF**

Internet Engineering Task Force. A subgroup of volunteers of the IAB that concentrates on technical issues on the Internet. The tactical arm of the IAB.

## **Image Map**

A graphic which is divided into different areas each of which link to different web pages. An example of where this could be used is by an Australian company that has an office in each state capital. The Graphic would be a Map of Australia. If the user clicked on Melbourne the Victoria Web Page would be displayed but If the user clicked on Sydney the New South Wales Web Page would be displayed

## **Index**

An index is something which points at other information - a program will often use an index to locate a particular record on a file - same concept as an index in a book. Most Databases make use of indexes

## **Install**

To add hardware or load a software application onto your PC.

## **Instruction Set**

Basically the set of instructions which a particular Microprocessor can recognise such as add, subtract.

## **Integer**

As in mathematics, a whole number which does not contain any decimals

## **Internet**

The Internet is a world wide computer network through which you can send a letter, chat to people

electronically or search for information on almost any subject you care to think of. Quite simply it is a "network of computer networks". It originated in the 1960's in the USA where the US defence were conscious of having its computer network destroyed by blowing up the central computer. A network was designed around the principle of "unreliable computers" - if one was destroyed or failed the remaining computers could still function. Each computer in the network acknowledges the existence of all of the others.

## **InterNIC**

InterNIC is a group of people who control domain name registration. They also provide various services to all users of the internet.

## **Intranet**

An internal or Company Internet that can be used by anyone who is directly connected to the companies computer network

## **I/O**

Input Output deals with 2 out of 3 of the activities (input, processing, and output) performed by a PC. I/O are complimentary tasks of gathering data for the microprocessor to work with and making the results available to the user through a device such as the monitor or printer. The keyboard and the mouse are input devices that make information available to the computer; the display and printer are output devices with which the computer makes its results available to the user. The Hard Disk is both an input and an output device because it can either provide stored information or store the data after processing

## **I/O Bus**

Input Output Bus - used to transmit data from the Cache & the RAM to the PC disks.

## **I/O Port**

Input Output Port - part of the PC which is used for passing data in and out of a computing device. This is normally located on the back of the PC. The port can be a Serial Port - data is sent/received one bit at a time through a cable containing a single wire, or a Parallel port where the data is sent/received through a cable containing several pieces of wire so that more than one bit at a time can be processed

## **IP Address**

The Internet Protocol address is a unique number which is used to represent every single computer in a Network. All the computers on the internet have a unique IP address. The format of the IP Address is 4 numbers separated by dots e.g. 198.123.456.7.

## **IRC**

Internet Relay Chat is the CB Radio of the Internet. Basically you can "chat" to a number of people by typing simple messages at your keyboard & these are responded to by one or more other people from all over the world who happen to be "chatting" to you via IRC.

## **IRQ**

Interrupt Request. This forces the CPU to stop what it is doing so that it can carry out the task requested as part of the IRQ.

## **IRTF**

Internet Research Task Force. A sub group of the IAB that considers the strategic approach to issues with the Internet - creates long term solutions to new challenges which have to be addressed. The strategic arm of the IAB.

## **ISDN**

Integrated Services Digital Network is a fast digital phone line - can be provided by most phone companies. To be able to reap the benefits you will need to add a special card to your PC and your Internet Service Provider must be able to provide an ISDN connection.

## **ISOC**

The Internet SOCIety, worldwide standards organization - sponsor the IAB.

## **ISP**

Internet Service Provider or sometimes referred to as Internet Access Provider (IAP) is a company which provides access to the Internet for people like you & me. The company handles the link from your PC to the rest of the Internet. The ISP's central computer is linked to the rest of the internet so the person using this service only pays the telephone charges to connect from their home computer to the ISP's central computer

*J*

## **Java**

Java is a modern Programming Language , first seen in 1995 , & is used to bring Web Pages to life. Java programs are referred to as applets.

Java is an interpreted, object-orientated program language with a syntax & structure similar to C++,

designed specifically for the internet by Sun microsystems

One huge plus for Java is that Java programs can run on many different types of computer (e.g. IBM PC, Apple Macintosh).

Java Applets are always small in size & can be downloaded from the Internet & executed as part of the Web page being displayed.

Once a programmer has completed the Java program it is compiled to produce an executable module. This executable module has instructions written for the "Java virtual machine" - this is designed for the platform on which the module is to be executed. These instructions are interpreted on the platform where the program is being executed. The "Java Virtual Machines" are available for a number of operating environments e.g. Windows, AIX, OS/2.

## **JavaScript**

JavaScript is a Programming Language for developing Client Internet applications. The WEB Browser interprets JavaScript statements embedded in an HTML page. LiveWire is the Server based equivalent which enables you to create applications similar to Common Gateway Interface (CGI) programs.

## **Joystick**

A pointing device mostly used for playing computer games

## **JPEG**

JPEG is a type of image file used on the Internet. Like GIF files, JPEG files are compressed. Unlike GIF files JPEG files cannot be interlaced or transparent.



## **Kermit**

A program developed at Columbia University to transfer files between computers  
A to Z index

---

## **Keyboard**

The Keyboard is the main device that we use for entering data into a PC or giving it an instruction to do something specific. The key arrangements resemble that of a tradition typewriter plus lots more additional keys for specific functions.

A to Z index

---

## Kilobyte

A Kilobyte is a unit of measure for Data Storage. 1 Kilobyte is equivalent to 1024 Bytes or 8192 Bits.

| Bit           | Byte          | Kilobyte  | Megabyte | Gigabyte |
|---------------|---------------|-----------|----------|----------|
| 8             | 1             | -         | -        | -        |
| 8,192         | 1,024         | 1         | -        | -        |
| 8,388,608     | 1,048,576     | 1,024     | 1        | -        |
| 8,589,934,592 | 1,073,741,824 | 1,048,576 | 1,024    | 1        |

*L*

## LAN

A Local Area Network is a group of PC's, Other Computers & Peripheral Devices which are linked together where each device is located in close proximity to all the other devices. LANs typically consist of a number of PC's, shared printers & Shared Directories & Files.

## Laptop

A Laptop is a portable PC. The term Laptop has been superseded by Notebook. The original laptops were bulky & quite heavy.

## LCD

Liquid Crystal Display - a low power display - frequently used in Laptops

## LED

Light Emitting Diode - An electronic device which gives off light when an electric current is passed through it. Most indicator lights, such as the one which comes on when you switch on your PC use an LED.

## Level 1 Cache

Cache Memory which is part of the processor itself - fast & expensive.

## Level 2 Cache

Cache Memory which is mounted on the Motherboard - slower than Level 1 Cache.

## **Link**

A component of a hypertext document which when clicked with a mouse takes the user to another document or a different section of the current document. The word "mouse" above in this paragraph - which you can probably see in mauve or blue is an example of a link.

## **Listserv**

The most common kind of maillist, Listservs originated on BITNET but they are now common on the Internet.

## **Local Bus**

Local Bus introduced to circumvent the delay due to the vast difference in speeds between the CPU/Memory Bus & the I/O Bus.

## **Login**

This is the term for the process of actually gaining access to the resources on a particular computer - normally this is done by entering a userid & a password.

## **Log off**

The process of actually ending your access to a particular computer.

## **Log out**

The process of actually ending your access to a particular computer.

*M*

## **Mailbox**

The file or directory where your incoming email messages are stored on the computer of your Internet Service Provider.

## Maillist

(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.

## Megabyte

A Megabyte is a unit of measure for Data Storage. 1 Megabyte is equivalent to 1024 Kilobytes or 1,048,576 Bytes or 8,388,608 Bits.

| Bit           | Byte          | Kilobyte  | Megabyte | Gigabyte |
|---------------|---------------|-----------|----------|----------|
| 8             | 1             | -         | -        | -        |
| 8,192         | 1,024         | 1         | -        | -        |
| 8,388,608     | 1,048,576     | 1,024     | 1        | -        |
| 8,589,934,592 | 1,073,741,824 | 1,048,576 | 1,024    | 1        |

## Megahertz

The measure of how fast a Chip can work

## Memory

Chips which hold information which the PC needs to use. These chips are connected directly to the Microprocessor. There are two types of Memory Chip:-

- Random Access Memory (RAM)
- Read Only Media (ROM)

## Menu

A Menu is a list of options presented to the user to enable them to perform a specific task. Each option on the list will perform a different task.

## Microprocessor

The Microprocessor is built onto a single piece of silicon, known as a wafer or chip, Its size is about 0.5 cm along one side and no more 0.05 cm thick. It can be programmed to perform a great number of information-handling tasks. It can serve as a general-purpose computer for instructional or word-processing use, to control other machines or industrial processes such as making food products, and for hand-held calculators. Its advent was brought about by the progressive miniaturization of integrated circuits and by advances in semiconductor technology.

A microprocessor may function by itself in a wide range of applications, incorporating from as few as 1000 or as many as several hundred thousand elements on its single chip. It may also serve as the CPU of a PC, when it is combined with support chips containing computer memories and is equipped with

input-output devices. Microcomputers gained great importance in the 1970s and '80s with the growth of the PC.

A microprocessor chip typically contains a read-only memory (ROM)-that is, a memory that can be read repeatedly but cannot be changed-but it may also have some random-access memory (RAM) for holding transient data. Also present are a register for holding computing instructions, a register for holding the "address" of each instruction in turn, similar data registers, and a logic unit. It also has interfaces for connecting with external memories and other systems as needed.

Microprocessors are classified in terms of the number of "bits" of information that can be transferred in parallel and held in their registers. This number has been steadily increasing with the growth of circuit technology. Thus 4-bit, 8-bit, and 16-bit microprocessors are now common, and 32-bit chips have also been developed.

## **MIDI**

Musical Instrument Digital Interface. A standard for connecting computers & musical instruments.

## **MIME**

Multipurpose Internet Mail Extensions - a standard by which people can send each other Email messages which contain pictures, videos or sounds.

## **MMX**

Multi Media eXtensions - a technology which is featured in a number of the latest Processors designed mainly for Multi-Media applications. To benefit from MMX the application running must have been written to take advantage of MMX technology

## **Modem**

Modem comes from the 2 words Modulation & Demodulation. A Modem converts information from Analog to Digital & vice versa. Digital Information is represented in a series of 1's & 0's. Analog information varies continuously such as a sound wave. Typical when you send an Email, your Modem converts the digital Email message to analog.

## **Monitor**

The Monitor is used to display the images which are generated by a PC's Video Adapter.

## **Motherboard**

The main circuit board containing the vital components of a PC such as the processor & the RAM.



## **Mouse**

A Mouse is a common pointing device used to maximise the benefits of a Graphical User Interface. Generally a mouse has two buttons which action various tasks either by a single or a double click. Windows 95 has some features which are activated via a triple click. The mouse also has a pointer on the screen which is moved by moving the mouse up or down or from side to side.

## **MPEG**

Moving Picture Experts Group - a standard used on the World Wide Web for video & audio files - compression techniques are used which enable the files to be transmitted across the internet significantly quicker than other audio & video files. The web browser you are using must be capable of running MPEG files

## **Multimedia**

Multimedia is the presentation of video, sound, graphics, text & animation by Software.

## **Multitasking**

A Multitasking operating system is one which allows a PC to perform more than one task at a time. There are several types of multitasking. Different types include:-

- Context switching - Only the foreground applications utilises the processor
- Cooperative multitasking - Background tasks utilise the processor during idle times
- Time-slice multitasking - Each task utilises the processor's for a fraction of a second:

*N*

## **net**

Part of the Domain Name which indicates that the company is an organisation which provides a network service - usually an Internet Service Provider e.g. www.enterprise.net

## **Netscape**

A WWW Browser and the name of a company. The Netscape (trn) browser was originally based on the Mosaic program developed at the National Center for Supercomputing Applications (NCSA).

Netscape has grown in features rapidly and is widely recognized as the best and most popular web browser, Netscape corporation also produces web server software.

Netscape provided major improvements in speed and interface over other browsers, and has also engendered debate by creating new elements for the HTML language used by Web pages -- but the Netscape extensions to HTML are

not universally supported.

The main author of Netscape, Mark Andreessen, was hired away from the NCSA by Jim Clark, and they founded a company called Mosaic Communications and soon changed the name to Netscape Communications Corporation.

## **Network**

A network is basically a series of wires & cables which connect a number of computers. Data is exchanged between computers via these cables. The maximum speed at which the data can be transmitted is called the bandwidth.

## **Newbie**

A term used to describe somebody who is new to the internet.

## **News group**

News groups are one of the many facilities available on the Internet. Like most of the internet, News groups are run voluntarily & co-operatively by people like you & me. A News group is centred around a discussion topic an example being rec.sport.soccer. Within these News groups several discussions or Threads take place on themes within the discussion topic. A news group devoted to the great rock guitarists may have a thread on who is the best guitarist out of Clapton, Beck & Page for instance. If you are having a problem getting something specific to work in a spreadsheet there will definitely be a news group to which you can pose your problem & it won't take long to get many responses. Unfortunately news groups appear to be the vehicle for a majority of the more undesirable topics that pollute the internet. If you see a particular News group of interest you can "subscribe" to it. Once this has been done you "post" your article & eventually it can be seen by anyone else who subscribes to the particular news group.

The categories of News groups (represented by the first 3 or 4 characters of the name followed by a "." are) :-

- rec - recreational activities
- biz - business related groups
- comp - computers including technical discussion & support
- soc - social issues
- sci - scientific discussions
- uk - groups of interest to us English, Scottish, Irish & Welsh
- alt - Alternative groups

## **Node**

A node is any device such as a PC which is connected to a Network

## **Notebook**

A notebook is a PC which is about the same size as a sheet of A4 paper & about 5cm thick. The term Notebooks has superseded the term laptop which generally referred to a portable PC. The original laptops were bulky & quite heavy.



## **Octal**

The Base 8 numbering system which has a very high use in PC technology. 10 in Octal is equivalent to 8 in decimal.

## **OEM**

Original Equipment Manufacturer is the company which actually made the computer equipment - it is quite common for one company to make the equipment & another company to sell it.

## **Online**

To be connected to the Internet

## **Operating System**

The Software which is responsible for running the PC, control & utilisation of the hardware & Peripherals Examples include:-

- DOS
- UNIX
- WINDOWS 95

## **OS**

Operating System



## **Page Impression**

A Page Impression occurs every time a particular web page is displayed by someone using the Internet - similar to a Hit except that a Hit is also registered when a spider or similar program accesses the web page.

## **Password**

The password is a code known only by a user to ensure that the individual who is trying to Login to the computer is the actual person that the Userid being used belongs to.  
A

## **Path**

Any program which a user tries to execute in DOS without supplying a directory causes DOS to have to find the Directory in which the Program resides. First it tries the Current Directory, If unsuccessful it then goes through in order all the Directories specified in the PATH. The PATH is defined in AUTOEXEC.BAT

## **PC**

PC - The Personal Computer - what this Glossary is all about. Quite Simply a computer designed to be used by one person at a time.

## **Pentium**

The Pentium processor was introduced by Intel in 1993. PC's with this kind of processor are normally referred to as Pentiums. The speed of the Pentium Processor when it was introduced was 60MHz - this increased to 100MHz in 1994, 120MHz in 1995 & 160MHz in 1996. By Mid 1996 Processor speeds were in excess of 200MHz.

## **Pentium II**

The Pentium II processor was introduced by Intel in the middle of 1997. The speed of the Pentium II Processor when it was introduced was around 300MHz. The Pentium II is basically the Pentium Pro incorporating MMX technology.

## **Pentium Pro**

The Pentium Pro processor was introduced by Intel at the end of 1997. The speed of the Pentium Pro Processor when it was introduced was around 200MHz.

## **Peripheral**

A device which can be attached to a PC & is controlled by its Processor. Examples include:-

- Printer
- Modem
- Joystick

## **PERL**

Practical Extraction & Report Language originally developed by Larry Wall for his personal use. It is now one of the most popular Internet tools. Perl is most often met in the context of the World Wide Web where its basic function is in the manipulating of Files, text & producing Reports. The basic concepts of Hypertext Markup Language are greatly extended by being able to run ancillary programs achieved using the Common Gateway Interface (CGI). This allows programs to be called in response to actions by the Web Client user i.e. something done by use on your PC on a particular Web Page. Almost any Programming Language can be used with Perl being the Most popular. The Perl program sits in between the Web Server & other software such as Databases

## **PIM**

Personal Information Manager - Application programs designed to help you manage your day to day affairs - features included are:-

- Diary
- List of contacts
- Notes
- Reminders

## **Pixel**

Pixel stands for picture element.. It is the smallest element of information that programs can display or print. A picture or image is made up of thousands of pixels. A pixel is sometimes called a pel

## **Plug-in**

A (usually small) piece of software that adds features to a larger piece of software. Common examples are plug-ins for the Netscape(& browser and web server, Adobe Photoshop(& also uses plug-ins.

The idea behind plug-in's is that a small piece of software is loaded into memory by the larger program, adding a new feature, and that users need only install the few plug-ins that they need, out of a much larger pool of possibilities. Plug-ins are usually created by people other than the publishers of the

software the plug-in works with.

## **POP**

**Post Office Protocol** - standard for exchanging Email between a users PC & their Internet Access Provider.

## **Port**

A Port is part of the PC which is used for passing data in and out of a computing device. This is normally located on the back of the PC. The port can be a Serial Port - data is sent/received one bit at a time through a cable containing a single wire, or a Parallel port where the data is sent/received through a cable containing several pieces of wire so that more than one bit at a time can be processed. Also referred to as the I/O Port.

## **PPP**

**Point to Point Protocol** - Standard for using a modem & telephone line to connect to the Internet using TCP/IP.

## **Primary Cache**

Another term for Level 1 Cache.

## **Processor**

In the PC field the Processor & Microprocessor are synonymous. Basically it is the brain of the PC which carries out all of the low level "processing" that the PC needs to do - calculating the sum of 2 numbers is a simple example of something that the processor will do. Basically every single task that the PC performs is dependant on the processor doing its stuff.

## **Program**

A Program is basically a series of instructions that causes the PC to do something. The Operating System such as DOS is known as a Systems Program. Application Programs such as a Word Processor or Spreadsheet perform the main tasks for which we use the PC i.e. a letter to Mum or managing the finances.

## **Programming Language**

An artificial language through which a set of instructions can be performed by a PC. Examples are:-

- Basic
- C, C++
- Cobol
- Java
- JavaScript
- Perl
- Visual Basic

People who use programming languages to create a computer program are called programmers.

## *R*

### **RAM**

**Random Access Memory** is a temporary storage area which the processor uses to execute Programs & hold Data. Information is put into RAM & held there. Once the RAM becomes full information has to be removed to make space for the current task being performed. A PC with limited RAM will take a long time to perform the simplest task as the information in the RAM is constantly being replaced. RAM requires a constant electric supply to keep the information intact. Should you switch off the PC then you will lose the contents of RAM forever

Different areas of RAM include:-

- Conventional Memory
- Expanded Memory
- Extended Memory
- High Memory Area
- Upper Memory Area

Types of RAM include

- DRAM
- EDO RAM
- SDRAM

### **RAM Doubler**

Software designed to make your RAM go further by allowing you to open more programs or handle more data within a program.

### **Record**

Files are comprised of a number of records. Each record normally has a common set of characteristics. For example at a College a particular File may contain a record of all the students. Each record could contain Student ID, Date of Birth, Year enrolled etc.

## **ROM**

Read Only Media. ROM chips cannot be written to. Therefore they contain information which never changes. All PC's have ROM chips. When the PC is switched on the Information in the ROM chip is used to test the RAM. ROM does not require a constant electric supply to keep the information intact. Information in ROM is retained should you switch the PC off

## **Root Directory**

The highest point in the Directory structure at which a user can access the files. For a typical PC running DOS this is C:\.

## **Route**

The path that data travels along moving from its starting point in a Network to its destination.

## **Router**

A communications device which routes data between Networks.

## **RS232**

The industry standard for the transmission of data between Serial (one bit at a time) Devices. The RS stands for Recommended Standard



## **Scanner**

A scanner is a peripheral device which is used to transer a picture, photograph, image into a file on your PC. The image is scanned & this is converted into a format which the PC can interpret.

## **SCSI**

Small Computer Systems Interface introduced by the American National Standards Institute (ANSI). A SCSI connects PC's to Peripherals & to other PC's & LANs. Up to 7 devices excluding the PC can be attached through a single SCSI connection, linking them together (known as a daisy chain). Only 1 device at a time can transmit through the SCSI connection - the devices are prioritised.



## **SDRAM**

**Synchronous Dynamic Random Access Memory.** It is a type of RAM capable of speeds of about 55MHz. It has superceded EDO RAM.

## **Search Engine**

One of the most essential tools on the Internet - they help you find web sites relating to a particular subject or the Email address of someone you know or articles posted to a Newsgroup or even companies which have a presence on the Internet. Most of the information provided by search engines is categorised so the search can be considerably refined before you even begin. The search engines are basically huge databases containing millions of records which include the URL of a particular Web page along with information relating to the content of the web page which is supplied in the HTML by the author. The search engine obtains this information via a submission from the author or by the search engines doing a "crawl" using "robot crawlers" of the internet for information.

Some search engines use Spiders to obtain information.

There are a number of facilities available on the web which allow authors to submit their web pages to hundreds of web sites at once.

Some search engines use a technique known as ICE to locate information on related topics.

The majority of the people that use this Glossary would have located it by using a Search Engine.

The most popular search engines are :-

- Alta Vista
- Excite
- Hotbot
- Galaxy
- Infoseek
- Lycos
- Webcrawler
- Yahoo

## **Secondary Cache**

Another term for Level 2 Cache.

## **Shareware**

Software that you can obtain for free. The author of the software does request a small fee to pay for registration, documentation etc.

## **Server**

A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running, e.g. Our mail server is down today, that's why e-mail isn't getting out. A single server machine could have several different server software packages running on it, thus providing many different servers to clients on the network.

## **SIMMs**

Single In-line Memory Modules. Memory chips which are soldered onto plugs which slot into sockets on the Motherboard of the PC - makes fitting memory much easier than it use to be.

SIMMs come in various speeds & sizes - 1Mb, 4Mb, 16Mb & 32Mb - with speeds of 90, 80, 70 or 60 nanoseconds (60 is faster than 90).

SIMMs can either be 30-pin or 72-pin.

DIMMs, Dual In-line Memory Modules are now available. These have 168 pins in two rows

## **SLIP**

Serial Line Internet Protocol, basically a standard which enables a user to connect to the internet using a modem & a telephone line.

## **Snail Mail**

A term that us Email users use to describe the traditional mail or post office service. A note will take seconds to go from London to Sydney via Email but a number of days via Snail Mail.

## **Software**

Software is basically a series of instructions that causes the PC to do something. The Operating System such as DOS is known as Systems Software. Application Programs such as a Word Processor or Spreadsheet perform the main tasks for which we use the PC i.e. a letter to Mum or managing the finances.

## **Spam**

Basically sending Emails to people who in no way asked you to send that information - normally done in huge numbers to promote a product.

## **Spider**

A search engine which obtains its information by starting at a specified Web Page & visiting each Web Page which has a link to it from the current page that the spider is accessing. This process continues as it moves it way through the WWW.

## **Spreadsheet**

An Application Program where the information is stored in a grid. The spreadsheet has Rows &

Columns. A spreadsheet with 3 rows & 3 columns will have 9 "Cells" where data can be manipulated. Typically they are used for tracking expenses, budgeting etc. The content of a Cell can be based on that of other Cells & the spreadsheet program has a number of built in functions for manipulating Cells e.g. Sum, Average etc. Example Spread sheet programs include:-

- Microsoft Excel
- Lotus 123

## SQL

Structured Query Language - a standard for managing, retrieving, changing & deleting records from relational databases.

## Subroutine

A subroutine is part of a program which performs a specific task & can be actioned from more than one place within the program. For instance, in a windows program the programmer may write a subroutine to close the current window as this task is likely to be actioned from several different places within the program.

## SVGA

Super Visual Graphics Array Video Aapter. A SVGA Monitor can display up to 1280 X 1024 pixels using over 16 million different colours.



## T-1

T-1 is a leased line Internet connection. The speed at which data can be transmitted is 1.45 megabits per second.

## T-3

T-3 is a leased line Internet connection. The speed at which data can be transmitted is 45 megabits per second.

## TCP/IP

TCP/IP stands for Transmission Control Protocol/Internet Protocol & is quite simply a standard set of protocols that govern the basic workings of the Internet which was implemented in 1982.

The TCP part is all about ensuring that data is transmitted correctly between 2 computers. If any errors occur these are detected & the data is retransmitted. The data transmitted is split up into small portions called Data packets. The IP part of TCP/IP is how these data packets are moved from one point to another. Each computer on the internet has a unique IP address & the data packets are moved from the source to the destination through many different computers & this is controlled via TCP/IP. This protocol is used on the Internet & also by computers which are part of a LAN.

## **Telnet**

Telnet is program which is part of the TCP/IP protocol. Its purpose is to allow a user to logon to a computer from a remote location.

## **Temporary Files**

These are Files which are set up by a Program because it needs to use them when it runs. For example a spreadsheet program might want to keep a record of the last change that was made by the user to allow the change to be "undone" if required. The program may decide to keep the copy of the changes in a Temporary File. All good programs will delete Temporary Files when they are no longer required.

## **Terminal**

A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry. Usually you will use terminal software in a personal computer - the software pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

## **Terminal Server**

A special purpose computer that has places to plug in many modems on one side, and a connection to a LAN or host machine on the other side. Thus the terminal server does the work of answering the calls and passes the connections on to the appropriate node. Most terminal servers can provide PPP or SLIP services if connected to the Internet.

## **Text File**

A common used term used to describe ASCII Text Files.

## **TIFF**

Tagged Image File Format. One of the many different types of File Format used on PC's. This particular type is a graphics file i.e. a picture.

## **Toolbar**

The Toolbar sits across the top or down the side of a particular Window. The toolbar allows the use to perform certain tasks such as opening a file or submitting a print. The toolbar can usually be customised so that the user can add those tasks most regularly performed

## **TSR**

Terminate and Stay Resident These are DOS programs which sit in memory so they can be run from within other application programs.

*U*

## **UNIX**

A Multitasking Operating System developed in 1969. There are many variants of Unix. Written in the C Programming Language it is very portable - running on a number of different computers. Unix is the main operating system used by Internet host computers.

## **Upload**

To copy files from your own PC to another computer via a network or using a modem. Opposite of download.

## **Upper Memory Area**

The 384 Kilobytes of memory immediately above the 640K Conventional memory on a PC.

## **URL**

Uniform Resource Locator - How documents on the WWW are referenced. The URL contains the protocol to be used e.g. HTTP

## **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.

## **Userid**

Each user that is permitted to use a computer can be allocated an identification code which uniquely

identifies them to the computer. Normally the user will first be asked to enter this code - their userid followed by their password when they Log on to the computer. My Userid to get onto the internet is jenko.

*V*

## **VESA**

Video Electronics Standards Association - responsible for graphics & Local Bus Standards.

## **VGA**

Visual Graphics Array Video Apapter introduced by IBM in 1987. A VGA Monitor can display 640 X 480 pixels using 16 different colours or 320 X 200 pixels using 256 colours. These colours can be chosen from a table of up to 262,144 colours.

## **Video Adapter**

Used to generate & send Video signals via a cable to the Monitor. The video adapter can be located on the Motherboard or in an Expansion Slot. Examples include :-

- CGA
- EGA
- VGA
- SVGA

## **Virtual memory**

Hard Disk space on your PC which is used as if it was actual memory. Windows reserves an area of your hard disk which it uses as virtual memory.

## **Virus**

This is a program which can damage the files on your PC - often created intentionally to do so.

## **Virus Scan**

A program which a PC user will invoke in order to check that their PC contains no known viruses.

## **VMEBus**

Versa Module Eurocard BUS. VMEbus is the term used to describe the established standard technology used by many systems developers/ integrators/vendors to serve user communities that require open systems architectures. It is the most utilized bus in real-time applications throughout the world. For More Information Click Here.

## **VRML**

Virtual Reality Modelling Language is a Programming Language which has been designed to build 3D worlds on the World Wide Web. With this language a programmer can create a virtual three dimensional world which the user can explore.



## **WAIS**

(Wide Area Information Servers) -- A commercial software package that allows the indexing of huge quantities of information, and then making those indices searchable across networks such as the Internet. A prominent feature of WAIS is that the search results are ranked (scored) according to how relevant the hits are, and that subsequent searches can find more stuff like that last batch and thus refine the search process.

## **WAN**

Stands for Wide Area Network. Basically a linked Network of LANs. The Internet can be considered to be the largest WAN there has ever been.

## **Web Browser**

An application program which interprets HTML & presents the final Web Page. Used to "Surf the WWW". Examples include:-

- Internet Explorer
- Netscape Navigator
- Mosaic

## **Web Master**

The person who is responsible for looking after a particular Web Site

## **Web Page**

An HTML document which contains information which can be seen on the Internet

## **Web Site**

A group of Web Pages which collectively represent a company, or individual on the WWW. A group of Web pages which have been developed together to present information on a specific subject(s) is also a Web Site - This Glossary falls into that category.

## **Web Space**

The amount of storage space that your Internet Service Provider gives you to use for your own personal web page. Normally between 2 Megabytes & 10 Megabytes.

## **Windows**

Windows is the everyday term for Microsoft Windows which is a multitasking Graphical User Interface which runs under DOS. This user interface is made up of a number of "views" which sit on top of each other - these are the Windows. Tasks are performed by using a mouse to click an Icon, selecting an item from a menu or using the mouse to click on an item on a toolbar.

## **Windows 95**

Microsoft's flagship Operating System introduced to the world in August 1995. The main benefit is that Windows 95 & DOS are one

## **Word Processor**

Word Processors are Application program used mainly for creating text-based documents. Used by everyone to send letters to Mum, do the CV, newsletters, prepare business documentation, Invoices etc. Word Processors have moved on significantly over a short period of time. Nowadays one can insert pictures, check spelling automatically, change the colour of the text. This Glossary was prepared using Microsoft Word.

Examples of Word processors include:-

- Microsoft Word
- Word Perfect
- Ami Pro

## **WWW**

The World Wide Web - The Internet facility that allows you to browse linked web pages.



## WYSIWYG

Stands for What You See Is What You Get basically it means that what you can see on the screen is what you will see on paper when you print the screen contents.



## ZIF Socket

The Processor in most modern PC's sits in what is called a ZIF (Zero Insertion Force) Socket. The idea is that it is easy to insert a new chip. A lever is pulled to get the chip out, plug in the new chip & throw the lever to lock it in place.

## 0 to 9

286

386

486

8086

8088

**286**

The 80286 Microprocessor was introduced by Intel in 1982. PC's with this kind of Microprocessor are normally referred to as 286 Computers.

**386**

The 80386 Microprocessor was introduced by Intel in 1985. PC's with this kind of Microprocessor are normally referred to as 386 Computers.

**486**

The 80486 Microprocessor was introduced by Intel in 1989. PC's with this kind of Microprocessor are normally referred to as 486 Computers.

**8086**

The 8086 Microprocessor was introduced by Intel in 1978.

**8088**

The 8088 Microprocessor was introduced by Intel in 1978.

# COMMONLY USED CHAT ROOM AND E-MAIL ACRONYMS

Most chat rooms have no-profanity rule and some rooms have foul-language filters that screen out inappropriate language. Likewise many parents who have access to their children's e-mail accounts will not permit certain language use by their children.

For these obvious reasons, and many others, some chat room users and e-mailers use a coded language that is based on acronyms. This is a rapidly developing language and complete literacy is very difficult. The Exploited Child Unit of the National Center for Missing and Exploited Children has compiled a list of the most commonly used acronyms. This list will be updated regularly and often.

## Acronym Meaning

|       |                                |
|-------|--------------------------------|
| adr   | address                        |
| afaik | As Far As I Know               |
| afk   | Away From Keyboard             |
| aka   | Also Known As                  |
| alol  | Actually Laughing Out Loud     |
| aml   | All My Love                    |
| asap  | As Soon As Possible            |
| asl   | Age/Sex/Location               |
| aslmh | Age/Sex/Location/Music/Hobbies |
| atm   | At The Moment                  |
| awol  | Absent Without Leave           |
| bak   | Back At Keyboard               |
| bbfn  | Bye Bye For Now                |
| bbl   | Be Back Later                  |
| bbs   | Be Back Soon                   |
| bbsl  | Be Back Sooner or Later        |
| bcnu  | Be Seeing You                  |
| bfm   | Bye For Now                    |
| bka   | Better Known As                |
| brb   | Be Right Back                  |
| brt   | Be Right There                 |
| btw   | By The Way                     |
| bbiab | Be back in a bit               |
| Bbeg  | Big evil grin                  |
| bfd   | Big f***ing deal               |
| bg    | Big grin                       |
| brb   | Be right back                  |
| cul   | See you later                  |
| cyo   | See you online                 |
| cy    | calm yourself                  |
| cya   | See You                        |
| dl    | Download                       |
| duct  | Did You See That?              |
| eg    | Evil grin                      |
| emfbi | Excuse me for butting in       |
| el    | Evil Laugh                     |
| f2f   | Face to Face                   |
| fawc  | For Anyone Who Cares           |
| ftf   | Face To Face                   |

## Acronym Meaning

|            |                                             |
|------------|---------------------------------------------|
| fwiw       | For What Its Worth                          |
| fya        | For Your Amusement                          |
| fyi        | For Your Information                        |
| fla        | Four-letter acronym                         |
| fomcl      | Falling off my chair laughing               |
| fubar      | F***ed up beyond all recognition            |
| fud        | Fear, Uncertainty, and Doubt                |
| fwiw       | For what it's worth                         |
| galgal     | Give A Little Get A Little                  |
| gbh        | Great Big Hug                               |
| gg         | Good Game                                   |
| ggn        | Gotta Go Now                                |
| gl         | Good Luck                                   |
| gmta       | Great Minds Think Alike                     |
| gr8        | Great                                       |
| g          | Grin                                        |
| ga         | Go ahead                                    |
| GOL        | Giggling out loud                           |
| hih        | Hope It Helps                               |
| hiliacaclo | Help I Lapsed Into A Coma And Can't Log Off |
| hth        | Hope This Helps                             |
| iae        | In Any Event                                |
| iat        | I am Tired                                  |
| ic         | I See                                       |
| icbw       | I Could Be Wrong                            |
| idk        | I Don't Know                                |
| igtp       | I Get The Point                             |
| ihno       | I have no opinion                           |
| iir        | If I Recall                                 |
| im         | Instant Message                             |
| imao       | In My Arrogant Opinion                      |
| imho       | In My Humble Opinion                        |
| imo        | In My Opinion                               |
| iow        | In Other Words                              |
| irl        | In Real Life                                |
| ianal      | I am not a lawyer (but)                     |
| iirc       | If I recall/remember/recollect correctly    |

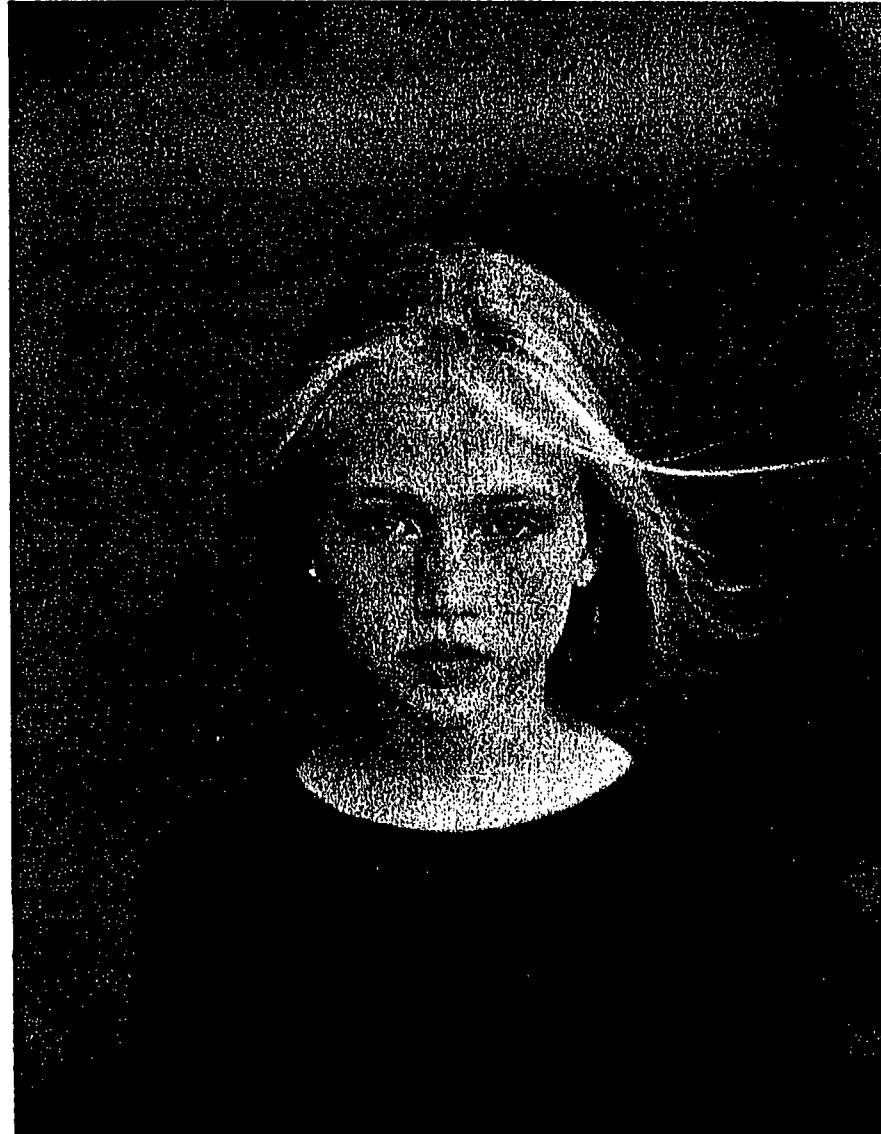
|           |                                           |
|-----------|-------------------------------------------|
| lu or ily | I love you                                |
| mho       | In my humble opinion                      |
| mnsno     | In my not so humble opinion               |
| pn        | I'm posting naked                         |
| ic        | Just in case                              |
| k         | Just Kidding                              |
| jt        | Just Teasing                              |
| k         | Okay                                      |
| kotc      | Kiss On The Cheek                         |
| kotl      | kiss on the lips                          |
| l8r       | Later                                     |
| lOl       | Laughing out loud                         |
| lmao      | Laughing My A** Off                       |
| lola      | Laugh Out Loud Again                      |
| lool      | Laughing Outragously Out Loud             |
| lwr       | Launch When Ready                         |
| lylas (b) | love you like a sister (brother)          |
| msg       | Message                                   |
| nfw       | No feasible way or no f*****g way         |
| n1        | nice one                                  |
| nda       | Non-Disclosure Agreement                  |
| nm        | Nevermind                                 |
| np        | No Problem                                |
| nrn       | No Reply Necessary                        |
| oic       | Oh, I see                                 |
| otoh      | On the other hand                         |
| omg       | Oh My God                                 |
| ooi       | Out Of Interest                           |
| otoh      | On The Other Hand                         |
| ousu      | Oh, You Shut U                            |
| pans      | Pretty awesome new stuff                  |
| pda       | Public Display of Affection               |
| pls       | please                                    |
| pm        | Personal Message                          |
| ppl       | people                                    |
| pmfjib    | Pardon me for jumping in but...           |
| pots      | Plain old telephone service               |
| ql        | quit laughing!                            |
| qs        | Quit Scrolling                            |
| qt        | cutie                                     |
| rbay      | right back at ya                          |
| rotfl     | Rolling on the floor laughing             |
| rotflmao  | Rolling on the floor laughing my a** off  |
| rotflbo   | Rolling on the floor laughing my butt off |
| rtfm      | Read the f***ing manual                   |
| seg       | S***-eating grin                          |
| sed       | Said Enough Darling                       |
| sfete     | Smiling From Ear To Ear                   |
| smaim     | Send Me An Instant Message                |
| somy      | Sick of me yet?                           |
| snafu     | Situation normal, all f***ed up           |
| tfds      | That's For Darn (Damn) Sure               |

|            |                            |
|------------|----------------------------|
| Tia        | Thanks In Advance          |
| tnc or tic | tongue in cheek            |
| tfn        | Ta-Ta for now              |
| ttyl       | Talk to you later          |
| vbg        | Very big grin              |
| vbseg      | Very big s***-eating grin  |
| w/         | with                       |
| w/b        | Write Back                 |
| w/o        | without                    |
| wad        | Without A Doubt            |
| wb         | welcome back               |
| wbs        | Write Back Soon            |
| weg        | Wicked Evil Grin           |
| wtg        | way to go                  |
| wth        | What The Heck (Hell)       |
| wywh       | Wish You Were Here         |
| wt?        | What/who the ?             |
| wtfu       | What the F***! Are You!    |
| xm         | excuse me                  |
| xme        | 'EXCUSE' me                |
| xo         | hugs, kisses               |
| ygbsm      | You got to be s***tin' me! |
| y          | why                        |
| yw         | Your Welcome               |
| zzz        | sleeping, bored, tired     |

## Emotional and Symbolic Acronyms

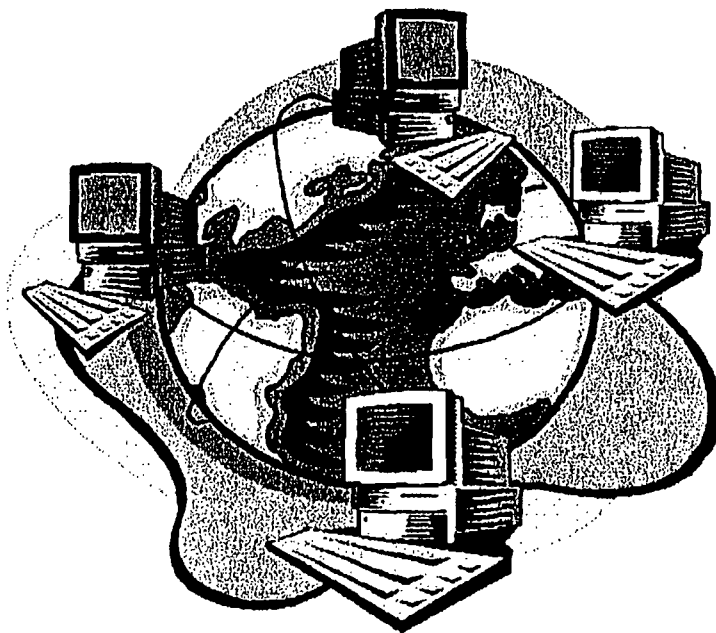
| <u>Acronym</u> | <u>Meaning</u>                  | <u>Acronym</u> | <u>Meaning</u>           |
|----------------|---------------------------------|----------------|--------------------------|
| :              | Ambivalent                      | :(             | Frown                    |
| o:-)           | Angelic                         | ~/             | Full Glass               |
| >:-(           | Angry                           | \_/            | Glass (drink)            |
| _I             | Asleep                          | ^5             | High Five                |
| (:():::)       | Bandaide                        | ((((name))))   | Hug (cyber hug)          |
| :-}            | Blowing a Kiss                  | (( )):**       | Hugs and Kisses          |
| \_o            | Bored                           | :-I            | Indifferent              |
| :-c            | Bummed Out                      | :-#            | Lips are Sealed          |
| C              | Can of Coke                     | :-~            | Mixed Up                 |
| P              | Can of Pepsi                    | :-O            | Mouth Open (Surprised)   |
| :()            | Can't Stop Talking              | ()             | Mug (coffee, beer)       |
| :*)            | Clowning                        | @[]~           | Mug of HOT Coffee or Tea |
| :'             | Crying                          | ****           | Popcorn                  |
| :'-)           | Crying with Joy                 | &&&&           | Pretzels                 |
| :'-(-          | Crying Sadly                    | @--)--(--      | Rose                     |
| :-9            | Delicious, Yummy                | :-@            | Screaming                |
| :->            | Devilish                        | :O             | Shocked                  |
| ;->            | Devilish Wink                   | :)             | Smile                    |
| :P             | Disgusted (sticking out tongue) | ^              | Thumbs Up                |
| :*)            | Drunk                           | :-&            | Tongue Tied              |
| :-6            | Exhausted, Wiped Out            | :-\            | Undecided                |
|                |                                 | ;) )           | Wink                     |
|                |                                 | _O             | Yawning                  |

# The Exploited Child Unit



*Protecting and Empowering Our Children*

# **THE INTERNET AND THE CYBERTIPLINE**



**The National Center for Missing and Exploited Children**

# Internet Related Reports

---



Your review of CyberTipline reports has or eventually will lead you to encounter the various components of the Internet. A follow-up to your first training, "Introduction to the Internet," this session will deal with applying your knowledge to your work with the CyberTipline. The topics we will discuss are as follows

- What is ftp?
- What is Listserv?
- What is Usenet and Newsgroups?
- Understanding URLs
- Understanding Email addresses
- Helper Applications & Plug-ins

**E  
C  
U**



# Domain Names

---



Several top-level domains (TLDs) are common in the United States:

|     |                                 |
|-----|---------------------------------|
| com | commercial enterprise           |
| edu | educational institution         |
| gov | U.S. government entity          |
| mil | U.S. military entity            |
| net | network access provder          |
| org | usually nonprofit organizations |

**U  
C  
E**

# Understanding Email Addresses

Since an email address can tell you a lot about an individual, I thought it might be useful to briefly explain email addresses and free email accounts.

## Email Basics

An email address has two parts: user\_name@domain\_name (eg. Trauch@ncmec.org)

The first part is the person's user name. That may be an abbreviated version of their name (eg. Trauch or raucht) or their name in full eg. Terry.Rauch or Terry\_Rauch).

The second part is the domain name which tells the email server on which computer the recipient's email account is located. Domain names are usually made up of three parts. The computer name, the high level domain to which the computer forms a part and the country domain.

The format is: [computer\_name].[domain\_type].[country]

[computer\_name] can be any name that the computer's administrator has registered eg. ncmec

[domain\_type] will be either "com", "edu", "gov", "mil" or "org".

[country] is a two letter code for each country. eg. "au" for Australia. The only country not to have a code is the United States. Domain names in the United States do not have a [country] on the end. eg www.missingkids.com.

## Types of Internet Domains

For the U.S., these are the following classes of Internet domains:

- .edu: an educational institution (ex. jhu.edu: John Hopkins University)
- .org: an organization not seen as being part of the for-profit sector (ex. ncmec.org: National Center for Missing and Exploited Children)
- .com: a commercial enterprise, including a commercial online service (ex. aol.com: America Online)
- .net: An Internet Service Provider (ISP, not really the same as a commercial online service) (ex. charm.net: Charm City's own Charm Net)
- .gov: a governmental body (ex. loc.gov: Library of Congress)
- .mil: a military body (ex. milinet.mil: interagency military network)

For the British Commonwealth countries, there are at least two domain types preceding the country code:

- .ac: an academic organization (ex. oxford.ac.uk: U. of Oxford)
- .co: A commercial organization (ex. blackwell.co.uk: Blackwell Co.)

### Free Email (Anonymous Email)

This type of email account allows individuals to send anonymous correspondence all over the world, at no charge. Free email provides access to email from wherever a person is -- at home, at work, while traveling, at the local public library, or at school in the computer lab. You don't need to own a computer to use these accounts. All one needs is a web connection. The email service stores all of the email for subscribers. This is important since a considerable amount of illegal and dangerous email correspondence (child luring and photo transfers) are done by individuals using "fake" emails (anonymous email). Identifying these email accounts might help you in your work.

### Large Free Email Providers

Yahoo! Mail: **trauch@yahoo.com.**

Net@address: **trauch@usa.net.**

Hotmail: Must use your web browser to Get/Send Mail. **trauch@hotmail.com**

MailCity: Pretty much the same as HotMail. **trauch@mailcity.com.**

Geocities: Gives an E-Mail address with a free web site. **trauch@geocities.com**

RocketMail: Free E-Mail Account. **trauch@rocketmail.com**

Bigfoot: Free E-mail Address when you become a member. **trauch@bigfoot.com**

Juno: They provide software to Get/Send Mail. **trauch@juno.com**

### Other Forwarding Email Services

|              |                    |             |                  |
|--------------|--------------------|-------------|------------------|
| INDOCITIES   | @indocities.com    | Callsign    | @callsign.com    |
| CHURCHUSA    | @churchusa.com     | Populus     | @populus.com     |
| SINGPOST     | @singpost.com      | Dotcom      | @mail.dotcom.fr  |
| FREEYELLOW   | @freeyellow.com    | GMX         | @gmx.net         |
| PLANETALL    | @planetall.com     | Infomedia   | @info-media.de   |
| BIGFOOT      | @bigfoot.com       | Chez        | @chez.com        |
| BROADCAST    | @broadcast.net     | Cybermail   | @cybermail.com   |
| ATLINK       | @atlink.com        | XTEL        | @free.xtel.com   |
| UNI          | @uni.de,@mailto.de | PRATOMIC    | @pratomic.com    |
| WONDER-NET   | @wonder-net.com    | Kitznet     | @kitznet.at      |
| GEOCITIES    | @geocities.com     | Onvillage   | @onvillage.com   |
| HEREMAIL     | @heremail.com      | Seguros     | @seguros.com.br  |
| YCLUB        | @yclub.com         | Visitweb    | @visitweb.com    |
| FWNB         | @fwnb.com          | Mailnet     | @mailnet.org.uk  |
| Beer.Com     | @beer.com          | Altern      | @altern.org      |
| Stones       | @stones.com        | Advalvas    | @advalvas.be     |
| Copacabana   | @copacabana.com    | Deneg       | @deneg.net       |
| Friends-café | @friends-café.com  | Stealthmail | @stealthmail.com |

**\*\*\*STARMAIL(MYOWNEMAIL), NETFORWARD, FRIENDLY MAIL, INAME,  
THEBOYS, NETFORWARD\*\*\***

The short list above are email forwarding services that provide numerous domain names. You can not create your own domain name but there are hundreds - possibly thousands to choose from. These names are easily identified because they are descriptive or are statements, for instance trauch@antisocial.com. The domain names always end in ".com" and can describe or make statements about sexual acts, music, TV, movies, sports, celebrities and quotes or funny statements. Examples of such domain names are:

@lover-boy.com, @cyberloveplace.com, @onecooldude.com @hehe.com,  
@metallicafan.com, @thepolice.com, @the-beatles.com, @lover-boy.com, @trust-  
me.com, @earthcorp.com, @POBoxes.com, @thepentagon.com, @theoffice.net,  
@writeme.com, @mindless.com, @Themarines.com, @thearmy.com,  
@collegemail.com, @LAOffice.com, @LondonOffice.com, @fan.theboys.com,  
@dallas.theboys.com, @phil-collins.com, @rednecks.com, @federalreserve.com,  
@smileyface.com, @most-wanted.com, @forpresident.com, @cindy-crawford.com,

**Anonymous remailer**

An anonymous remailer (also called an "anonymous server") is a free computer service that privatizes your e-mail. A remailer allows you to send electronic mail to a Usenet news group or to a person without the recipient knowing your name or your e-mail address.

By using an anonymous remailer, an individual can write to any email and have their true email address STRIPPED AWAY(the header at the top of your e-mail), and have it replaced with a dummy address. The Anonymous remailer or server then forwards your message to wherever you want it to go.

Currently, there are roughly a dozen active, PUBLIC remailers on the Internet. Undoubtedly, there are PRIVATE remailers that restrict who may use them.) Remailers tend to come and go. First, they require equipment and labor to set up and maintain; second, they produce zero revenue.

|          |                             |
|----------|-----------------------------|
| Nym      | config@nym.alias.net        |
| Htp      | mixer@htp.org               |
| Cracker  | remailer@anon.efga.org      |
| Redneck  | config@anon.efga.org        |
| Replay   | remailer@replay.com         |
| Squirrel | mix@squirrel.owl.de         |
| jam      | remailer@cypherpunks.ca     |
| mix      | mixmaster@remai.obscura.com |
| privacy  | remailer@privacynb.ml.org   |
| htuttle  | h_tuttle@juno.com           |
| grit     | grit_remailer@juno.com      |
| palnu    | palnu@juno.com              |

tea  
neva  
bureau42

tea@notatla.demon.co.uk  
remailer@neva.org  
remailer@bureau42.ml.org

# What is FTP?



Definition: File Transfer Protocol (FTP) is an Internet protocol which allows you to move files from one computer to another. FTP allows you to retrieve publicly accessible files on anonymous FTP servers and transfer them to your local computer account. Publicly accessible FTP servers are called anonymous servers because you log into them with the keyword anonymous.

Searching for FTP files?

Archie is the search engine of anonymous FTP sites. It is easiest to search FTP sites using Web-based Archie search engines. For an example, view the list of FTP search engines at this URL:

<http://www.albany.edu/library/internet/engines.html>

**E  
C  
U**

# What is Listserv

---



Listserv discussion groups are electronic discussion groups relating to specific topics which distribute all messages sent to the list to the e-mail addresses of all the list members. Listserv itself is a software program that allows users to join groups, configure subscription options, and search the archives of previous messages.

Try these directories on the World Wide Web:

LISZT - <http://www.liszt.com/>

TILE.NET - <http://tile.net/>

**U  
C  
E**

# What is Usenet and Newsgroups?

---



Usenet is a network of computers which exchange electronic mail tagged with predetermined headers. The mail is referred to as articles, the subjects are newsgroups. Usenet is implemented by software that downloads and uploads newsgroup mail. This software implements the Network News Transfer Protocol (NNTP). You can read Usenet articles by the use of a software program called a newsreader.

Newsgroup names begin with a group name identifier which describes the general type of newsgroup: See "Supplemental 1"

**E  
C  
U**



# Usenet and Newsgroups Headers

---



When Usenet messages are sent, the predetermined headers are available for all members of the Usenet to see. These headers hold information about the sender, the date and the identifies which newsgroup it is going to.

Subject: Upcoming baseball season

Date: Fri, 27 Feb 1998 17:15:36 -0500

From: janedoe <janedoe@hotmail.com>

Organization: BBallRUs - Ohio

Newsgroups: alt.sports.baseball

-- OR --

Subject: Upcoming Fashion

Date: 27 Feb 1998 03:23:47 GMT

From: johndoe@aol.com (johndoe)

Organization: AOL <http://www.aol.com>

Newsgroups: society.style.fallfashion

**E  
C  
U**

# Understanding URLs

---



URL stands for Uniform Resource Locator. The URL specifies the Internet address of a file stored on a host computer connected to the Internet. Every file on the Internet, no matter what its access protocol, has a unique URL. Web software programs use the URL to retrieve the file from the host computer and the directory in which it resides. This file is then displayed on the user's computer monitor.

URLs are translated into numeric addresses using the Internet Domain Name System (DNS). The numeric address is actually the "real" URL. Since numeric strings are difficult for humans to use, alphnumeric addresses are employed by end users. Once the translation is made, the Web server can send the requested page to the user's Web browser.

**E  
C  
U**

# Anatomy of URLs

---



This is the format of the URL:

protocol://host/path/filename

For example, this is a URL of the Preperation page of the CyberTipline

<http://www.missingkids.com/cybertip/cybertipline.html>

This URL is typical of addresses hosted in domains in the United States.

Structure of this URL:

- 1.Protocol: http
- 2.Host computer name: www
- 3.Second-level domain name: missingkids
- 4.Top-level domain name: com
- 5.Directory name: cybertip
- 6.File name: cybertipline.html

**E  
C  
U**

# Domain Names

---

In addition, dozens of domain names have been assigned to identify and locate files stored on host computers in countries around the world. These are referred to as two-letter Internet country codes, and have been standardized by the International Standards Organization as ISO 3166. For example:

|    |                |
|----|----------------|
| ch | Switzerland    |
| de | Germany        |
| jp | Japan          |
| uk | United Kingdom |

**U  
C  
E**

# Email Addresses

---



An email address has two parts: user name@domain name (eg. Trauch@ncmec.org)

The first part is the person's user name. That may be an abbreviated version of their name (eg. Trauch or raucht) or their name in full eg. Terry.Rauch or Terry\_Rauch).

The second part is the domain name which tells the email server on which computer the recipient's email account is located. Domain names are usually made up of three parts. The computer name, the high level domain to which the computer forms a part and the country domain.

The format is: [computer\_name].[domain\_type].[country]  
See “Supplemental 2”

**UCC**

# Helper Applications and Plug-ins

---



- Software programs may be configured to a Web browser in order to enhance its capabilities. When the browser encounters a sound, image or video file, it hands off the data to other programs, called helper applications, to run or display the file. Many helper applications are available for free.

- Plug-ins are software programs that extend the capabilities of a Web browser in a specific way, such as the ability to play audio files or view video movies from within Navigator. Web browsers are often standardized with a small suite of plug-ins. Additional plug-ins may be obtained at the browser's Web site, at special download sites on the Web, or from the home pages of the companies that created the programs. The number of available plug-ins is increasing rapidly. Nearly 200 plug-ins are available for downloading at the Netscape site.

**E  
C  
U**

# Helper Applications and Plug-ins

---



- Apple's Quick Time Player downloads files with the .mov extension and displays these as "movies" in a small window on your computer screen. Quick Time files can be quite large, and it may take patience to wait for the entire movie to download into your computer before you can view it.
- The RealPlayer plug-in plays streaming audio and video files. Extensive files such as interviews, speeches and hearings work very well with the RealPlayer. The RealPlayer is also ideal for the broadcast of real-time events. These may include press conferences, live radio and television broadcasts, concerts, etc.
- Shockwave presents another multimedia experience. Shockwave allows for the creation and implementation of an entire multimedia display combining graphics, animation and sound.

**E  
C  
U**

| Group Name | Meaning                                                |
|------------|--------------------------------------------------------|
| Alt        | alternative groups that are often very free in content |
| Bit        | usually a cross-posting of a listserv discussion group |
| Comp       | computers, computer science, software                  |
| Misc       | newsgroups that don't fall into any other category     |
| News       | general news and topical subjects                      |
| Rec        | recreational activities, arts, hobbies                 |
| Sci        | science                                                |
| Soc        | social issues, socializing                             |
| Talk       | debate-oriented discussions                            |





Federal Resources on  
Missing and Exploited  
Children:

***A Directory for Law  
Enforcement and Other  
Public and Private  
Agencies***



# **Federal Agency Task Force for Missing and Exploited Children**



**U.S. Department of Defense**  
Family Advocacy Program  
Legal Assistance Offices

**U.S. Department of Education**  
Office of Elementary and Secondary Education  
Safe and Drug-Free Schools Program

**U.S. Department of Health and Human Services**  
Family and Youth Services Bureau  
National Center on Child Abuse and Neglect

**U.S. Department of Justice**  
Child Exploitation and Obscenity Section  
Federal Bureau of Investigation  
Office for Victims of Crime  
Office of Juvenile Justice and Delinquency Prevention/  
Missing and Exploited Children's Program  
U.S. Immigration and Naturalization Service  
U.S. National Central Bureau (INTERPOL)

**U.S. Department of State**  
Office of Children's Issues

**U.S. Department of Treasury**  
U.S. Customs Service  
U.S. Secret Service  
Forensic Services Division

**U.S. Postal Service**  
U.S. Postal Inspection Service

**National Center for Missing and Exploited Children**

**Federal Resources on Missing and Exploited Children:  
A Directory For  
Law Enforcement and Other Public and Private Agencies**

---

---

---

---

---

---

**Federal Agency Task Force for Missing and Exploited Children**

**Revised Edition - December 1997**

This document was prepared by Fox Valley Technical College under Cooperative Agreement 95-MC-CX-K002 from the Office of Juvenile Justice and Delinquency Prevention of the U.S. Department of Justice.

The Office of Juvenile Justice and Delinquency Prevention is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the National Institute of Justice, and the Office for Victims of Crime.

## Foreword

Our children are our most important resource, and providing a safe environment for them is our most important responsibility. When a child is reported missing or victimized, our response as a society must be swift, efficient, and effective.

Faced with reduced budgets and high violent crime rates, state and local law enforcement are often unable to actively investigate missing children cases on a long-term basis. In stranger abduction cases, where victim life expectancy often can be measured in hours, local law enforcement is under incredible pressure to recover the child immediately. All missing and exploited children cases, whether short or long-term, can strain the resources of the investigating agency. Consequently, it is critical for information about Federal programs and services to be available so that local law enforcement can request them when needed.

This directory was prepared by the Federal Agency Task Force for Missing and Exploited Children and represents the Task Force's initial efforts to enhance the coordination of the delivery of Federal services to missing and exploited children and their families. Designed to provide information about Federal resources, the directory is a compilation of the many services, programs, publications, and training that address issues of child sexual exploitation, child pornography, child abductions, and missing children cases. The directory contains information ranging from access to specialized forensic resources for an abducted child case, to proactive training and prevention programs.

This second edition of the directory has been prepared to insure that the most up-to-date information is readily available and accessible to law enforcement officials as they investigate cases involving missing and exploited children. It is the Task Force's hope that child-serving professionals and law enforcement will find this publication to be a valuable supplement and that it will enhance their activities and programs for missing and exploited children.

I invite you to make use of this directory as we all work to protect our Nation's children.

Shay Bilchik  
*Administrator*  
Office of Juvenile Justice and Delinquency Prevention



## Acknowledgments

Compiling a directory of this type is a labor of love. It requires the commitment, dedication, and cooperation of many agencies and many persons within those agencies. The Task Force wishes to thank the following individuals in particular, who gave their time and energy so generously to the development of the first and revised versions of the Resource Directory:

Thomas Andreotta  
U.S. Immigration and Naturalization Service  
U.S. Department of Justice

Gail Beaumont  
Safe and Drug-Free Schools Program  
U.S. Department of Education

Joe Bock  
Family and Youth Services Bureau  
U.S. Department of Health and Human Services

Greg Burns  
U.S. Customs Service  
U.S. Department of Treasury

Ray Clore  
Office of Children's Issues  
U.S. Department of State

Emily Cooke  
National Center on Child Abuse and Neglect  
U.S. Department of Health and Human Services

Richard Dusak  
Forensic Services Division  
U.S. Secret Service  
U.S. Department of Treasury

William Hagmaier, S.S.A.  
Child Abduction and Serial Killer Unit  
Morgan P. Hardiman Task Force on Missing and  
Exploited Children  
Federal Bureau of Investigation  
U.S. Department of Justice

John Hargett  
Forensic Services Division  
U.S. Secret Service  
U.S. Department of Treasury

Don Huycke, S.S.A.  
U.S. Customs Service  
U.S. Department of Treasury

Margie Kazdin  
National Center for Missing and Exploited Children

Richard Laczynski, S.S.A.  
U.S. National Central Bureau (INTERPOL)  
U.S. Department of Justice

Ronald C. Laney  
Missing and Exploited Children's Program  
Office of Juvenile Justice and Delinquency  
Prevention  
U.S. Department of Justice

Cynthia J. Lent  
Child Abduction and Serial Killer Unit  
Federal Bureau of Investigation  
U.S. Department of Justice

Terry R. Lewis  
Family and Youth Services Bureau  
U.S. Department of Health and Human Services

David Lloyd  
Family Advocacy Program  
U.S. Department of Defense

Terry Lord  
Child Exploitation and Obscenity Section  
U.S. Department of Justice

George Martinez  
Office of Crimes Against Children  
Federal Bureau of Investigation  
U.S. Department of Justice

Michael Medaris  
Missing and Exploited Children's Program  
Office of Juvenile Justice and Delinquency  
Prevention  
U.S. Department of Justice

Carolyn O'Doherty  
Violent Crimes Unit  
Federal Bureau of Investigation  
U.S. Department of Justice

Curtis Porter  
Family and Youth Services Bureau  
U.S. Department of Health and Human Services

James R. Prietsch, S.A.  
U.S. National Central Bureau (INTERPOL)  
U.S. Department of Justice

John Rabun  
National Center for Missing and Exploited Children

Leslie Rowe  
Office of Children's Issues  
U.S. Department of State

Judy Schretter  
Child Exploitation and Obscenity Section  
U.S. Department of Justice

Jim Schuler  
Office of Children's Issues  
U.S. Department of State

Sue Shriner  
Office for Victims of Crime  
U.S. Department of Justice

Raymond C. Smith  
Office of Criminal Investigations  
U.S. Postal Inspection Service  
U.S. Postal Service

Dan Wright, S.S.A.  
Violent Crime and Fugitive Unit  
Federal Bureau of Investigation  
U.S. Department of Justice

Elizabeth Yore  
National Center for Missing and Exploited Children

Jim York  
Interpol - U.S. Central Bureau  
U.S. Department of Justice

Cynthia Quinn  
Interpol - Criminal Division  
U.S. Department of Justice



# Table of Contents

|                                                                                                             |     |
|-------------------------------------------------------------------------------------------------------------|-----|
| Foreword . . . . .                                                                                          | iii |
| Acknowledgments . . . . .                                                                                   | v   |
| Introduction . . . . .                                                                                      | 1   |
| Where To Get Help . . . . .                                                                                 | 3   |
| List of Acronyms . . . . .                                                                                  | 13  |
| Federal Agencies                                                                                            |     |
| U.S. Department of Defense                                                                                  |     |
| Family Advocacy Program . . . . .                                                                           | 17  |
| Legal Assistance Offices . . . . .                                                                          | 21  |
| U.S. Department of Education                                                                                |     |
| Office of Elementary and Secondary Education                                                                |     |
| Safe and Drug-Free Schools Program . . . . .                                                                | 23  |
| U.S. Department of Health and Human Services                                                                |     |
| Family and Youth Services Bureau . . . . .                                                                  | 27  |
| National Center on Child Abuse and Neglect . . . . .                                                        | 33  |
| U.S. Department of Justice                                                                                  |     |
| Child Exploitation and Obscenity Section . . . . .                                                          | 35  |
| Federal Bureau of Investigation . . . . .                                                                   | 37  |
| Office for Victims of Crime . . . . .                                                                       | 43  |
| Office of Juvenile Justice and Delinquency Prevention/Missing and<br>Exploited Children's Program . . . . . | 47  |
| U.S. Immigration and Naturalization Service . . . . .                                                       | 51  |
| U.S. National Central Bureau (INTERPOL) . . . . .                                                           | 53  |
| U.S. Department of State                                                                                    |     |
| Office of Children's Issues . . . . .                                                                       | 57  |
| U.S. Department of Treasury                                                                                 |     |
| U.S. Customs Service . . . . .                                                                              | 61  |
| U.S. Secret Service                                                                                         |     |
| Forensic Services Division . . . . .                                                                        | 63  |
| U.S. Postal Service                                                                                         |     |
| U.S. Postal Inspection Service . . . . .                                                                    | 65  |
| Organizations                                                                                               |     |
| National Center for Missing and Exploited Children . . . . .                                                | 71  |

# Appendixes

|                                                                                                                 |      |
|-----------------------------------------------------------------------------------------------------------------|------|
| Appendix 1. Department of Defense Investigative Liaisons for Law Enforcement Agencies . . .                     | 1-1  |
| Appendix 2. Safe and Drug-Free Schools Comprehensive Regional Centers . . . . .                                 | 2-1  |
| Appendix 3. Family and Youth Services Bureau Regional Centers . . . . .                                         | 3-1  |
| Appendix 4. Organizations Concerned With the Prevention of Child Abuse and Neglect:<br>State Contacts . . . . . | 4-1  |
| Appendix 5. FBI Field Offices . . . . .                                                                         | 5-1  |
| Appendix 6. FBI Legal Attaches . . . . .                                                                        | 6-1  |
| Appendix 7. Crime Victims Compensation/Assistance - State Agencies and Programs . . . . .                       | 7-1  |
| Appendix 8. Interpol State Liaison Offices . . . . .                                                            | 8-1  |
| Appendix 9. Office of Children's Issues Abduction and Custody Information Checklist . . . . .                   | 9-1  |
| Appendix 10. U.S. Customs Service Field Offices . . . . .                                                       | 10-1 |
| Appendix 11. U.S. Postal Inspection Service Division Boundaries . . . . .                                       | 11-1 |

## Introduction

Creation of the Federal Agency Task Force for Missing and Exploited Children was announced by Attorney General Janet Reno on May 25, 1995, at the 12th Annual Missing Children's Day. The mission of the Task Force is to coordinate Federal resources and services to effectively address the needs of missing, abducted, and exploited children and their families. The Task Force:

- Serves as an advocate for missing and exploited children and their families.
- Initiates positive change to enhance services and resources for missing and exploited children, their families, and the agencies and organizations that serve them.
- Promotes communication and cooperation among agencies and organizations at the Federal level.
- Serves as the focal point for coordination of services and resources.

The Task Force includes representatives from 16 Federal agencies and one private agency that work directly with cases involving missing, abducted, and exploited children and their families. As used in this guide, the term "missing child" refers to any youth under the age of 18 whose whereabouts are unknown to his or her legal guardian. This includes children who have been abducted or kidnaped by a family member or a nonfamily member, a child who has run away from home, a child who is a throwaway, or a child who is otherwise missing. It also includes both national and international abductions. The term "child exploitation" refers to any child under the age of 18 who has been exploited or victimized for profit or personal advantage. This includes children who are victims of pornography, prostitution, sexual tourism, and sexual abuse.

Members of the Task Force are acutely aware of the tremendous pressure placed on people who handle these types of cases on an ongoing basis. The devastating impact on the child, family, community, and practitioner; the gravity and severity of these offenses; and the overwhelming amount of time required to resolve such cases often place unfair burdens and challenges on those responsible for case investigations. Yet, when a child is missing, abducted, or victimized, an immediate and continual response is key to the successful resolution of a case.

In response to these concerns, the Task Force developed this resource manual to contribute support and to provide real solutions to practitioners when they most need them. This manual contains information on the resources, technical assistance and support, and services that are available during the investigation of cases involving missing and exploited children. The manual describes the role of each Task Force agency in the location and recovery of missing and exploited children, the types of services and support that are available, the procedures for accessing these services, and instructions for obtaining additional information. To make the information accessible, the next section, "Where To Get Help," categorizes the type of assistance offered by each agency. In addition, telephone quick reference cards can be removed and kept where most needed; addresses and phone numbers are correct as of the date of publication.

The information contained in this manual will help to expand the resources that are available, enhance services for children and their families, increase coordination of services for missing and exploited children and their families, and promote positive system change. We hope this manual provides the added tools and information practitioners need to face the many challenges that lie ahead.

The manual is from the Office of Juvenile Justice and Delinquency Prevention's (OJJDP's) Juvenile Justice Clearinghouse, P.O. Box 6000, Rockville, MD 200849-6000, 800-638-8736. The manual is also available through OJJDP's home page at <http://www.ncjrs.org/pdffiles/fedredir/pdf>.

# Where To Get Help

## Agencies that provide...

### TRAINING

- National Center for Missing and Exploited Children
- U.S. Department of Education
  - Safe and Drug-Free Schools Program*
- U.S. Department of Health and Family Services
  - Family and Youth Services Bureau*
  - National Center on Child Abuse and Neglect*
- U.S. Department of Justice
  - Child Exploitation and Obscenity Section*
  - Federal Bureau of Investigation*
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency*
  - Prevention/Missing and Exploited Children's Program*
  - U.S. Immigration and Naturalization Service*
  - U.S. National Central Bureau (INTERPOL)*
- U.S. Department of State
  - Office of Children's Issues*
- U.S. Department of Treasury
  - U.S. Customs Service*
- U.S. Postal Service
  - U.S. Postal Inspection Service*

### TECHNICAL ASSISTANCE

- National Center for Missing and Exploited Children
- U.S. Department of Defense
  - Family Advocacy Program*
- U.S. Department of Education
  - Safe and Drug-Free Schools Program*
- U.S. Department of Health and Family Services
  - Family and Youth Services Bureau*
  - National Center on Child Abuse and Neglect*
- U.S. Department of Justice
  - Child Exploitation and Obscenity Section*
  - Federal Bureau of Investigation*
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency*
  - Prevention/Missing and Exploited Children's Program*
- U.S. Department of Treasury
  - U.S. Secret Service/Forensic Services Division*
- U.S. Department of State
  - Office of Children's Issues*

**LEGAL ASSISTANCE TO CHILDREN AND FAMILIES**

National Center for Missing and Exploited Children  
U.S. Department of Defense  
*Legal Assistance Offices*

**LITIGATION ASSISTANCE**

U.S. Department of Justice  
*Child Exploitation and Obscenity Section*

**PUBLICATIONS**

National Center for Missing and Exploited Children  
U.S. Department of Defense  
*Family Advocacy Program*  
U.S. Department of Education  
*Safe and Drug-Free Schools Program*  
U.S. Department of Health and Human Services  
*Family and Youth Services Bureau*  
*National Center on Child Abuse and Neglect*  
U.S. Department of Justice  
*Federal Bureau of Investigation*  
*Office for Victims of Crime*  
*Office of Juvenile Justice and Delinquency Prevention/*  
*Missing and Exploited Children's Program*  
U.S. Department of State  
*Office of Children's Issues*  
U.S. Department of Treasury  
*U.S. Secret Service/Forensic Services Division*

**RESEARCH AND EVALUATION**

U.S. Department of Education  
*Safe and Drug-Free Schools Program*  
U.S. Department of Health and Human Services  
*Family and Youth Services Bureau*  
*National Center on Child Abuse and Neglect*  
U.S. Department of Justice  
*Federal Bureau of Investigation*  
*Office of Juvenile Justice and Delinquency Prevention/*  
*Missing and Exploited Children's Program*

## **Agencies that provide services to...**

### **MISSING AND EXPLOITED YOUTH AND THEIR FAMILIES**

National Center for Missing and Exploited Children

U.S. Department of Defense

*Family Advocacy Program*

U.S. Department of Health and Human Services

*Family and Youth Services Bureau*

*National Center on Child Abuse and Neglect*

U.S. Department of State

*Office of Children's Issues*

### **FEDERAL PROSECUTORS**

U.S. Department of Justice

*Child Exploitation and Obscenity Section*

*Federal Bureau of Investigation*

*U.S. National Central Bureau (INTERPOL)*

U.S. Department of State

*Office of Children's Issues*

U.S. Department of Treasury

*U.S. Customs Service*

U.S. Postal Service

*U.S. Postal Inspection Service*

### **STATE AND LOCAL PROSECUTORS**

National Center for Missing and Exploited Children

U.S. Department of Justice

*Federal Bureau of Investigation*

*Office for Victims of Crime*

*Office of Juvenile Justice and Delinquency Prevention/*

*Missing and Exploited Children's Program*

*U.S. National Central Bureau (INTERPOL)*

U.S. Department of State

*Office of Children's Issues*

U.S. Department of Treasury

*U.S. Customs Service*

U.S. Postal Service

*U.S. Postal Inspection Service*

**LAW ENFORCEMENT AGENCIES**

- National Center for Missing and Exploited Children
- U.S. Department of Defense
  - Family Advocacy Program*
- U.S. Department of Justice
  - Federal Bureau of Investigation*
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency Prevention/  
Missing and Exploited Children's Program*
  - U.S. Immigration and Naturalization Service*
  - U.S. National Central Bureau (INTERPOL)*
- U.S. Department of State
  - Office of Children's Issues*
- U.S. Department of Treasury
  - U.S. Customs Service*
  - U.S. Secret Service/Forensic Services Division*
- U.S. Postal Service
  - U.S. Postal Inspection Service*

**STATE AND LOCAL GOVERNMENT AGENCIES**

- National Center for Missing and Exploited Children
- U.S. Department of Health and Family Services
  - National Center on Child Abuse and Neglect*
- U.S. Department of Justice
  - Federal Bureau of Investigation*
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency Prevention/  
Missing and Exploited Children's Program*
- U.S. Department of State
  - Office of Children's Issues*
- U.S. Department of Treasury
  - U.S. Customs Service*
- U.S. Postal Service
  - U.S. Postal Inspection Service*

**NATIVE AMERICAN TRIBES**

- U.S. Department of Health and Family Services
  - National Center on Child Abuse and Neglect*
- U.S. Department of Justice
  - Federal Bureau of Investigation*
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency Prevention/  
Missing and Exploited Children's Program*



**DIRECT SERVICE PROVIDERS AND YOUTH SERVICE AGENCIES**

- U.S. Department of Education
  - Safe and Drug-Free Schools Program*
- U.S. Department of Health and Human Services
  - Family and Youth Services Bureau*
  - National Center on Child Abuse and Neglect*
- U.S. Department of Justice
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency Prevention/*
  - Missing and Exploited Children's Program*

**NONPROFIT ORGANIZATIONS**

- National Center for Missing and Exploited Children
- U.S. Department of Health and Human Services
  - Family and Youth Services Bureau*
  - National Center on Child Abuse and Neglect*
- U.S. Department of Justice
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency Prevention/*
  - Missing and Exploited Children's Program*
- U.S. Department of State
  - Office of Children's Issues*

**GENERAL PUBLIC**

- National Center for Missing and Exploited Children
- U.S. Department of Health and Human Services
  - Family and Youth Services Bureau*
  - National Center on Child Abuse and Neglect*
- U.S. Department of Justice
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency Prevention/*
  - Missing and Exploited Children's Program*
- U.S. Department of State
  - Office of Children's Issues*
- U.S. Department of Treasury
  - U.S. Customs Service*

## **Agencies that provide assistance on cases involving...**

### **PARENTAL KIDNAPING**

National Center for Missing and Exploited Children  
U.S. Department of Defense  
*Legal Assistance Offices*  
U.S. Department of Justice  
*Federal Bureau of Investigation*  
*U.S. Immigration and Naturalization Service*  
*U.S. National Central Bureau (INTERPOL)*  
U.S. Department of State  
*Office of Children's Issues*

### **RUNAWAY CHILDREN**

National Center for Missing and Exploited Children  
U.S. Department of Health and Human Services  
*Family and Youth Services Bureau*  
U.S. Department of Justice  
*U.S. National Central Bureau (INTERPOL)*  
U.S. Department of Treasury  
*U.S. Secret Service Forensic Services Division*

### **MISSING AND EXPLOITED CHILDREN**

National Center for Missing and Exploited Children  
U.S. Department of Defense  
*Family Advocacy Program*  
U.S. Department of Health and Human Services  
*Family and Youth Services Bureau*  
*National Center on Child Abuse and Neglect*  
U.S. Department of Justice  
*Federal Bureau of Investigation*  
*Office for Victims of Crime*  
*Office of Juvenile Justice and Delinquency Prevention/*  
*Missing and Exploited Children's Program*  
*U.S. Immigration and Naturalization Service*  
*U.S. National Central Bureau (INTERPOL)*  
U.S. Department of State  
*Office of Children's Issues*  
U.S. Department of Treasury  
*U.S. Customs Service*  
*U.S. Secret Service/Forensic Services Division*  
U.S. Postal Service  
*U.S. Postal Inspection Service*

#### **CHILD SEXUAL EXPLOITATION**

- National Center for Missing and Exploited Children
- U.S. Department of Defense
  - Family Advocacy Program*
- U.S. Department of Health and Family Services
  - National Center on Child Abuse and Neglect*
- U.S. Department of Justice
  - Child Exploitation and Obscenity Section*
  - Federal Bureau of Investigation*
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency Prevention/  
Missing and Exploited Children's Program*
  - U.S. National Central Bureau (INTERPOL)*
- U.S. Department of Treasury
  - U.S. Customs Service*
  - U.S. Secret Service/Forensic Services Division*
- U.S. Postal Service
  - U.S. Postal Inspection Service*

#### **CHILD PROSTITUTION**

- National Center for Missing and Exploited Children
- U.S. Department of Justice
  - Child Exploitation and Obscenity Section*
  - Federal Bureau of Investigation*
  - Office for Victims of Crime*
  - U.S. National Central Bureau (INTERPOL)*

#### **CHILD PORNOGRAPHY**

- National Center for Missing and Exploited Children
- U.S. Department of Justice
  - Child Exploitation and Obscenity Section*
  - Federal Bureau of Investigation*
  - Office for Victims of Crime*
  - Office of Juvenile Justice and Delinquency Prevention/  
Missing and Exploited Children's Program*
  - U.S. National Central Bureau (INTERPOL)*
- U.S. Department of Treasury
  - U.S. Customs Service*
  - U.S. Secret Service/Forensic Services Division*
- U.S. Postal Service
  - U.S. Postal Inspection Service*

### **SEXUAL TOURISM**

National Center for Missing and Exploited Children  
U.S. Department of Justice  
*Child Exploitation and Obscenity Section*  
*Federal Bureau of Investigation*  
*Office for Victims of Crime*  
U.S. Department of Treasury  
*U.S. Customs Service*  
*U.S. Secret Service/Forensic Services Division*

### **INTERNATIONAL ABDUCTION**

National Center for Missing and Exploited Children  
U.S. Department of Defense  
*Legal Assistance Offices*  
U.S. Department of Justice  
*Federal Bureau of Investigation*  
*U.S. National Central Bureau (INTERPOL)*  
U.S. Department of State  
*Office of Children's Issues*

### **INTERNATIONAL ADOPTION**

U.S. Department of Justice  
*U.S. National Central Bureau (INTERPOL)*  
U.S. Department of State  
*Office of Children's Issues*

### **Agencies that provide 24-hour information and referral sources to children and their families...**

National Center for Missing and Exploited Children  
U.S. Department of Health and Human Services  
*Family and Youth Services Bureau*  
U.S. Department of State  
*Consular Affairs Duty Officer (when an international abduction is in progress)*

### **Agencies that provide compensation to crime victims...**

U.S. Department of Justice  
*Office for Victims of Crime*

**Agencies that provide forensic services...**

National Center for Missing and Exploited Children

U.S. Department of Justice

*Federal Bureau of Investigation*

U.S. Department of Treasury

*U.S. Secret Service/Forensic Services Division*



## **List of Acronyms**

AFIS -- Automated Fingerprint Identification System  
BCP -- Basic Center Program  
CASKU -- Child Abduction and Serial Killer Unit  
CCR -- Community Crisis Response  
CEOS -- Child Exploitation and Obscenity Section  
CI -- Children's Issues  
CIRG -- Critical Incident Response Group  
CJA -- Children's Justice Act  
DoD -- Department of Defense  
FBI -- Federal Bureau of Investigation  
FISH -- Forensic Information System for Handwriting  
FYSB -- Family and Youth Services Bureau  
JJDP -- Juvenile Justice and Delinquency Prevention  
NCB -- National Central Bureau  
NCCAN -- National Center on Child Abuse and Neglect  
NCFY -- National Clearinghouse on Families and Youth  
NCIC -- National Crime Information Center  
NCJRS -- National Criminal Justice Reference Service  
NCMEC -- National Center for Missing and Exploited Children  
OVC -- Office for Victims of Crime  
OJJDP -- Office of Juvenile Justice and Delinquency Prevention  
RICO -- Racketeer Influenced and Corrupt Organizations  
SOP -- Street Outreach Program  
TECS -- Treasury Enforcement Computer System  
TLP -- Transitional Living Program  
USNCB -- U.S. National Central Bureau (INTERPOL)  
VICAP -- Violent Criminal Apprehension Program  
VOCA -- Victims of Crime Act





---

---

**FEDERAL AGENCIES**

---

---



# U.S. Department of Defense

## Family Advocacy Program

### Agency Description

The Family Advocacy Program of the Department of Defense (DoD) is designed to prevent and treat child and spouse abuse in accordance with DoD Directive 6400.1, Family Advocacy Program. DoD maintains a central registry of reports of alleged child and spouse abuse. Allegations of child sexual abuse that occur in out-of-home care settings, such as in child care centers, family day care homes, schools, or recreation programs, must also be reported within 72 hours to the Service Family Advocacy Program for inclusion in the central registry and to the DoD Assistant Secretary (Force Management Policy) or to his or her designee. Criminal prosecution is the primary goal of intervention in cases involving multiple victim child sexual abuse in an out-of-home care setting.

### Services

If more than one child is a victim of sexual abuse in an out-of-home care setting, the Service may convene a multidisciplinary technical assistance team for the installation at the request of the installation commander, or the Assistant Secretary of Defense (Force Management Policy) may deploy a joint service multidisciplinary team of specially trained personnel from the four Services to provide technical assistance. Technical assistance may include law enforcement investigations, forensic medical examinations, forensic mental health examinations, and victim assistance to the child and family.

The primary recipients at the installation are the Family Advocacy Program Manager, the investigators of the installation law enforcement agency, and the physicians and mental health professionals at the military treatment facility or those who provide services under contract.

For cases involving missing and exploited children, appendix 1 lists the investigative liaisons for law enforcement agencies.

### Availability of Services

Services are available to: (1) members of the Armed Services who are on active duty and their family members who are eligible for treatment in a military treatment facility, and (2) members of a reserve or National Guard component who are on active duty and their family members who are eligible for treatment in a military treatment facility.

At the request of the installation commander, a multidisciplinary team is convened by the Family Advocacy Program Manager for a particular Service. A joint Service team is deployed by the Office of the Assistant Secretary (Force Management Policy) at the request of the installation

commander. These services are directed to cases in which multiple children are victims of sexual abuse in an out-of-home care setting.

## **Publications**

Copies of the following publications are available from the Military Family Resource Center:

- ▶ DoD Directive 6400.1, "Family Advocacy Program."
- ▶ DoD Instruction 6400.2, "Child and Spouse Abuse Report."
- ▶ DoD Instruction 6400.3, "Family Advocacy Command Assistance Team."
- ▶ DoD Directive 5525.9, "Compliance of DoD Members, Employees, and Family Members Outside the United States With Court Orders."

Publication orders should be directed to:

Military Family Resource Center  
4040 N. Fairfax Drive, 4<sup>th</sup> Floor  
Arlington, VA 22203-1635  
Telephone: (703) 696-9053  
Fax: (703) 696-9062

## **Agency Contact**

For further information, contact the appropriate Department of Defense Family Advocacy Program Manager listed below:

### ***Army***

Army Family Advocacy Program Manager  
HQDA, CFSC-FSA  
Department of the Army  
Hoffman #1, Room 1407  
Alexandria, VA 22331-0521  
Telephone: (703) 325-9390  
Fax: (703) 325-5924

### ***Navy***

Director  
Family Advocacy Program  
BUPERS 661  
Department of the Navy  
Washington, DC 20370-5000  
Telephone: (703) 697-6616/8/9  
Fax: (703) 697-6571

***Air Force***

Chief  
Family Advocacy Division  
HQ AFMOA/SGPS  
8901 18th Street, Suite 1  
Brooks Air Force Base, TX 78235-5217  
Telephone: (210) 536-2031  
Fax: (210) 536-9032

***Marine Corps***

Marine Corps Family Advocacy Program  
Manager  
Headquarters USMC  
Human Resources Division (Code MHF)  
Washington, DC 20380-0001  
Telephone: (703) 696-2066 or 696-1188  
Fax: (703) 696-1143

***Defense Logistics Agency***

Family Advocacy Program Manager  
Quality of Life Program CAAPQ  
Defense Logistics Agency  
8725 John J. Kingman Road, STE 2533  
Fort Belvoir, VA 22060-6221  
Telephone: (703) 767-5372  
Fax: (703) 767-5374



# U.S. Department of Defense

## Legal Assistance Offices

### Agency Description

The Army, Navy, Air Force, and Marine Corps legal assistance offices serve as the point of contact for inquiries concerning the legal issues in the abduction of a child by a parent or other family member either on active duty with that Armed Service or accompanying such a Service member. They are also the point of contact for the State Department in cases of international abduction of the children of Service members.

### Services

Responsibility for ensuring a Service member's compliance with child custody orders is placed with that Service member's commander. Legal assistance offices provide advice to active-duty and retired Service members and their family members on personal civil legal matters, but do not provide representation in civilian court. The legal assistance offices listed below can provide assistance in locating a Service member and will coordinate with the local legal office where that Service member is stationed. That local legal office provides legal assistance to the Service member's commander. The legal assistance offices listed below are also the points of contact for the State Department in cases of international abduction of the children of Service members.

### Availability of Services

Legal advice is available to active-duty and retired Service members and their family members who are parents of children who have been abducted. In all other cases, services are limited to assistance in locating the Service member and coordinating with the local legal office or commander. Representation in civilian court is not provided. Services may be obtained directly by a parent at the Service's legal assistance agency or through the legal office where the Service member is stationed. The parent seeking assistance must have a valid court order for custody or visitation.

### Publications

Copies of the following publication are available from the Military Family Resource Center:

DoD Directive 5525.9, "Compliance of DoD Members, Employees, and Family Members Outside the United States With Court Orders."

Publication orders should be directed to:

Military Family Resource Center  
4040 N. Fairfax Drive, 4<sup>th</sup> Floor  
Arlington, VA 22203-1635  
Telephone: (703) 696-9053  
Fax: (703) 696-9062

## **Agency Contact**

For further information, contact the appropriate Department of Defense Legal Assistance Office listed below:

### ***Army***

DAJA-LA  
Office of the Judge Advocate General  
Room 2C463  
Pentagon  
Washington, DC 20310-2200  
Telephone: (703) 697-3170

### ***Air Force***

AFLSA/JACA  
1420 Air Force Pentagon  
Washington, DC 20330-1420  
Telephone: (202) 697-0413

### ***Navy***

Legal Assistance (Code 36)  
Office of the Judge Advocate General  
Department of the Navy  
9S25 Hoffman II Building  
200 Stovall Street  
Alexandria, VA 22332-2400  
Telephone: (703) 325-7928

### ***Marine Corps***

Legal Assistance Office  
Judge Advocate Division  
Headquarters, USMC  
301 Henderson Hall  
Southgate Road and Orme Street  
Arlington, VA 22214  
Telephone: (703) 614-1266



# U.S. Department of Education

## Office of Elementary and Secondary Education Safe and Drug-Free Schools Program

### Agency Description

The Safe and Drug-Free Schools Program supports initiatives to meet the seventh National Education Goal, which provides that by the year 2000 all schools will be free of drugs and violence and the unauthorized presence of firearms and alcohol and will offer a disciplined environment that is conducive to learning. These initiatives are designed to prevent violence in and around schools and to strengthen programs that prevent the illegal use of alcohol, tobacco, and drugs; that involve parents; and that are coordinated with related Federal, State, and community efforts and resources.

### Services

Programs and activities supported by the Safe and Drug-Free Schools Program are primarily prevention efforts. The Program provides funding for formula grants to States to support local educational agencies and community-based organizations in developing and implementing programs to prevent drug use and violence among children and youth. The Program also provides funding for national leadership activities that meet identified needs and that directly support classroom teaching. Examples of such activities include:

- Development and implementation of comprehensive drug and violence prevention programs for all students from preschool through grade 12 that include health education, early intervention, pupil services, mentoring, rehabilitation referral, and related activities.
- Strategies to integrate services, such as family counseling and early intervention to prevent family dysfunction, from a variety of providers to enhance school performance and boost attachment to school and family.
- Dissemination of drug and violence prevention materials for classroom use.
- Professional training and development for school personnel, parents, law enforcement officials, and other community members.
- Support for "safe zones of passage" for students between home and school through enhanced law enforcement, neighborhood patrols, and similar measures.
- Interagency initiatives that coordinate Federal efforts to achieve safe and drug-free schools.

- Direct services to schools and school systems afflicted with especially severe drug and violence problems.

## Availability of Services

Training and technical assistance for States, school districts, schools, community-based organizations, and other recipients of funds under the Improving America's Schools Act are available by contacting the appropriate Comprehensive Regional Center listed in appendix 2. Information about programs for elementary and secondary students that are provided by local schools and school districts can be obtained by contacting local Safe and Drug-Free Schools coordinators. State coordinators for Safe and Drug-Free Schools can provide information about statewide programs operated by State education agencies and governors' offices.

## Publications

The publications listed below can be obtained by calling 1-800-624-0100:

*Art of Prevention* (1994).

*Creating Safe and Drug Free Schools: An Action Guide* (1996).

*Drug Prevention Curricula: A Guide to Selection and Implementation* (1988).

*Growing Up Drug Free: A Parent's Guide to Prevention* (1991).

*Learning To Live Drug Free: A Curriculum Model for Prevention* (1991).

*Manual to Combat Truancy* (1996).

*Success Stories From Drug-Free Schools* (1994).

*What Works: Schools Without Drugs* (revised 1992).

*Youth and Alcohol: Selected Reports to the Surgeon General* (1994).

*Youth and Tobacco: Preventing Tobacco Use Among Young People, A Report of the Surgeon General* (1995).

## Legislative Citations

- ▶ Safe and Drug-Free Schools and Communities Act of 1994, Title IV of the Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 2701 *et seq.*).

- ▶ Gun-Free Schools Act of 1994, enacted in March 1994, reauthorized as part of the Improving America's Schools Act in October 1994.
- ▶ Pro-Children Act of 1994, enacted as part of the Goals 2000 Educate America Act, March 1994.
- ▶ Comprehensive Regional Assistance Centers program, Title XIII of the Improving America's Schools Act.
- ▶ Safe Schools Act of 1994 enacted as Title VII of the Goals 2000: Educate America Act.

## **Agency Contact**

For further information about services, contact:

Safe and Drug-Free Schools Program  
U.S. Department of Education  
Portals Building  
600 Independence Avenue SW.  
Room 604  
Washington, DC 20202-6123  
Telephone: (202) 260-3954  
Fax: (202) 260-7767  
e-mail: <http://www.ed.gov/offices/OESE/SDFS>



# U.S. Department of Health and Human Services

## Family and Youth Services Bureau

### Agency Description

The Family and Youth Services Bureau (FYSB) is an agency within the Administration on Children, Youth and Families, Administration for Children and Families. FYSB provides national leadership on youth-related issues and helps individuals and organizations to provide comprehensive services for youth in at-risk situations, as well as for their families. The primary goals of FYSB programs are to provide positive alternatives for youth, ensure their safety, and maximize their potential to take advantage of available opportunities. FYSB programs and services support locally based youth services.

### Services

There are six major FYSB programs that relate to missing and exploited children: the Basic Center Program (BCP), the Transitional Living Program (TLP) for Homeless Youth, the Street Outreach Program (SOP), the National Runaway Switchboard, the National Clearinghouse on Families and Youth (NCFY), and the Runaway and Homeless Youth Training and Technical Assistance System.

#### *Basic Center Program*

FYSB's Basic Center Program supports agencies that provide crisis intervention services to runaway and homeless youth who are outside the traditional juvenile justice and law enforcement systems. The goal of the Program is to reunite youth with their families, whenever possible, or to find another suitable placement when reunification is not an option. Discretionary grants are awarded to Basic Center projects each year on a competitive basis.

There are 350 Basic Center projects across the country. More than three-quarters of these projects are operated by community-based organizations. Some of the projects are freestanding, single-purpose emergency shelters, while others are multipurpose youth service agencies. All Basic Center projects are required to provide a set of essential core services to runaway and homeless youth, including the following:

- Short- and long-term emergency shelter.
- Individual, group, and family counseling for youth and families.
- Aftercare services to stabilize and strengthen families and to ensure that additional assistance is available, if necessary.
- Recreation programs for youth.

- Linkages to other local providers for services that are not available through the Basic Center Program.
- Outreach efforts to increase awareness of available services.

### ***Transitional Living Program for Homeless Youth***

TLP helps homeless youth, ages 16 through 21, make a successful transition to self-sufficient living. The goal is to help young people avoid long-term dependency on social services. Discretionary funds are awarded to local agencies that provide youth with comprehensive services in a supervised living arrangement. The first TLP projects were funded in fiscal year 1990. To date, 86 projects have been funded.

Most local agencies operating TLP's are multipurpose youth service organizations, of which more than half also receive FYSB funds to operate temporary shelter and counseling services for runaway and homeless youth. TLP project staff provide the following services:

- Safe, supportive living accommodations in group homes, host family homes, or supervised apartments.
- Mental and physical health care.
- Education in basic living skills.
- Development of an individual transitional plan.
- Educational advancement assistance.
- Employment preparation and job placement.

### ***Street Outreach Program for Runaway and Homeless Youth***

The primary focus of the Street Outreach Program for Runaway and Homeless Youth is the establishment and building of relationships between staff of local youth service providers and street youth, with the goal of helping young people leave the streets. The local grantee programs provide a range of services directly to or through collaboration with other agencies, specifically those working to protect and treat young people who have been, or who are at risk of being, subjected to sexual abuse or exploitation. Those services include the following:

- Street-based education and counseling.
- Emergency shelter.
- Survival aid.

- Individual assessment.
- Treatment and counseling.
- Prevention and education activities.
- Information and referral.

### ***National Runaway Switchboard***

The National Runaway Switchboard is a confidential, 24-hour, toll-free hotline (1-800-621-4000) that provides assistance to runaway and homeless youth and helps them to communicate with their families and service providers. The switchboard provides the following services to at-risk youth and their families:

- Message delivery.
- Crisis intervention counseling.
- Information and referral services.

The switchboard uses a computerized national resource directory that includes more than 9,000 resources. In addition, the switchboard maintains a management information system for local switchboard staff and conducts an annual conference for local switchboard service providers.

Since early 1970 the switchboard has responded to approximately 120,000 crisis intervention calls. In 1990 the switchboard provided 7,000 referrals to youth service organizations. Through a collaborative agreement with the SONY Corporation, public service announcements are run on SONY's giant video screen in New York City's Times Square.

### ***National Clearinghouse on Families and Youth***

NCFY is a resource for communities interested in developing effective new strategies to support young people and their families. NCFY serves as a central information source on family and youth issues for youth service professionals, policymakers, and the general public. Services include:

**Information Sharing.** NCFY distributes information about effective program approaches, available resources, and current activities relevant to the family and youth services fields. The agency uses special mailings, maintains literature and FYSB program databases, and operates a professionally staffed information line.

**Issue Forums.** NCFY facilitates forums that bring together experts in the field to discuss critical issues and emerging trends and to develop strategies for improving services to families and youth.

**Materials Development.** NCFY produces reports on critical issues, best practices, and promising approaches in the field of family and youth services, as well as information briefs on FYSB and its programs.

**Networking.** NCFY supports FYSB's efforts to form collaborations with other Federal agencies, State and local governments, national organizations, and local communities to address the full range of issues facing young people and their families today.

### ***Runaway and Homeless Youth Training and Technical Assistance System***

Ten regionally based centers (see appendix 3) provide training and technical assistance to projects funded under the Basic Center Program, the Transitional Living Program, the Drug Abuse Prevention Program, and other programs serving runaway and homeless youth. Training and technical assistance are designed to enhance the skills and increase the effectiveness of youth service providers by facilitating information exchange on programmatic and operational procedures that are critical to runaway and homeless youth programs. The 10 regional centers offer onsite consultations; local, State, and regional conferences; information sharing; and skill-based training.

### **Availability of Services**

Services provided by FYSB are directed to runaway and homeless youth and their families. To locate a service provider in your community or to secure services, contact the regional center serving your area (see appendix 3).

### **Publications**

National Clearinghouse on Families and Youth, *Research Summary: Youth With Runaway, Throwaway, and Homeless Experiences: Prevalence, Drug Use, and Other At-Risk Behaviors* (October 1995).

National Clearinghouse on Families and Youth, *Supporting Your Adolescent: Tips for Parents* (January 1996).

### **Legislative Citations**

The Runaway Youth Act, Title III, Juvenile Justice and Delinquency Prevention (JJDP) Act of 1974 (P.L. 93-415) focused attention on the need to develop a nonpunitive system of social services for vulnerable youth and authorized resources to support shelters for runaway and homeless youth. The 1977 Amendments to the JJDP Act (P.L. 95-115) extended services to "otherwise homeless youth" and authorized support for coordinated networks to provide training and technical assistance to runaway and homeless youth service providers (Basic Center Program). The 1980 JJDP Act Amendments (P.L. 96-509) changed the title to the Runaway and Homeless Youth Act. The Program was reauthorized through 1992 by the Anti-Drug Abuse Act of 1988



(P.L. 100-690) and was subsequently reauthorized through FY 1996 by the 1992 JJDP Act Amendments (P.L. 102-586).

The 1988 Amendments to Title III of the Juvenile Justice and Delinquency Prevention Act (P.L. 100-690) included the Transitional Living Program, which was subsequently reauthorized through 1996 by the 1992 Amendments to the JJDP Act (P.L. 102-586).

## **Agency Contact**

For further information about services, contact any of the agencies listed below:

Family and Youth Services Bureau  
U.S. Department of Health and Human Services  
P.O. Box 1882  
Washington, DC 20013  
Telephone: (202) 205-8102  
Fax: (202) 260-9333

National Clearinghouse on Families and Youth  
P.O. Box 13505  
Silver Spring, MD 20911-3505  
Telephone: (301) 608-8098  
Fax: (301) 608-8721

National Runaway Switchboard Hotline  
Telephone: 1-800-621-4000



# **U.S. Department of Health and Human Services**

## **National Center on Child Abuse and Neglect**

### **Agency Description**

The National Center on Child Abuse and Neglect (NCCAN), established by the Child Abuse Prevention and Treatment Act of 1974 (P.L. 93-247), is an agency within the Administration on Children, Youth and Families, Administration for Children and Families. It is the primary Federal agency with responsibility for assisting States and communities in the prevention, identification, and treatment of child abuse and neglect. The Center grants congressionally appropriated funds to States to improve and increase their prevention and intervention efforts. The Center generally coordinates Federal activities in this field.

### **Services**

NCCAN's major activities include: three State grant programs (Basic State Grants, Children's Justice Act [CJA] grants, and Community-Based Family Resource and Support Grants); funding for research, service improvement programs and demonstration projects; the National Child Abuse and Neglect Data System (NCANDS); the National Incidence Study (NIS); the National Clearinghouse on Child Abuse and Neglect Information; and the National Resource Center for Child Maltreatment.

All of these programs relate to missing and exploited children in the sense that all victims of child abuse are exploited in some way. However, in a more specific way CJA grantees are required to improve procedures for the State's investigation and prosecution of child abuse cases, particularly child abuse and exploitation, and to improve the handling of these cases so that additional trauma to the child is limited. Also, the National Resource Center for Child Maltreatment assists States, local agencies, and tribes in developing effective and efficient child protective services (CPS) systems to handle reports of child abuse and neglect.

### **Availability of Services**

The NCCAN Clearinghouse and Resource Center for Child Maltreatment provide information to public and private agency personnel, professionals working in related fields, and members of the general public. See appendix 4 for more information.

### **Publications**

The NCCAN Clearinghouse maintains a complete database of up-to-date information, including all NCCAN publications, on all aspects of child abuse and neglect for professionals and members of

the general public. The Clearinghouse can provide annotated bibliographies on specific topics by request, as well as a copy of the database on CD-ROM.

The **1997 State Statute Series** reflects the status of the law as of December 1996. It includes six volumes of State statutes summaries organized according to the following topic areas:

|                    |                           |                   |                             |
|--------------------|---------------------------|-------------------|-----------------------------|
| <i>Volume I:</i>   | <i>Reporting Laws</i>     | <i>Volume IV:</i> | <i>Child Witnesses</i>      |
| <i>Volume II:</i>  | <i>Central Registries</i> | <i>Volume V:</i>  | <i>Crimes</i>               |
| <i>Volume III:</i> | <i>Investigations</i>     | <i>Volume VI:</i> | <i>Permanency Planning*</i> |

\*This latest volume currently includes one topic element: *Termination of Parental Rights*. Please contact the NCCAN Clearinghouse at (800) FYI-3366 for price information.

In addition to the State Statute Series, the NCCAN Clearinghouse has produced the **1997 Statutes at a Glance Series**. Available free of charge, this series includes 6-7 page fact sheets on the following topic areas:

*Reporting Penalties (1997)*  
*Central Registry Expungement (1997)*  
*HIV Testing of Sex Offenders (1997)*  
*Sex Offender Registration (1997)*  
*Public Notification of the Release of Sex Offenders (1997)*

Finally, law enforcement officials may also be interested in the most recent **User Manuals**, which also are available free of charge:

*Crisis Intervention in Child Abuse and Neglect (1995)*  
*Treatment for Abused and Neglected Children: Infancy to Age 18 (1994)*

## **Agency Contact**

For further information about services, contact:

National Center on Child Abuse and Neglect  
Administration on Children, Youth and  
Families  
U.S. Department of Health and Human  
Services  
P.O. Box 1182  
Washington, DC 20013-1182  
Telephone: (202) 205-8586  
Fax: (202) 260-9351

NCCAN Clearinghouse  
P.O. Box 1182  
Washington, DC 20013-1182  
Telephone: 1-800-FYI-3366  
Fax: (703) 385-3206

# U.S. Department of Justice

## Child Exploitation and Obscenity Section

### Agency Description

Established in 1987 and expanded in 1994, the Child Exploitation and Obscenity Section (CEOS) is a group of attorneys who have specialized in the prosecution of obscenity, child exploitation, and child abuse cases, in international child abduction, and in victim-witness issues. CEOS attorneys, who are responsible for the enforcement of Federal laws in these areas, work with Federal law enforcement agencies, other Federal agencies, and U.S. Attorneys around the country. Although CEOS will assist State and local law enforcement agencies upon request, CEOS's jurisdiction is limited to enforcement of Federal statutes; strictly intrastate cases must be handled at the local level. The CEOS chief serves as the legal advisor to the Missing and Exploited Children Task Force.

### Services

- Litigation support, including assistance to U.S. Attorney's Offices; legal research; legal assistance to other Federal agencies, task forces, and committees on projects relating to child exploitation and obscenity; and policy development.
- Technical assistance.
- Training for prosecutors and investigators on topics such as interviewing skills, case preparation, and child exploitation law.

### Availability of Services

Upon request, CEOS provides litigation support, technical assistance, and training to Federal investigators and prosecutors who work on child sexual exploitation cases, including child pornography, child prostitution, sexual tourism, and sexual abuse occurring on Federal lands. Services are available by contacting the local U.S. Attorney's Office or the FBI field office in the Federal judicial district where the matter arises and requesting that these offices contact CEOS by telephone and/or by writing, and if no response is forthcoming, contacting CEOS directly at the address below.

### Legislative Citations

- ▶ 18 U.S.C. § 228 Child support.
- ▶ 18 U.S.C. § 1204 International parental child kidnaping.

- ▶ 18 U.S.C. § 2241 *et seq.* Sexual abuse.
- ▶ 18 U.S.C. § 2251 *et seq.* Sexual exploitation and other abuse of children.
- ▶ 18 U.S.C. § 2421 *et seq.* Transportation for illegal sexual activity (Mann Act).
- ▶ 18 U.S.C. § 3509 Child victims' and witnesses' rights.
- ▶ 42 U.S.C. § 5776a Morgan P. Hardiman Task Force on Missing and Exploited Children.

## **Agency Contact**

For further information about services, contact:

Child Exploitation and Obscenity Section  
Criminal Division  
U.S. Department of Justice  
1331 F Street NW.  
6th Floor  
Washington, DC 20530  
Telephone: (202) 514-5780  
Fax: (202) 514-1793

# U.S. Department of Justice

## Federal Bureau of Investigation

### Agency Description

The Federal Bureau of Investigation (FBI) exercises its jurisdiction and investigative responsibilities pursuant to Federal statutes addressing various crimes against children including kidnaping and sexual exploitation. Federal law defines children as minors under the age of 18, often referred to as "children of tender years." FBI investigations involving crimes against children generally include violations of Federal statutes relating to child abuse, sexual exploitation of children, interstate transportation of obscene material, computer pornography, interstate transportation of children for sexual activity, parental kidnaping, and violations of the Child Support Recovery Act. In some instances, the RICO (Racketeer Influenced and Corrupt Organizations) statute also may apply. While some of those Federal violations may not necessarily involve the sexual abuse or sexual exploitation of children, such as violations of the International Parental Kidnaping Act, the FBI pursues any child victimization offense within its lawful jurisdiction, often coordinating those investigations with other Federal, State, and local agencies.

Cases related to the sexual abuse and exploitation of children and other crimes against children are given high priority within the FBI. All available and necessary FBI resources are used during these investigations, and each case is aggressively prosecuted. Nonfamily abductions, often referred to as stranger abductions, receive immediate attention. Particular attention is also given to investigations involving organized criminal activity, commercialized child prostitution, and the manufacture and distribution of child pornography. The transmission and exchange of child pornography through computer bulletin boards are aggressively investigated as an insidious form of child sexual exploitation.

The FBI also investigates allegations of sexual assault in Indian country, including the investigation of child abuse and the sexual exploitation of children. The FBI addresses these sensitive investigations by participating with other professionals in a multidisciplinary team approach that enlists the expertise of investigators, social workers, clinical psychologists, victim-witness coordinators, and Federal prosecutors.

### Services

#### *Investigative Services and Support*

**FBI Headquarters.** On January 20, 1997, a new unit and two new offices were established within the Violent Crime and Major Offenders Section, Criminal Investigations Division, at FBI Headquarters. These entities, the Office of Crimes Against Children (OCAC) and the Office of Indian Country Investigations (OICI), are managed within the Special Investigations and Initiatives Unit (SIIU), and became operational during March 1997. Staffed by Supervisory Special Agents

and support professionals, these entities were established to specifically focus on crimes against children and crimes in Indian country. The OCAC addresses all crimes under the FBI's jurisdiction that in any way involve the victimization of children, providing program management and field wide investigative oversight of those critical FBI operations. Likewise, the OICI addresses crimes in Indian country, providing program management and investigative oversight of those sensitive FBI operations. The SIIU, OCAC, and OICI work closely with FBI field offices, other FBI components, and various other entities to provide and coordinate operational support to more effectively address crimes against children.

**FBI Field Offices.** Individual FBI field offices throughout the country serve as the primary point of contact for persons requesting FBI assistance. Special agents assigned as Crimes Against Children Coordinators use all available resources--including investigative, forensic, tactical, informational, and behavioral science--in the investigation of crimes against children. The special agents coordinate their investigations with appropriate local law enforcement agencies, as well as with Federal or State prosecutors. Upon receiving notification that a child has been abducted, FBI Evidence Response Team personnel may be assigned immediately to conduct the forensic investigation of the abduction site and any other appropriate areas, while other special agents typically join law enforcement personnel in coordinating and conducting the comprehensive neighborhood investigation that is vital to the resolution of these cases. A Rapid Start Team may also be deployed immediately to begin the overwhelming task of coordinating and tracking the investigative leads, which often number in the thousands during protracted child abduction investigations. Special Agents will also coordinate child abduction investigations with the National Center for Missing and Exploited Children (NCMEC) and other entities to make full use of all available resources.

**Child Abduction and Serial Killer Unit.** The Child Abduction and Serial Killer Unit (CASKU) is a rapid response element of the FBI's Critical Incident Response Group (CIRG). The unit has primary responsibility for providing investigative support through profiling, violent crime analysis, technical and forensic resource coordination, and application of the most current expertise available in matters involving the abduction or mysterious disappearance of children and serial murder. (Serial murder involves the killing of two or more victims in separate incidents).

Child abductions are among the most difficult crimes to resolve and require immediate dedication of significant resources. A specialized CASKU staff provides operational assistance to Federal, State, and local law enforcement agencies involved in these important investigations. The unit responds immediately to requests and provides onsite assistance as appropriate. CASKU services include:

- Profiles of unknown offenders.
- Crime analysis.
- Investigative strategies.



- Interview and interrogation strategies.
- Behavioral assessments.
- Trial preparation and prosecutive strategy.
- Expert testimony.
- Coordination of other resources, including FBI Evidence Response Teams and FBI laboratory services.

Case consultations may include any or all of the services listed above. Services are provided by telephone, in writing, or in person. In some cases investigators may travel to Quantico for consultation sessions, or CASKU members may be sent to the area of the crimes.

CASKU can also assist in coordinating the deployment of Rapid Start, a computerized major case management support system. CASKU maintains a close working relationship with NCMEC and can help to arrange the use of their resources, such as poster distribution and age enhancement of photographs.

Another CIRG component, the Violent Criminal Apprehension Program (VICAP), works closely with CASKU and provides automated support. To assist investigators working on cases, VICAP analysts perform standard and ad hoc searches of their databases, as well as other law enforcement databases. The VICAP database contains reports submitted by participating law enforcement agencies concerning certain violent crimes, which can be used to analyze and link multiple cases.

In addition to case consultation services, CASKU conducts research regarding child abduction and serial murder in an effort to develop further understanding of the crimes and criminals. Results of research are applied to cases and shared with the criminal justice community through publications and training.

**Morgan P. Hardiman Task Force on Missing and Exploited Children.** Created by the Violent Crime Control and Law Enforcement Act of 1994, the Morgan P. Hardiman Task Force on Missing and Exploited Children coordinates Federal law enforcement resources to assist State and local authorities in investigating the most difficult cases of missing and exploited children. The Task Force is composed of at least two members from each of seven Federal agencies: Bureau of Alcohol, Tobacco, and Firearms; Drug Enforcement Administration; FBI; U.S. Customs Service; U.S. Marshals Service; U.S. Postal Inspection Service; and U.S. Secret Service. As legislated by Congress, the FBI manages the Task Force, which is co-located with CASKU and therefore works closely with that unit. The unit chief of CASKU also serves as chief of the Task Force.

### ***FBI Forensic and Technical Support Services***

CASKU was created to centralize services in child abduction and serial homicide cases. In addition to providing investigative consultation, CASKU can coordinate the application of all FBI headquarters resources needed in particular cases.

The FBI laboratory is the only full-service Federal forensic science laboratory serving the law enforcement community. The FBI is mandated by Title 28, CFR Section 0.85, to conduct scientific examinations of evidence, free of charge, for any duly constituted law enforcement agency in the United States. Assistance is provided through:

- Evidence response teams.
- Document services.
- Latent fingerprint services.
- Scientific analysis services (including chemistry-toxicology, DNA analysis/serology examinations, explosives, firearms-toolmarks, hairs and fibers, and materials analysis).
- Special projects (including graphic design, photographic processing, special photographic services, structural design, and visual production and video enhancement).
- Forensic science research and training.

Detailed information about these services, including instructions for collecting, preserving, and shipping evidence, can be found in the *Handbook of Forensic Science*, which is available from the Government Printing Office. The FBI's Rapid Start Team, developed since the *Handbook* was last revised, provides onsite information management services to support the handling of crisis situations. The team is capable of operating in a bivouac environment, bringing with them all equipment required.

The Special Techniques Program, established in 1993, is another part of the Information Resources Division/Engineering Section. This group uses geophysical methodology and other remote sensing equipment to search for clandestinely concealed evidence. These techniques are considered as an investigative tool only after more expedient measures have been exhausted.

**Criminal Justice Information Services.** Criminal justice information services provided by the FBI include a fingerprint repository and the National Crime Information Center (NCIC).

- **Fingerprint repository.** The FBI serves as the Nation's civil and criminal fingerprint repository and responds to the information needs of Federal, State, local, and international members of the criminal justice community. The FBI receives more than 34,000 fingerprint cards each day.

- **National Crime Information Center.** NCIC is a nationwide computer-based inquiry and response information system that was established in 1967 to serve the criminal justice community. NCIC's purpose is to maintain a computerized filing system of accurate, timely, documented criminal justice information that is readily available through a telecommunications network. An average of 1.3 million inquiry-response transactions per day are processed through more than 100,000 NCIC terminals.

The *Handbook of Forensic Science* describes technical services of the Criminal Justice Information Services Division and the Information Resources Division of the FBI.

### ***Training***

The FBI offers an extensive training program for the law enforcement community. Training in a broad spectrum of topics is offered to bona fide law enforcement personnel in settings throughout the United States, around the world, and at the FBI Academy. Each FBI field office has a training coordinator. International requests for training can be made through the FBI Legal Attaches at American Embassies.

### ***Victim-Witness Assistance***

Each FBI field office has a victim-witness coordinator. The FBI's Victim-Witness Assistance Program operates on a referral basis for victims of Federal violations.

### **Availability of Services**

Recipients of FBI services include law enforcement agencies and the U.S. Government (hence the citizens of the United States). Services can be accessed by a request from a law enforcement agency, either through the Child Abduction and Serial Killer Unit or through the local FBI field office or Legal Attache (see appendix 5 and 6 for a list of these offices and attaches).

### **Legislative Citations**

FBI investigations involving child victimization are based upon violations of Federal statutes, including the crime of kidnaping (Title 18, U.S. Code, Sections 1201 and 1202); International Parental Kidnaping Act (Title 18, U.S. Code, Section 1024); Unlawful Flight to Avoid Prosecution (UFAP) - Parental Kidnaping (Title 18, U.S. Code, Section 1073); crimes committed in Indian country (Title 18, U.S. Code, Section 1153); child sexual abuse (Title 18, U.S. Code, Sections 2241, 2242, 2243, and 2244); sexual exploitation of children (Sections 2251, 2251A, 2252, and 2258); interstate transportation of obscene material (Sections 1462, 1465, and 1466); interstate transportation of children for sexual activity (Sections 2421, 2422, 2423, and 2424); Child Support Recovery Act (Title 18, U.S. Code, Section 228); and in some instances the RICO statute (Title 18, U.S. Code, Section 1961).

## **Agency Contact**

For further information about services or to request immediate FBI assistance, contact one of the local FBI field offices, which are listed in appendix 5 and in local telephone directories, or contact one of the units listed below:

**FBI Headquarters**  
Special Investigations and Initiatives Unit  
Office of Crimes Against Children  
Office of Indian Country Investigations  
935 Pennsylvania Avenue NW.  
Washington, DC 20535-0001  
Telephone: (202) 324-3666  
Fax: (202) 324-2731

**Child Abduction and Serial Killer Unit**  
Federal Bureau of Investigation  
Quantico, VA 22135  
Telephone: (540) 720-4700  
Fax: (540) 720-4790

**Morgan P. Hardiman Task Force on Missing and Exploited Children**  
Federal Bureau of Investigation  
Quantico, VA 22135  
Telephone: (540) 720-4760  
Fax: (540) 720-4792

# U.S. Department of Justice

## Office for Victims of Crime

### Agency Description

The mission of the Office for Victims of Crime (OVC) is to enhance the Nation's capacity to assist crime victims and to provide leadership in order to change attitudes and practices to promote justice and healing for all victims of crime. OVC administers the Crime Victims Fund (hereafter called the Fund), which was authorized by the Victims of Crime Act of 1984 (VOCA). Financing for the Fund comes from criminal fines, forfeited bail bonds, penalty fees, and special assessments collected by U.S. Attorneys, U.S. Courts, and the Federal Bureau of Prisons.

Each year OVC makes awards to State crime victim assistance and compensation programs to supplement State funding for victim services. In addition, OVC provides victim assistance training and technical assistance for criminal justice officials and direct service providers. Exploited children, families of missing and exploited children, practitioners who provide direct services to victim families, and law enforcement personnel who investigate and prosecute such cases are eligible to participate in OVC-sponsored programs.

### Services

#### *Crime Victim Compensation*

Crime victim compensation is the direct payment to a crime victim or to his or her family to help cover crime-related expenses such as medical treatment, mental health counseling, lost wages, or funeral services. Every State administers a crime victim compensation program. Most of these programs have similar eligibility requirements and offer a comparable range of benefits. Most programs require victims to report crimes to the police in a timely manner and to file claims within a fixed period of time.

Each year OVC uses VOCA funds to supplement State resources. States receive a grant based on 40 percent of the amount of compensation benefits made by the State in a previous year.

#### *Crime Victim Assistance*

Crime victim assistance programs provide direct services such as crisis intervention, counseling, emergency transportation to court, temporary housing, and criminal justice support and advocacy. All States receive VOCA victim assistance grant funds, which are then awarded by the States to community-based public and nonprofit organizations that serve crime victims, such as domestic violence shelters, child abuse treatment programs, victim service units in law enforcement agencies and prosecutor's offices, hospitals, and social service agencies. Each State receives a base amount of \$500,000, plus a percentage of the amount remaining in the Fund based on population.

### ***Training and Technical Assistance***

OVC's Trainers Bureau seeks to improve services to crime victims by providing training and technical assistance to the programs and agencies that serve crime victims. The Trainers Bureau helps Federal, State, and local agencies address training, administrative, and programmatic issues.

### ***Community Crisis Response Program***

OVC's Community Crisis Response (CCR) program seeks to improve services to communities that have experienced crimes involving multiple victimizations. The program provides rapid response and limited technical assistance to victim service agencies; Federal, State, and local criminal justice agencies; U.S. Attorney's Offices; Native American tribes; and other agencies that assist crime victims.

### ***Information Dissemination***

OVC's Resource Center provides victim-related information to criminal justice practitioners, researchers, policymakers, and crime victims. The OVC Resource Center collects, maintains, and disseminates information on national, State, and local victim-related organizations and on State programs that receive funds authorized by VOCA. The OVC Resource Center is a component of the National Criminal Justice Reference Service (NCJRS), the world's largest criminal justice information clearinghouse.

## **Availability of Services**

OVC services are directed to:

- Missing and exploited children and their families.
- Victims of child pornography.
- Victims of sexual tourism.
- Parents of abducted children.
- Federal, State, and local criminal justice officials and other professionals who handle cases of missing and exploited children.
- Members of the general public who have an interest in child-victim information.

State crime victim compensation applications can be obtained from the appropriate State program. A list of agencies responsible for the administration of crime victims compensation in each State can be found in appendix 7.

### ***Crime Victim Assistance***

OVC provides funding to over 2,500 State crime victim assistance programs. A list of local crime victim assistance programs is available from each State VOCA victim assistance administrator (see appendix 7).

### ***Training and Technical Assistance***

Programs and agencies can access OVC's Trainers Bureau by submitting a request on agency letterhead that: (1) describes the problem to be addressed and explains why it cannot be funded with existing resources, (2) provides information about the individuals to be trained, (3) estimates the number of hours of training or the number of days of technical assistance needed, (4) details the expected outcome of the assistance, and (5) indicates what special skills or knowledge are required of the trainer or assistance provider. If the request is approved for funding, OVC will match trainers and/or technical assistance providers to the request. For additional information, write to the Trainers Bureau at the OVC address below or call (202) 307-5983.

### ***Community Crisis Response (CCR) Program***

Agencies and communities can access OVC's CCR program by submitting a request on agency letterhead that: (1) contains a statement of facts concerning the situation, (2) enumerates the number of victims and describes the impact of the crime on the community, (3) explains why existing resources are inadequate, (4) describes the type of technical assistance requested and the desired outcome, and, if known, (5) lists any special skills required by the consultants. If approved, onsite assistance usually will be short-term, generally from 1 to 3 days. For additional information, write to the CCR program at the OVC address below or call (202) 307-5983.

### ***Information Dissemination***

The OVC Resource Center can be accessed through its toll-free number (1-800-627-6872). A list of publications and other information is available.

OVC has initiated an interactive homepage on the Internet -- <http://www.ojp.usdoj.gov/ovc/>. The new website enables victims, victims advocates, and others interested in victims' rights to obtain information about available services on a state-by-state basis. OVC website visitors can also obtain information about available funding and training and technical assistance opportunities.

## **Publications**

A complete list of OVC publications is available from the OVC Resource Center (1-800-627-6872).

*Child Sexual Exploitation: Improving Investigations and Protecting Victims* (1995), NCJ 153527.

*Crime Victim Compensation: A Good Place to Start* (1996, Video, 9.2 minutes), NCJ 162359.

## **Agency Contact**

For further information about services, contact:

Office for Victims of Crime  
U.S. Department of Justice  
810 7th Street NW.  
Washington, DC 20531  
Telephone: (202) 307-5983  
Fax: (202) 514-6383  
Gopher to: [ncjrs.aspensys.com](mailto:ncjrs.aspensys.com)  
World Wide Web: <http://www.ojp.usdoj.gov/ovc/>



# **U.S. Department of Justice**

## **Office of Juvenile Justice and Delinquency Prevention Missing and Exploited Children's Program**

### **Agency Description**

The Juvenile Justice and Delinquency Prevention (JJDP) Act of 1974 (P.L. 93-415), as amended by the Missing Children's Assistance Act of 1984, establishes the Missing and Exploited Children's Program in the Office of Juvenile Justice and Delinquency Prevention (OJJDP). The purpose of the Missing Children's Assistance Act is to develop leadership and provide funding support to address the needs of the Nation's missing and exploited children and their families and to foster coordination of programs and services for this population.

The Missing and Exploited Children's Program conducts research, demonstration, and service programs pertaining to missing and exploited children; provides training and technical assistance; and coordinates various activities. In addition, the Missing and Exploited Children's Program supports the National Center for Missing and Exploited Children, the national resource center and clearinghouse dedicated to missing and exploited children issues.

Since 1984, the Missing Children's Assistance Act has provided for research, training, and technical assistance to support local law enforcement efforts to locate and recover missing children. Each year the Missing and Exploited Children's Program trains more than 3,500 law enforcement officials in the investigation of missing children cases, at no cost to State or local governments.

### **Services**

- Training and technical assistance.
- Demonstration programs.
- Research projects.
- Evaluation studies.
- Publications.
- Funding for the National Center for Missing and Exploited Children.
- Support for nonprofit organizations that work with missing and exploited children.
- Coordination of the Federal Agency Task Force for Missing and Exploited Children.

## Availability of Services

Training and technical assistance is available to State and local units of government, nonprofit organizations, and other agencies serving missing and exploited children. Research briefs and other publications are available to the general public. Some materials are restricted to law enforcement personnel.

## Training Programs

The following training programs are sponsored by the Missing and Exploited Children's Program. These courses are designed to assist law enforcement officers and other professionals who handle child abuse and exploitation cases.

**Responding to Missing and Abducted Children.** The aim of this course is to enhance the knowledge and skills of law enforcement officials who investigate cases involving abducted, runaway, and other missing youth.

**Child Sexual Exploitation Investigations.** This course provides law enforcement officials and other professionals with the knowledge and information they need to understand, recognize, investigate, and resolve cases of child pornography and sexual exploitation.

**Child Abuse and Exploitation Investigative Techniques.** This course is designed to enhance the skills of experienced law enforcement officials and other professionals who investigate cases involving child abuse, sexual exploitation of children, child pornography, and missing children.

**Missing and Exploited Children Comprehensive Action Program (M/CAP).** M/CAP is a training and technical assistance program that emphasizes community-wide, interagency collaboration and self-assessment, information sharing, and comprehensive case management to address the needs of and respond to missing and exploited children and their families.

**Child Abuse and Exploitation Team Investigative Process.** This course focuses on the development of a community interagency protocol that is unique to jurisdictions implementing a collaborative investigative process for child abuse cases.

## Publications

The following documents are available from the Missing and Exploited Children's Program. Publications with an NCJ number are also available from the National Criminal Justice Reference Service (1-800-851-3420).

*America's Missing and Exploited Children: Their Safety and Their Future* (1986), NCJ 100581.

*Charging Parental Kidnaping* (American Prosecutor's Research Institute, 1995).

*Child Sexual Exploitation: Improving Investigations and Protecting Victims - A Blueprint for Action* (Education Development Center, Inc., 1995)

*Hiring the Right People: Guidelines for the Screening and Selection of Youth-Serving Professionals and Volunteers* (Missing and Exploited Children Comprehensive Action Program/Public Administration Service and the National School Safety Center, 1994).

*Investigation and Prosecution of Child Abuse, second edition* (American Prosecutors Research Institute, 1993).

*Law Enforcement Policies and Practices Regarding Missing Children and Homeless Youth* (Research Triangle Institute, 1993) NCJ 145644.

*Missing, Abducted, Runaway, and Thrownaway Children in America, First Report: Numbers and Characteristics. National Incidence Studies (Full Report and Executive Summary)* (1990), NCJ 123668.

*Missing and Abducted Children: A Law Enforcement Guide to Case Investigation and Program Management* (National Center for Missing and Exploited Children, 1994), NCJ 151268.

*National Center for Missing and Exploited Children* (OJJDP Fact Sheet, 1995).

*Obstacles to the Recovery and Return of Parentally Abducted Children* (American Bar Association, 1993), NCJ 144535.

*Obstacles to the Recovery and Return of Parentally Abducted Children: Research Summary* (American Bar Association, 1994), NCJ 143458.

*Parental Kidnaping* (OJJDP Fact Sheet, 1995).

*Parental Kidnaping, Domestic Violence, and Child Abuse: Changing Legal Responses to Related Violence* (American Prosecutor's Research Institute, 1995).

*Portable Guides to Investigating Child Abuse: An Overview* (Office of Juvenile Justice and Delinquency Prevention, 1997), NCJ 165153.

*Sharing Information: A Guide to the Family Educational Rights and Privacy Act* (1997).

*Using Agency Records To Find Missing Children: A Guide for Law Enforcement* (1995), NCJ 154633.

## **Videos**

"Conducting Sensitive Child Abuse Investigations" is a six series video that was produced in 1996 by the Missing and Exploited Children's Program in conjunction with the National Child Welfare Resource Center, Edmund S. Muskie Institute of Public Affairs, University of Southern Maine.

## **Agency Contact**

For further information about services, contact:

Missing and Exploited Children's Program  
Office of Juvenile Justice and Delinquency Prevention  
810 7th Street, NW.  
Washington, DC 20531  
Telephone: (202) 616-3637  
Fax: (202) 307-2819

# U.S. Department of Justice

## U.S. Immigration and Naturalization Service

### Agency Description

The Inspections Program of the U.S. Immigration and Naturalization Service (INS) controls and guards the boundaries and borders of the United States at designated Ports-of-Entry (POEs) against the illegal entry of aliens to protect the health, welfare, safety, and security of the public and the nation. Under authority granted by the Immigration and Nationality Act (INA), as amended, an immigration inspector may question any person coming into the United States to determine his or her admissibility. In addition, an inspector has authority to search without warrant the person and effects of any person seeking admission, if there is reason to believe that grounds of exclusion exist which may be disclosed by such search. The INA is based on the law of presumption - an applicant for admission is presumed to be an alien until he or she shows evidence of citizenship, and an alien is presumed to be an immigrant until he or she proves that he or she fits into one of the nonimmigrant classifications.

Persons seeking entry into the United States are inspected at POEs by Immigration Inspectors who determine their admissibility. Inspectors are responsible for determining the nationality and identity of each applicant for admission. United States citizens are automatically admitted on verification of citizenship. Aliens' documents are reviewed to determine admissibility based on the requirements of the U.S. immigration law. Because of this unique status, the Immigration Inspector is usually the first U.S. official encountered by travelers who seek to enter the United States. Within this context, the INS is ideally situated to assist in preventing the movement of missing children across U.S. borders.

### Services

Services provided by the INS include:

- Training for common carriers to improve ability of personnel to identify missing or exploited children.
- Interdiction of missing children at United States Ports-of-Entry, when encountered.
- Information dissemination to the public.

### Availability of Services

Services available from the INS are directed to law enforcement officials and selected travel industry personnel. Services can be obtained by contacting the INS Office of Inspections.

## **Agency Contact**

For further information about services, contact:

U.S. Immigration and Naturalization Service  
Office of Inspections (HQINS)  
425 I Street NW  
Washington, DC 20536  
Telephone: (202) 514-3019  
Fax: (202) 514-8345  
After Hours: (202) 616-5000 (INS Command Center, 7 x 24)

# U.S. Department of Justice

## U.S. National Central Bureau (INTERPOL)

### Agency Description

INTERPOL is the international criminal police organization that comprises designated national central bureaus (NCB's) from the law enforcement agencies of its 177 member nations. The primary mission of INTERPOL is:

- (a) To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the 'Universal Declaration of Human Rights.'
- (b) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes.

By law, INTERPOL is forbidden to undertake any intervention or activities of a political, military, religious, or racial character.

INTERPOL maintains a sophisticated global communications network to coordinate international criminal investigations among its member countries. This network is also used to relay humanitarian requests, such as missing person inquiries. INTERPOL provides a forum for discussions, organizes working group meetings, and stages symposia for law enforcement authorities of member nations to focus attention on specific areas of criminal activity affecting their countries.

### Services

Each INTERPOL member country establishes, funds, and staffs a national central bureau, which serves as the point of contact for the international law enforcement community. Every NCB operates within the parameters of its own nation's law and policies and within the framework of the INTERPOL constitution. In the U.S., authority for the INTERPOL function rests with the Attorney General. Authority for administering the U.S. National Central Bureau (USNCB) is shared by the Departments of Justice and Treasury.

The mission of USNCB is twofold:

- To receive foreign requests for criminal investigative assistance and direct them to the appropriate U.S. Federal, State, or local law enforcement or judicial authorities.

- To receive domestic law enforcement requests and direct them to the appropriate NCB abroad.

The USNCB's coordinative services provide Federal, State, and local law enforcement authorities with the most effective means available to secure the assistance of foreign police in matters ranging from a criminal record check to the arrest and extradition of wanted persons.

The USNCB investigative staff includes senior agents who are detailed from more than 16 Federal and State law enforcement agencies and a permanent analytical staff. Agents and analysts work in five investigative divisions: alien/fugitive, criminal, drugs, financial fraud and economic crimes, and State liaison. Cases involving the exploitation of minors are assigned to one of these divisions, depending on the nature of the offense. For example, the Fraud Division investigates sexual abuse against minors, sexual assault against minors, child pornography, and sexual tourism. The Criminal Division is responsible for cases involving missing persons, parental kidnaping, and child abduction.

Through INTERPOL's worldwide telecommunications network, messages can be directed to one country, to an entire region, or to the whole INTERPOL membership. Messages destined for regional or worldwide distribution are referred to as "diffusions." Diffusions inform other NCB's of the circumstances of a case and request their assistance or intervention.

If information is not obtained from other NCB's as a result of a diffusion message, the originating agency can request that a formal notice be issued for worldwide distribution through the INTERPOL Secretariat General Office. INTERPOL notices are categorized (color-coded) according to the circumstances surrounding the request.

- International Red Notices request a subject's provisional arrest with a view toward extradition. A Red Notice provides specific details concerning charges against a subject, along with warrant information, and includes prior criminal history.
- International Blue Notices are designed to collect information about persons. For example, to trace and locate a subject whose extradition may be requested.
- International Yellow Notices are circulated to provide information about persons who are missing, abducted or who are unable to identify themselves, such as children.

Upon receipt of these notices, most member countries enter the information into their databases and border lookout systems.



## Availability of Services

### *Requests for Assistance*

To reach the international law enforcement community, USNCB enters information on the child-related crime, subject, victim, abducting parent, or missing child(ren) into the INTERPOL network. Requests can be made immediately following the incident, but they must be made by a U.S. law enforcement agency or judicial authority (see appendix 8 for a listing of USNCB - State Liaison offices). The USNCB **cannot** accept requests for assistance from members of the public, including a victim parent.

Virtually every request normally handled through law enforcement channels can be accommodated by INTERPOL, provided communication is needed within the international law enforcement community. Generally, correspondents on INTERPOL messages are the law enforcement authorities in the respective member countries.

Responses to inquiries are sent to the originating law enforcement agency. Interested parties, such as a victim parent, can ask for a status report directly from the originating law enforcement agency.

When a request is received, a USNCB analyst will search the internal case tracking system to determine if there is any prior correspondence regarding the principals in the investigation. Additional searches will be conducted on a wide range of internal and external computer databases to determine if there are any records that will disclose prior investigative information or if there is any information that will help to locate a missing or abducted child and/or the abducting parent.

A determination is then made as to what action should follow, and a message is usually sent to one or more foreign NCB's through the INTERPOL communications network by the agent or analyst. Because local customs, policies, and laws dictate what the receiving NCB can and will do, USNCB has little or no control over how a message will be handled by a foreign NCB. Most requests from U.S. police entail interviewing witnesses, victims, or subjects of child exploitation crimes who reside in foreign countries or concern efforts to locate missing or abducted children and/or abductors.

### *Domestic Child Abduction Cases*

In domestic child abduction cases, the initial request seeks to confirm if border-entry records can establish the presence of the abductor or the child in the foreign country. Once entry has been established, discreet verification is requested to confirm the exact location of the abductor in the hope of preventing that person from fleeing to another location.

If an NCB confirms the location of an offender, abductor, or child, USNCB notifies the originating police agency, which then coordinates subsequent investigative or retrieval efforts with the prosecuting attorney or the victim parent via the Department of State, Office of Children's Issues. If USNCB messages fail to locate an offender, abductor, or child, USNCB helps the originating

agency complete the application process that will lead to the publication of INTERPOL international notices.

If a child is located abroad, INTERPOL may request protective custody of the child, even in countries that are party to the Hague Convention treaty.

If a subject is charged with a child exploitation offense or parental kidnaping, a request for provisional arrest with a view toward extradition must be sent first through the proper diplomatic channels. Cases resulting in extradition are handled by the Department of Justice's Office of International Affairs, which uses the INTERPOL channel to transmit information pertaining to the extradition process.

### ***Foreign Requests for Assistance***

Foreign requests for investigative assistance are handled similarly to domestic cases. USNCB agents or analysts query various law enforcement databases--including the NCIC--to determine whether prior investigative information exists in the United States. The investigative request is then forwarded to the appropriate Federal or State police authority and, oftentimes, is coordinated with NCMEC. The results of such investigative actions are then routed back to USNCB for relay to the requesting country. If another NCB requests such action, USNCB can initiate a border-lookout notice using the Treasury Enforcement Communications System (TECS) database. Such a notice would request that INTERPOL be notified if the subject and/or missing/abducted child(ren) were to attempt to enter the United States.

In foreign origin abduction cases, the names of the abductor and of the child cannot be entered into the NCIC computer system unless a Red Notice has been issued for the abductor and a Yellow Notice for the child. In some cases USNCB can enter the victim child's name into NCIC without the existence of a Yellow Notice, but all efforts to locate the child must have been exhausted previously, and the request for such entries must be made by the National Center for Missing and Exploited Children.

### **Agency Contact**

For further information about services, contact:

U.S. National Central Bureau (INTERPOL)  
U.S. Department of Justice  
Bicentennial Building Room 600  
600 E Street NW.  
Washington, DC 20530  
Telephone: (202) 616-9000  
Fax: (202) 616-8400  
NLETS: DCINTER00

# U.S. Department of State

## Office of Children's Issues

### Agency Description

The Office of Children's Issues (CI) is located in the Overseas Citizens Services, Bureau of Consular Affairs, U.S. Department of State. CI formulates, develops, and coordinates policies and programs and provides direction to foreign service posts on international parental child abduction and international adoption. CI also fulfills U.S. treaty obligations relating to international parental abduction of children.

### Services

The Office of Children's Issues provides services in two areas: international parental child abduction and international adoption.

#### *International Abduction*

CI works closely with parents, attorneys, private organizations, and government agencies in the United States and abroad to prevent and resolve international parental child abductions. Since the late 1970's, the Bureau of Consular Affairs has taken action in more than 8,000 cases of international parental child abduction. In addition, the Office has answered thousands of inquiries concerning international child abduction, enforcement of visitation rights, and abduction prevention techniques.

CI acts as the U.S. Central Authority for the operation and implementation of the Hague Convention on the Civil Aspects of International Child Abduction. Forty-seven countries, including the United States, have joined the Hague Abduction Convention. The Convention discourages abduction as a means of resolving a custody matter by requiring, with a few limited exceptions, that the abducted child be returned to the country where he or she resided prior to the abduction. About 60 percent of applications for assistance under the Hague Abduction Convention involve children abducted from the United States and taken to other countries, and 40 percent involve children who were abducted in other countries and brought to the United States. The countries with the most abduction cases are, in descending order, Mexico, United Kingdom, Canada, Germany, and France. These five countries account for about half of the abduction cases in which CI becomes involved.

Many countries have not yet accepted the Hague Convention. In 1996 CI handled the cases of more than 250 children who were abducted to non-Hague countries. In the event of an abduction to a non-Hague country, one option for the left-behind parent is to obtain legal assistance in the country where the child was taken and to follow the local judicial process. Of non-Hague countries, the

largest number of cases have involved children taken to Egypt, Japan, Jordan, the Philippines, and Saudi Arabia.

For international abduction cases, CI can:

- Provide information in situations where the Hague Convention applies and help parents file an application with foreign authorities to obtain the return of or access to the child.
- Contact U.S. Embassies and consulates abroad and request that a U.S. Consul Officer attempt to locate, visit, and report on a child's general welfare.
- Provide the left-behind parent with information on the legal system, especially concerning family law, of the country to which the child was abducted and furnish a list of attorneys willing to accept American clients.
- Monitor judicial or administrative proceedings overseas.
- Help parents contact local officials in foreign countries or make contact with such officials on the parent's behalf.
- Inform parents of domestic remedies, such as warrants, extradition procedures, and U.S. passport revocations.
- Alert foreign authorities to any evidence of child abuse or neglect.

CI cannot re-abduct a child, help a parent in any way that violates the laws of another country, or give refuge to a parent who is involved in re-abduction. CI also cannot act as a lawyer, represent parents in court, or pay legal expenses or court fees.

### ***International Adoption***

CI offers general information and assistance regarding the adoption process in more than 60 countries. In 1996 U.S. citizens adopted more than 11,000 foreign-born children. Because adoption is a private legal matter within the judicial sovereignty of the Nation where the child resides, the Department of State cannot intervene on behalf of an individual U.S. citizen in foreign courts.

For international child adoption cases, CI can:

- Provide general information about international adoption in countries around the world.
- Provide general information on U.S. visa requirements for international adoptions.
- Make inquiries regarding the status of specific adoption cases and clarify documentation and other requirements to the U.S. consulate abroad.

- Make efforts to ensure that U.S. citizens are not discriminated against by foreign authorities or court personnel.

CI cannot become directly involved in the adoption process in another country, cannot act as an attorney or represent adoptive parents in court, and cannot order that an adoption take place or that a visa be issued.

## **Availability of Services**

### ***International Abduction***

In cases involving international abduction, services are directed to the parents or the attorneys of children who have been abducted internationally or to those who fear a child may be abducted by another parent abroad. CI promotes the use of civil legal mechanisms to resolve international parental abduction cases. CI also works closely with local and Federal law enforcement agencies, the Department of Justice, and the Department of State Advisors Office, all of which pursue criminal remedies to international parental abduction cases.

General information on international parental child abduction and custody issues is available to any interested person. As the U.S. Central Authority for the Hague Convention on the Civil Aspects of International Child Abduction, CI processes applications from parents seeking access to and the return of abducted children under the Convention. CI coordinates U.S. government assistance in cases involving children abducted abroad. CI works closely with U.S. Embassies and Consulates, and foreign Hague Convention Central Authorities to help resolve international parental child abduction cases. The International Child Remedies Act (52 U.S.C. 11601; P.L. 100-300; 22 CFR Part 94) is the Federal legislation implementing the Hague Abduction Convention in the United States. A Memorandum of Understanding signed by the Departments of State and Justice and by the National Center for Missing and Exploited Children gives NCMEC the authority to process Hague abduction cases involving children taken to the United States.

Although the Convention does not require that requests for services be in the form of an application, CI has created a special form (DSP-105), "Application for Assistance Under the Hague Convention on Child Abduction," to help organize information (see appendix 9). It should be noted that CI does not adjudicate the validity of the application claim for the return of or access to a child; rather, CI provides information on the operation of the treaty and on the issues that the appropriate judicial or administrative body that reviews the application will consider in making a determination.

### ***International Adoption***

International adoption services provided by CI are directed to parents seeking to adopt abroad, to agencies involved in international adoption, and to U.S. Embassies or consulates abroad that provide information on the local adoption situation and that issue visas to children to enter the United States. Most services are accessed when a parent calls CI or uses the automated information

system. Any individual, agency, or group wanting information on international adoption may contact CI to obtain information.

Under guidance from CI, Embassies and consulates monitor and report changes in local adoption procedures that may affect U.S. citizens wishing to adopt abroad. The Embassies also inform other governments of the effect that their laws, regulations, and procedures have on Americans who wish to adopt a child who resides in that country.

## **Agency Contact**

For further information about services, contact:

Office of Children's Issues  
Room 4811  
Overseas Citizens Services  
Bureau of Consular Affairs  
U.S. Department of State  
Washington, DC 20520-4818  
Telephone: (202) 736-7000  
Fax: (202) 647-2835  
Autofax: (202) 647-3000  
Consular Affairs Electronic Bulletin Board: (202) 647-9225 (modem number)  
Internet Address: <http://travel.state.gov>

# U.S. Department of Treasury

## U.S. Customs Service

### Agency Description

The U.S. Customs Service is on the frontline of the Nation's defense against the illegal importation and trafficking of child pornography. Long recognized by both the domestic and international law enforcement communities for its knowledge of and skill in the area of child pornography investigations, the U.S. Customs Service aggressively targets importers, distributors, and purveyors of child pornography to prevent the sexual exploitation and abuse of children both in the United States and abroad. The U.S. Customs Service Child Pornography Enforcement Program works closely with the FBI, the Department of Justice's Child Exploitation and Obscenity Section, the U.S. Postal Inspection Service, and the National Center for Missing and Exploited Children.

Through an agreement with NCMEC, the U.S. Customs Service Child Pornography Enforcement Program has assumed primary responsibility for all NCMEC child pornography-related complaints. NCMEC has established a national toll-free child pornography Tipline (1-800-THE LOST, or 1-800-843-5678) for the reporting of information regarding child pornography. NCMEC refers such data directly to the Child Pornography Enforcement Program for dissemination to the appropriate field offices.

### Services

- Training for law enforcement officers who are involved in child pornography investigations.
- Investigative support for child pornography investigations.
- Information dissemination to the public.

### Availability of Services

Services available through the U.S. Customs Service are directed to law enforcement officials, investigators, and parents involved in cases of child pornography. Services can be accessed by contacting the nearest Customs Service office (see appendix 10).

A training course curriculum is available through the training center in Atlanta, Georgia. All training courses are coordinated through local Customs Service offices (see appendix 10).

## **Agency Contact**

For further information about services, contact:

U.S. Customs Service  
International Child Pornography Investigation and Coordination Center  
45365 Vintage Park Road, Suite 250  
Sterling, VA 20166  
Telephone: (703) 709-9700, ext. 353  
Fax: (703) 709-8286



# U.S. Department of Treasury

## U.S. Secret Service Forensic Services Division

### Agency Description

Under Title XXXI of the Violent Crime Control and Law Enforcement Act of 1994, the U.S. Secret Service is mandated to work with the National Center for Missing and Exploited Children to provide forensic and technical assistance to State and local authorities in investigating the most difficult cases of missing and exploited children.

### Services

Services provided by the U.S. Secret Service include access to the following:

- The Forensic Information System for Handwriting (FISH) database, which allows handwritten or handprinted material to be searched against previously recorded writings, making possible links or consolidations.
- The Automated Fingerprint Identification System (AFIS), a nationwide network with access to the largest collection of automated fingerprint databases in the United States.
- Polygraph examinations, to help detect deception through physiological means, resulting in investigative leads.
- Visual information services, such as image enhancement, age progression and regression, suspect drawings, video and audio enhancement, and graphic and photographic support.

### Availability of Services

Services are directed to local, State, and Federal law enforcement investigators who deal with cases involving missing children, runaways, parental abductions, international abductions, sexual tourism, and child pornography. Services are available at the discretion of the investigating agency when a missing or exploited child case is involved.

### Publications

Publications include two brochures: the *Forensic Services Division* brochure, and the *U.S. Secret Service, Forensic Services Division, National Center for Missing and Exploited Children* brochure.

## **Agency Contact**

Further information about services may be obtained from any local Secret Service field office or from:

U.S. Secret Service  
Forensic Services Division  
1800 G Street NW.  
Suite 929  
Washington, DC 20223  
Telephone: (202) 435-5926  
Fax: (202) 435-5603

National Center for Missing and Exploited Children  
2101 Wilson Boulevard  
Suite 550  
Arlington, VA 22201-3052  
Hotline: 1-800-THE-LOST (1-800-843-5678)  
Telephone: (703) 235-3900  
Fax: (703) 235-4067

# **U.S. Postal Service**

## **U.S. Postal Inspection Service**

### **Agency Description**

The U.S. Postal Inspection Service is the law enforcement arm of the U.S. Postal Service with responsibility for investigating crimes involving the U.S. mail, including all child pornography and child sexual exploitation offenses. Specially trained postal inspectors are assigned to each of the 28 field divisions nationwide (see appendix 11). As Federal law enforcement agents, U.S. postal inspectors carry firearms, serve warrants and subpoenas, and possess the power of arrest.

Recognizing that child molesters and child pornographers often seek to communicate with one another through what they perceive as the security and anonymity provided by the U.S. mail, postal inspectors have been involved extensively in child sexual exploitation and pornography investigations since 1977. Since the Federal Child Protection Act of 1984 was enacted, postal inspectors have conducted more than 2,800 child pornography investigations, resulting in the arrest and conviction of more than 2,500 child pornographers and preferential child molesters.

### **Services**

Postal inspectors in the United States use an established, nationwide network of intelligence to implement a wide variety of undercover programs designed to identify suspects and develop prosecutable cases. These undercover operations recognize the clandestine nature of their targets and the inherent need of many offenders to validate their behavior. The techniques used in these programs include placement of contact advertisements in both local and national publications, written contacts and correspondence with the subject, and more recently, contact via computer networks and the Internet. Postal inspectors are ready to assist in any related investigation involving child sexual exploitation.

### **Availability of Services**

Investigative assistance by the Postal Inspection Service is available and should be sought under the following circumstances:

- When a subject may be using the U.S. mail to exchange, send, receive, buy, loan, advertise, solicit, or sell child pornography.
- When a subject is believed to be using the U.S. mail to correspond with others concerning child sexual exploitation, child pornography, or child erotica.

- When a subject is believed to be using a computer network or bulletin board to exchange child pornography or child erotica or to correspond with others concerning child sexual exploitation, and the actual exchange or initial contact may involve the U.S. mail.
- When a subject is believed to be clearly predisposed to receive or purchase child pornography and a reverse sting investigative approach appears warranted.
- When there is a need to execute a controlled delivery of child pornography.
- When the activities of a subject warrant further investigation and there is a need for assistance from a postal inspector who is trained in the investigation of child pornography or child sexual exploitation cases.
- When other local investigative leads have been exhausted and a postal inspector is needed to utilize additional resources.

Services and investigative assistance provided by the Postal Inspection Service are available to any local, State, or Federal law enforcement agency. Contact the nearest office of the U.S. Postal Inspection Service for further information.

## **Legislative Citations**

For over a century, the Postal Inspection Service has had specific responsibility for investigating the mailing of obscene matter (Title 18 U.S. Code, Section 1461). While over the years child pornography has been, as a matter of course, investigated along with obscenity matters, increased public concern resulted in the enactment of the Sexual Exploitation of Children Act of 1977 (Title 18 U.S. Code, Section 2251-2253). The Child Protection Act of 1984 (18 U.S.C. 2251-2255) amended the 1977 Act by:

- ▶ Eliminating the obscenity requirement.
- ▶ Eliminating the commercial transaction requirement.
- ▶ Changing the definition of a minor from a person under age 16 to one under age 18.
- ▶ Adding provisions for criminal and civil forfeiture.
- ▶ Amending the Federal wiretap statute to include the Child Protection Act.
- ▶ Raising the potential maximum fines from \$10,000 to \$100,000 for an individual and to \$250,000 for an organization.

On November 7, 1986, Congress enacted the Child Sexual Abuse and Pornography Act (18 U.S.C. 2251-2256), which amended the two previous acts by:

- ▶ Banning the production and use of advertisements for child pornography.
- ▶ Adding a provision for civil remedies of personal injuries suffered by a minor who is a victim.
- ▶ Raising the minimum sentence for repeat offenders from imprisonment of not less than 2 years to imprisonment of not less than 5 years.

On November 18, 1988, Congress enacted the Child Protection and Obscenity Enforcement Act (18 U.S.C. 2251-2256), which:

- ▶ Made it unlawful to use a computer to transmit advertisements for or visual depictions of child pornography.
- ▶ Prohibited the buying, selling, or otherwise obtaining temporary custody or control of children for the purpose of producing child pornography.

On November 29, 1990, Congress amended 18 U.S.C. 2252, making it a Federal crime to possess three or more depictions of child pornography that were mailed or shipped in interstate or foreign commerce or that were produced using materials that were mailed or shipped by any means, including by computer.

Most recently, a new criminal statute was enacted with the passage of the Telecommunications Act of 1996. Title 18 U.S.C. 2422 makes it a Federal crime for anyone using the mail, interstate or foreign commerce, to persuade, induce, or entice any individual under the age of 18 years to engage in any sexual act for which the person may be criminally prosecuted.

## **Agency Contact**

For further information about the U.S. Postal Inspection Service, contact:

U.S. Postal Inspection Service  
Office of Criminal Investigations  
475 L'Enfant Plaza West SW.  
Room 3141  
Washington, DC 20260-2166  
Telephone: (202) 268-4286  
Fax: (202) 268-4563



---

---

## **ORGANIZATIONS**

---

---





# **National Center for Missing and Exploited Children**

## **Agency Description**

The mission of the National Center for Missing and Exploited Children (NCMEC) is to assist in the location and recovery of missing children and to prevent the abduction, molestation, sexual exploitation, and victimization of children. A private, nonprofit organization established in 1984, NCMEC operates under a congressional mandate in a cooperative agreement with the Department of Justice's Office of Juvenile Justice and Delinquency Prevention. The goal is to coordinate the efforts of law enforcement personnel, social service agency staff, elected officials, judges, prosecutors, educators, and members of the public and private sectors to break the cycle of violence that historically has perpetuated crimes against children.

## **Services**

NCMEC offers a variety of services to aid in the search for a missing child, including a toll-free hotline; technical case assistance; a national computer network; photograph and poster distribution; age-enhancement, facial reconstruction, and imaging-identification services; a resource directory of nonprofit organizations; recovery assistance; and international case assistance.

### ***Toll-Free Hotline***

One of NCMEC's primary activities is its toll-free hotline: 1-800-THE-LOST (1-800-843-5678). The multilingual hotline, which is available throughout the United States, Canada, and Mexico, operates every day of the year, 24 hours a day. It is used by individuals to report the location of a missing child or of other children whose whereabouts are unknown to the child's legal custodian and to learn about the procedures necessary to reunite a child with the child's legal custodian. Reports of missing children are entered immediately into a national missing child database. Reports of sightings of missing children are disseminated directly to the investigative agency handling the case.

### ***Technical Case Assistance***

Trained case managers assist citizens and law enforcement officials in filing missing person reports, verify data concerning missing children that have been entered into the FBI's NCIC computer system, and send publications designed to enhance the investigative skills of agency personnel involved in missing child cases.

### ***National Computer Network and Online Services***

NCMEC is linked via computer online services to 50 State clearinghouses plus the District of Columbia, the U.S. Department of State Office of Children's Issues, the U.S. National Central Bureau (INTERPOL), the U.S. Secret Service Forensic Services Division, and other Federal

agencies. Internationally, NCMEC is linked to the Australian Police, the Belgium Police, the Netherlands Police, the Royal Canadian Mounted Police, New Scotland Yard, Mexican government contacts, and others. These computer links allow images of and information on missing and exploited children to be transmitted instantly.

In addition, NCMEC has taken the search for missing children to the Internet with the creation of the Missing Children Web Page. This free, publicly available channel allows Internet users to search a database for information on current missing children cases, to view images of missing children, and to obtain safety and resource information. The NCMEC Missing Children Web Page can be found at <http://www.missingkids.com>.

### ***Photograph and Poster Distribution***

NCMEC maintains an up-to-date library of missing children posters on the Internet, CompuServe, and the State Clearinghouse bulletin-board computer network. The organization also places missing child kiosks in high-traffic areas, such as airports and shopping malls. NCMEC simultaneously transmits posters and other case-related information to more than 9,000 law-enforcement agencies throughout the Nation through a broadcast fax dissemination service. NCMEC coordinates national media exposure of missing children cases, including public service announcements for breaking cases. Through a network of private-sector partners that includes major corporations, television networks, and publishers, NCMEC has distributed millions of photographs of missing children.

### ***Age-Enhancement, Facial Reconstruction, and Imaging-Identification Services***

Supported by forensic specialists and computer industry leaders, NCMEC provides computerized age-progression of photographs of long-term missing children, reconstructs facial images from morgue photographs of unidentified deceased individuals, provides assistance in the creation of artist composites, and trains forensic artists in imaging applications and techniques.

### ***Resource Directory of Nonprofit Organizations***

NCMEC maintains a list of nonprofit organizations located throughout the United States, Canada, and Europe that provide direct services (as stipulated by the Missing Children's Assistance Act) to families of missing and exploited children. This directory is provided as a public service to individuals who are looking for a resource group to help with a missing or exploited child case.

### ***Recovery Assistance***

Through NCMEC, several corporations provide lodging and transportation to custodial parents who are recovering their missing children. This service is available to parents or guardians who cannot afford such expenses themselves, provided that established criteria and guidelines are met. To find out if a particular case meets these criteria, call the NCMEC hotline.

### ***International Case Assistance***

NCMEC acts on behalf of the U.S. Central Authority in the handling of applications seeking the return of or access to children abducted in the United States. This assistance is provided in compliance with the Hague Convention of the Civil Aspects of International Child Abduction. NCMEC also handles outgoing international abductions.

### ***CyberTipline***

Through support from the U.S. congress, NCMEC operates a Federally-mandated CyberTipline aimed at reducing crimes against children occurring on the Internet. Families are encouraged to call its national tollfree hotline at 1-800-843-5678 to report incidences involving child sexual exploitation including online enticement of children for sexual acts; information on the possession, manufacture, or distribution of child pornography; child prostitution; and child-sex tourism. Leads received are immediately forwarded directly to the U.S. Customs Service's Child Pornography Enforcement Program, the U.S. Postal Inspection Service, and the U.S. Department of Justice's Federal Bureau of Investigation. Additionally, online users can report information on the same topics via the Internet. For more information, visit the CyberTipline section of NCMEC's web site at [www.missingkids.com/cybertip](http://www.missingkids.com/cybertip).

### ***Exploited Child Unit (ECU)***

The ECU was created to combat child molestation, pornography and prostitution and raise awareness about child exploitation both nationally and internationally. The ECU seeks to generate leads in cases of child exploitation and forward them to the appropriate investigative agencies; provide technical assistance in these cases to State and local law enforcement; develop tools and resources to assist in the investigation of these cases; and increase awareness about the problem of child exploitation among law enforcement and the general public.

Funding for the ECU is provided by the U.S. Department of the Treasury. Additional partners in this effort include the U.S. Department of Justice and the U.S. Postal Service.

### ***Jimmy Ryce Law Enforcement Training Center***

NCMEC, OJJDP, and the FBI have established the Jimmy Ryce Law Enforcement Training Center, housed at NCMEC. Named for a 9-year old boy abducted and murdered out of South Florida, this training and technical assistance program is designed to enhance the investigative response to missing children cases. The Training Center provides training to senior-level law enforcement officers and is broken down into three areas: a two-day intensive seminar for law enforcement officers that focuses on research and policy issues; a five-day regional training that emphasizes investigative resources for local law enforcement working these cases; and two-day training for State control terminal officers on the new National Crime Information Center flagging system that immediately alert NCMEC and the FBI to highly endangered cases.

In addition, the following services are available to law enforcement agencies:

- **Informational Analysis Services.** NCMEC receives thousands of leads and provides law enforcement officials with the most usable, relevant information possible. NCMEC prioritizes its leads and identifies similar patterns in cases across the country, helping to tie cases together and coordinate investigations.
- **Queries and Database Searches.** Through its networked database, NCMEC can search active missing child cases using any series of identifiers. NCMEC also has access to a number of national informational databases, including employment records, motor vehicle records, telephone listings, school registrations, and the Federal Parent Locator Service.
- **Project ALERT (America's Law Enforcement Retiree Team).** Fourteen national law enforcement associations work with NCMEC to provide free onsite assistance by volunteer retired police officers. This project allows hardpressed local police involved in difficult missing or exploited child cases to benefit from the expertise of the retired officers.

Working closely with crime prevention officers, NCMEC reaches out to the general public with positive, effective child-safety information and services, including:

***KIDS AND COMPANY: Together for Safety***, a state-of-the-art personal safety curriculum for children in kindergarten through grade six.

**Project KidCare**, a campaign to ensure that parents have a current photograph as well as descriptive information of their child. A list of safety tips is included in the passport-like booklet.

**Kidprint**, a program through which families can obtain a free videotape of their child.

## **Availability of Services**

Services provided by NCMEC are directed to:

- Parents and families of missing and exploited children.
- Local, State, and Federal law enforcement investigators and agencies handling cases of missing and exploited children.
- Child care staff, child protection and social service personnel, criminal justice professionals, and legal practitioners who work with missing and exploited children and their families.
- Nonprofit organizations that seek access to a national network of resources and information.

- Members of the general public who have an interest in child safety.

Services are provided for:

- ▶ Cases of missing children, including endangered runaways; victims of family and nonfamily abduction; and those who have been lost, injured, or are otherwise missing.
- ▶ Reports of sightings of missing children.
- ▶ Other cases handled by law enforcement agencies that involve the victimization and possible exploitation of children.
- ▶ Reports of child exploitation and child pornography.

For **parents** of missing children, cases are taken in through the hotline when it has been determined that: (1) the child was younger than 18 years of age at the time of disappearance, (2) a missing child report has been filed with the police, and (3) the parent reporting the case has court-awarded custody of the child, unless otherwise noted. These cases include:

- **Voluntary missing (runaway) cases**, which can be taken immediately by NCMEC when the child is 13 or younger or when specific conditions indicate that the child is endangered, such as the existence of a life-threatening medical condition, a serious mental illness, a substance abuse problem, or a belief that the child is with a potentially dangerous individual or in a potentially dangerous situation.
- **Family abduction cases**, which are taken by NCMEC when it is determined that the parent reporting the case has court-awarded custody of the child and that the child's whereabouts are unknown.
- **International family abduction cases**, which are taken by NCMEC when it is believed that the child has been taken out of or brought into the United States and when the child's whereabouts are unknown, or when a child has been brought into the United States and the left-behind parent has made appropriate applications to invoke the Hague Convention on the Civil Aspects of International Child Abduction.
- **Nonfamily abduction cases**, which may involve kidnaping by a stranger or by an acquaintance.
- **Other cases**, in which the facts are insufficient to determine the cause of a child's disappearance. The criteria for intake of a "lost, injured, or otherwise missing" child are the same as for a nonfamily abduction.

For **law enforcement professionals**, requests for resources, technical assistance, and access to NCMEC's database may be obtained by contacting NCMEC's hotline or case management department. All services are free of charge.

For **callers reporting a sighting** of a missing child, the NCMEC hotline will obtain complete information concerning the individual involved and the circumstances surrounding the sighting. A report will be distributed to law enforcement officials.

For **callers reporting specific information concerning child pornography**, the NCMEC hotline also serves as the National Child Pornography Tipline. Reports of alleged child sexual exploitation, including child pornography and prostitution, are forwarded to the U.S. Customs Service, the U.S. Department of Justice, or to the U.S. Postal Inspection Service for verification and investigation.

For **callers reporting instances of possible sexual exploitation**, NCMEC acts as a referring agency and may provide technical assistance, but it does not formally handle such cases. Requests for services in cases of child sexual abuse, incest, and molestation are referred to appropriate law enforcement and child protection agencies.

The resources and services listed above are available to parents of missing children once they have filed a missing person report with the police. There is no waiting period for or time limitation on these services. All other calls and requests for information may be made at any time to NCMEC's hotline. Free publications on child protection and prevention are available upon request.

## **Resources**

### ***Technical Assistance***

*Safeguard Their Tomorrows* is a 4-hour nationally accredited educational program for health care professionals designed to address the prevention and investigation of infant abductions. The program was produced by Mead-Johnson Nutritionals in cooperation with the Association of Women's Health, Obstetric, and Neonatal Nurses; the National Association of Neonatal Nurses; and NCMEC.

NCMEC has joined forces with America's leading law enforcement associations to launch Project ALERT, a national program that uses retired law enforcement professionals as volunteers. Upon request by a law enforcement agency, NCMEC will assign a trained volunteer consultant to provide free, hands-on assistance to agencies struggling with missing child cases, child homicides, and child exploitation issues.

### ***Publications***

NCMEC has written and published a number of books, brochures, and pamphlets. Up to 50 copies of most brochures are available free of charge. Single copies of books are available free of charge.

Call NCMEC's hotline at 1-800-THE-LOST (1-800 843-5678) for more information about fees for bulk orders.

### **Brochures**

*Child Protection* (English/Spanish)  
*Child Safety on the Information Highway* (English)  
*For Camp Counselors* (English)  
*For Law Enforcement Professionals* (English)  
*Just in Case...Finding Professional Help in Case Your Child Is Missing or the Victim of Sexual Abuse or Exploitation* (English, Spanish, Vietnamese)  
*Just in Case...You Are Considering Daycare* (English, Spanish)  
*Just in Case...You Are Considering Family Separation* (English, Spanish, Vietnamese)  
*Just in Case...You Are Dealing With Grief Following the Loss of a Child* (English, Spanish)  
*Just in Case...You Are Using the Federal Parent Locator Service* (English, Spanish)  
*Just in Case...You Need a Babysitter* (English, Spanish)  
*Just in Case...Your Child Is a Runaway* (English, Spanish, Vietnamese)  
*Just in Case...Your Child Is Testifying in Court* (English, Spanish)  
*Just in Case...Your Child Is the Victim of Sexual Abuse or Exploitation* (English, Spanish)  
*Just in Case...Your Child May Someday Be Missing* (English, Spanish, Vietnamese)  
*My 8 Rules for Safety* (English, Spanish, Haitian, Creole, Braille )  
*National Center for Missing and Exploited Children* (English)  
*Tips to Prevent the Abduction and Sexual Exploitation of Children* (Braille)

### **Books**

*A Report to the Nation* (English)  
*An Analysis of Infant Abductions* (English)  
*Child Molesters: A Behavioral Analysis* (English)  
*Child Molesters Who Abduct: A Summary of the Case-in-Point Series* (English)  
*Child Sex Rings: A Behavioral Analysis* (English)  
*Children Traumatized in Sex Rings* (English)  
*Family Abduction Guide* (English, Spanish)  
*Female Juvenile Prostitution: Problem and Response* (English)  
*For Health Care Professionals: Guidelines on Prevention of and Response to Infant Abduction* (English)  
*Missing and Abducted Children: A Law Enforcement Guide to Case Investigation and Program Management* (English)  
*My 8 Rules for Safety: Multilingual Child Safety and Prevention Tips* (23 languages)  
*Nonprofit Service Provider's Handbook* (English)  
*Recovery and Reunification of Missing Children: A Team Approach* (English)  
*Selected State Legislation* (English)

Also available is a resource list of nonprofit organizations throughout the United States, Canada, and Europe that work on missing and exploited child issues in their communities.

## **Legislative Citations**

*42 U.S.C. §§ 5771 and 5780.* The National Center for Missing and Exploited Children was established in 1984 as a private, nonprofit organization to serve as a clearinghouse of information on missing and exploited children, to provide technical assistance to citizens and to law enforcement agencies, to offer training programs to law enforcement and social service professionals, to distribute photographs and descriptions of missing children, to coordinate child protection efforts with the private sector, to network with nonprofit service providers and State clearinghouses on missing person cases, and to provide information on effective State legislation to ensure the protection of children. Working in conjunction with the U.S. Postal Inspection Service, the U.S. Customs Service, and the U.S. Department of Justice, NCMEC serves as the National Child Pornography Tipline.

## **Contact Information**

For information about the services provided by NCMEC, contact:

National Center for Missing and Exploited Children

2101 Wilson Boulevard, Suite 550

Arlington, VA 22201-3052

Hotline: 1-800-THE-LOST (1-800-843-5678), for the United States, Canada, and Mexico

Telephone (Business): (703) 235-3900

TTD: 1-800-826-7653

Fax: (703) 235-4067

World Wide Web: <http://www.missingkids.com>

Internet e-mail: [77431.177@Compuserve.com](mailto:77431.177@Compuserve.com)

CyberTipline: <http://www.missingkids.com/cybertip>.



# Appendix 1

## Department of Defense Investigative Liaisons for Law Enforcement Agencies

### Army

#### *Criminal Investigation Command*

CIOP-CO  
6010 Sixth Street  
Fort Belvoir, VA 22060-5506  
Telephone: (703) 806-0305  
Fax: (703) 806-0307

#### *Criminal Investigation Division District Offices*

##### **Area: Georgia**

Fort Benning District  
Third Military Police Group (CID)  
Building 1698  
Fort Benning, GA 31905-6200  
Telephone: (706) 545-8921  
Fax: (706) 545-2509

##### **Area: Hawaii**

Hawaii District  
Sixth Military Police Group (CID)  
Schofield Barracks, HI 96857-5455  
Telephone: (808) 655-2396  
Fax: (808) 655-2387

##### **Area: Kansas**

Fort Riley District  
Sixth Military Police Group (CID)  
Building 406  
Pershing Court  
Fort Riley, KS 66442-0365  
Telephone: (913) 239-3933  
Fax: (913) 239-6388

##### **Area: Kentucky**

Fort Campbell District  
Third Military Police Group (CID)  
Building 2745  
Fort Campbell, KY 42223-5637  
Telephone: (502) 798-7247  
Fax: (502) 798-2479

##### **Area: National Capital Area**

Washington, D.C., District  
Third Military Police Group (CID)  
Building 305  
Fort Meyer, VA 22211-5199  
Telephone: (703) 696-3496  
Fax: (703) 696-6270

##### **Area: New Jersey**

Fort Dix District  
Third Military Police Group (CID)  
Building 6530  
Fort Dix, NJ 08640-5780  
Telephone: (609) 562-5006  
Fax: (609) 562-5853

**Area: North Carolina**

Fort Bragg District  
10th MP Det CID Abn  
Third Military Police Group (CID)  
Building 8-1221  
Fort Bragg, NC 28307-5000  
Telephone: (910) 396-7516  
Fax: (910) 396-8607

**Area: Texas**

Fort Bliss District  
Sixth Military Police Group (CID)  
P.O. Box 6310  
Building 13  
Fort Bliss, TX 79916-6310  
Telephone: (915) 568-5905  
Fax: (915) 568-6899

**Area: Texas**

Fort Hood District  
Sixth Military Police Group (CID)  
P.O. Box V  
Fort Hood, TX 76544-5000  
Telephone: (817) 287-5039  
Fax: (817) 287-9744

**Area: Washington State**

Fort Lewis District  
Sixth Military Police Group (CID)  
P.O. Box 331009  
Fort Lewis, WA 98433-1009  
Telephone: (206) 967-7859  
Fax: (206) 967-4462

## **Navy and Marine Corps**

### *Naval Criminal Investigative Service Headquarters*

Washington Navy Yard  
Building 111 (Code 0023B)  
901 M Street SE.  
Washington, DC 20388-5383  
Telephone: (202) 433-9234  
Fax: (202) 433-4922

### *Naval Criminal Investigative Service Field Offices*

**Area:** Northern California, Colorado,  
Nevada, Utah, and Wyoming

Naval Criminal Investigative Service Field  
Office  
161 Coral Sea Street  
Naval Air Station  
Alameda, CA 94501-5085  
Telephone: (510) 273-4158  
Fax: (510) 273-7965

**Area:** Central California

Naval Criminal Investigative Service Field  
Office  
1317 West Foothill Boulevard  
Suite 120  
Upland, CA 91786  
Telephone: (908) 985-2264  
Fax: (908) 985-9763

**Area:** Southern California, Arizona, New  
Mexico, and West Texas

Naval Criminal Investigative Service Field  
Office  
Box 368130  
3405 Welles Street  
Suite 1  
San Diego, CA 92136-5050  
Telephone: (619) 556-1364  
Fax: (619) 556-0999

**Area:** Georgia, South Carolina, Central  
America, and South America

Naval Criminal Investigative Service Field  
Office  
2365 Avenue F  
Suite A  
Charleston, SC 29408-1941  
Telephone: (803) 743-3750  
Fax: (803) 743-1058

**Area:** Hawaii and Pacific Islands

Naval Criminal Investigative Service Field  
Office  
P.O. Box 122  
Pearl Harbor, HI 96860-5090  
Telephone: (808) 474-1218  
Fax: (808) 474-1210

**Area:** Maryland, Northern Virginia, and  
Washington, D.C.

Naval Criminal Investigative Service Field  
Office  
Washington Navy Yard  
Building 200  
Washington, DC 20374  
Telephone: (202) 433-3658  
Fax: (202) 433-6045

**Area: Tidewater Virginia**

**Naval Criminal Investigative Service Field Office**

1329 Bellinger Boulevard  
Norfolk, VA 23511-2395  
Telephone: (804) 444-7327  
Fax: (804) 444-3139

**Area: New Jersey, New York, and Pennsylvania**

**Naval Criminal Investigative Service Field Office**

Naval Weapons Station  
Colts Neck, NJ 07722-1901  
Telephone: (908) 866-2235  
Fax: (908) 866-1065

**Area: North Carolina**

**Naval Criminal Investigative Service Field Office**

H-32 Julian C. Smith Boulevard  
Camp LeJeune, NC 28547-1600  
Telephone: (910) 451-8017  
Fax: (910) 451-8205

**Area: Northwest Washington**

**Naval Criminal Investigative Service Field Office**

1010 Skate Street  
Suite A  
Silverdale, WA 98315-1093  
Telephone: (360) 396-4660  
Fax: (360) 396-7009

**Area: New England and Bermuda**

**Naval Criminal Investigative Service Field Office**

344 Meyerkord Avenue, Third Floor  
Newport, RI 02841-1607  
Telephone: (401) 841-2241  
Fax: (401) 841-4056

**Area: North Central United States**

**Naval Criminal Investigative Service Field Office**

Building 2  
Second Floor East  
Great Lakes, IL 60088-5001  
Telephone: (708) 688-5655  
Fax: (708) 688-2636

**Area: South Central United States**

**Naval Criminal Investigative Service Field Office**

341 Saufley Street  
Pensacola, FL 32508-5133  
Telephone: (904) 452-4211  
Fax: (904) 452-2194

**Area: Southeastern United States, Cuba, and Puerto Rico**

**Naval Criminal Investigative Service Field Office**

Naval Station  
P.O. Box 280076  
Mayport, FL 32228-0076  
Telephone: (904) 270-5361  
Fax: (904) 270-6050

## **Air Force**

### ***During normal working hours:***

Investigative Operations Center  
Major Crimes Investigations  
Bolling Air Force Base  
Washington, DC 20332-5113  
Telephone: (202) 767-5192/7760  
Fax: (202) 767-5196

### ***After normal working hours:***

HQ AFOSI Staff Duty Office  
Bolling Air Force Base  
Washington, DC 20332-5113  
Telephone: (202) 767-5450  
Fax: (202) 767-5452

1 - 6



## Appendix 2

### Safe and Drug-Free Schools Comprehensive Regional Centers

Training and technical assistance for States, school districts, schools, community-based organizations, and other recipients of funds under the Improving America's Schools Act are available through the following Comprehensive Regional Assistance Centers:

**Region I:** Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont

Dr. Vivian Guilfooy, Director  
Education Development Center, Inc.  
55 Chapel Street  
Newton, MA 02158-1060  
Telephone: (617) 969-7100, ext. 2201

**Region II:** New York

Dr. LaMar P. Miller, Executive Director  
New York University  
32 Washington Place  
New York, NY 10003  
Telephone: (212) 998-5100

**Region III:** Delaware, Maryland, New Jersey, Ohio, Pennsylvania, and Washington, D.C.

Dr. Charlene Rivera, Director  
George Washington University  
1730 North Lynn Street, Suite 401  
Arlington, VA 22209  
Telephone: (703) 528-3588

**Region IV:** Kentucky, North Carolina, South Carolina, Tennessee, Virginia, and W. Virginia

Dr. Terry L. Eidell, Executive Director  
Appalachia Educational Laboratory, Inc.  
P.O. Box 1348  
Charleston, WV 25325-1348  
Telephone: (304) 347-0400

**Region V:** Alabama, Arkansas, Georgia, Louisiana, and Mississippi

Dr. Betty Matluck, Vice President  
Southwest Educational Development Laboratory  
211 East Seventh Street  
Austin, TX 78701-3281  
Telephone: (512) 476-6861

**Region VI:** Iowa, Michigan, Minnesota, North Dakota, and Wisconsin

Dr. Minerva Coyne, Director  
University of Wisconsin  
1025 West Johnson Street  
Madison, WI 53706  
Telephone: (608) 263-4326

**Region VII:** Illinois, Indiana, Kansas, Missouri, Nebraska, and Oklahoma

Dr. Hai Tran, Director  
University of Oklahoma  
1000 ASP - Room 210  
Norman, OK 73019  
Telephone: (405) 325-2243

**Region VIII:** Texas

Dr. Maria Robledo Montecel, Executive Director  
Dr. Albert Cortez, Site Director  
Intercultural Development Research Association  
5835 Callaghan Road, Suite 350  
San Antonio, TX 78228-1190  
Telephone: (210) 684-8180

**Region IX:** Arizona, Colorado, New Mexico, Nevada, and Utah

Dr. Paul E. Martinez, Director  
New Mexico Highlands University  
121 Tijeras NE., Suite 2100  
Albuquerque, NM 87102  
Telephone: (505) 242-7447

**Region X:** Idaho, Montana, Oregon, Washington, and Wyoming

Mr. Carlos Sundermann, Director  
Northwest Regional Educational Laboratory  
101 Southwest Main Street, Suite 500  
Portland, OR 97204  
Telephone: (503) 275-9479

**Region XI:** Northern California

Dr. Beverly Farr, Director  
Far West Laboratory for Educational Research  
730 Harrison Street  
San Francisco, CA 90242  
Telephone: (415) 565-3009

**Region XII:** Southern California

Dr. Celia C. Ayala, Director  
Los Angeles County Office of Education  
9300 Imperial Highway  
Downey, CA 90242-2890  
Telephone: (310) 922-6319

**Region XIII:** Alaska

Dr. John Anttonen, Executive Director  
South East Regional Resource Center  
210 Ferry Way  
Suite 200  
Juneau, AK 99801  
Telephone: (907) 586-6806

**Region XIV:** Florida, Puerto Rico, and the Virgin Islands

Dr. Trudy Hensley, Director  
Educational Testing Service  
1979 Lake Side Parkway, Suite 400  
Tucker, GA 30084  
Telephone: (770) 723-7443

**Region XV:** American Samoa, Commonwealth of the Northern Mariana Islands, Federated States of Micronesia, Guam, Hawaii, Republic of the Marshall Islands, and Republic of Palau

Dr. John W. Kofel, Chief Executive  
Pacific Region Educational Laboratory  
828 Fort Street Mall, Suite 500  
Honolulu, HI 96813  
Telephone: (808) 533-6000



## Appendix 3

### Family and Youth Services Bureau Regional Centers

Empire State Coalition of Youth and Family  
Services/Region II  
121 Avenue of the Americas, Room 507  
New York, NY 10013-1505  
Telephone: (212) 966-6477  
Fax: (212) 431-9783  
EMPSTACOAL@aol.com

Mid-Atlantic Network of Youth and Family  
Services, Inc.  
9400 McKnight Road, Suite 204  
Pittsburgh, PA 15237  
Telephone: (412) 366-6562  
Fax: (412) 366-5407  
NancyJMANY@ol.com

MINK - c/o Synergy/Region VII  
P.O. Box 14403  
Parkville, MO 64152  
Telephone: (816) 587-4100  
Fax: (816) 587-6691  
MINKPAM@aol.com

Mountain Plains Youth Services/Region VIII  
221 West Rosser Avenue  
Bismarck, ND 58501  
Telephone: (701) 255-7229  
Fax: (701) 255-3922  
MTNPLAINS@aol.com

New England Consortium for Families and  
Youth/Region I  
25 Stow Road  
Boxboro, MA 01719  
Telephone: (508) 266-1998  
Fax: (508) 266-1999  
NECFY@aol.com

Northwest Network of Runaway and Youth  
Services/Region X  
603 Stewart Street, Suite 609  
Seattle, WA 98101  
Telephone: (206) 628-3760  
Fax: (206) 628-3746  
Northwestnw@aol.com

Southeastern Network of Youth and Family  
Services/Region IV  
337 South Milledge Avenue, Suite 209  
Athens, GA 30605  
Telephone: (706) 354-4568  
Fax: (706) 353-0026  
SENCYFS@aol.com

South West Network of Youth Services, Inc./  
Region VI  
Texas Network of Youth Services  
2525 Wallingwood Drive, Suite 1503  
Austin, TX 78746  
Telephone: (512) 328-6860  
Fax: (512) 328-6863  
TheresaTod@aol.com

Western States Youth Services Network/  
Region IX  
1309 Ross Street, Suite B  
Petaluma, CA 94954  
Telephone: (707) 763-2213  
Fax: (707) 763-2704  
WSYN@aol.com

Youth Network Council  
Illinois Collaboration on Youth  
59 East Van Buren Street, Suite 1610  
Chicago, IL 60605  
Telephone: (312) 427-2710  
Fax: (312) 427-3247  
YNCICOY@aol.com

3 - 2

## Appendix 4

### Organizations Concerned With The Prevention of Child Abuse and Neglect: State Contacts

*The following organizations can serve as resources for information and materials in the prevention of child abuse and neglect:*

- *"Don't Shake the Baby"* is a national public awareness campaign, organized in all 50 States, the District of Columbia and Puerto Rico, focused on decreasing the incidence of Shaken Baby Syndrome and thereby decreasing disability and death caused by child maltreatment.
  
- *Children's Trust and Prevention Funds* are State-level organizations that support community prevention programs through policy formation, funding innovative programs, public awareness, and education.
  
- *National Committee to Prevent Child Abuse* is a not-for-profit, volunteer-based organization committed to the prevention of child maltreatment through education, research, public awareness, and advocacy services to community members.
  
- *Parents Anonymous* is a parent self-help program with neighborhood-based support groups throughout the United States and several foreign countries.

## **"DON'T SHAKE THE BABY" CONTACTS**

### **ALABAMA**

Betsy Taff  
Alabama Children's Trust Fund  
P.O. Box 4251  
Montgomery, AL 36103  
(334) 242-5710  
(334) 242-5711 (fax)

### **ALASKA**

Debra Bruneau/Judy Saha  
Rural Community Action  
Program  
P.O. Box 200908  
Anchorage, AK 99520  
(907) 279-2511  
(907) 279-6343 (fax)

### **ARIZONA**

Becky Ruffner  
State Coordinator  
Arizona Chapter, NCPA  
P.O. Box 442  
Prescott, AZ 86302  
(602) 445-5038  
(602) 778-6120 (fax)

### **ARKANSAS**

Sherri McLemore  
AK Child Abuse Prevention  
2915 Kavanaugh, Suite 379  
Little Rock, AR 72205  
(501) 374-9003  
(501) 372-5257 (fax)

### **CALIFORNIA**

Margery Winter  
Office of Child Abuse  
Prevention CCDSS  
744 P Street, MS 9-100  
Sacramento, CA 95814  
(916) 445-0456  
(916) 445-2898 (fax)

### **COLORADO**

Jacy Showers, Ed.D.  
Pueblo City-County Health  
Department  
151 Central Main Street  
Pueblo, CO 81003-4297  
(719) 583-2000  
(719) 583-2004 (fax)

### **CONNECTICUT**

Jane Bourns  
Director of Children's Services  
Susanne Santangelo  
Wheeler Clinic  
91 Northwest Drive  
Plainville, CT 06062  
(203) 747-6801, ext. 244  
(203) 793-3520 (fax)

### **DELAWARE**

Karen Derasmo  
Delawareans United to Prevent  
Child Abuse  
124CD Senatorial Drive  
Greenville Place  
Wilmington, DE 19807  
(302) 654-1102  
(302) 655-5761 (fax)

### **DISTRICT OF COLUMBIA**

Dr. Lavdena Orr  
Division of Child Protection  
Children's National Medical  
Center  
111 Michigan Avenue, N.W.  
Washington, DC 20010-2970  
(202) 884-4950  
(202) 884-6997 (fax)

### **FLORIDA**

Stephanie Meinke, MSW  
President  
Parent Network/FCPCA  
2728 Pablo Avenue, Suite B  
Tallahassee, FL 32308  
(904) 488-5437  
(904) 921-0322 (fax)

### **GEORGIA**

Pam Brown  
GA Council on Child Abuse,  
Inc.  
First Steps Program  
1375 Peachtree Street, N.E.  
Suite 200  
Atlanta, GA 30309-3111  
(404) 870-6565  
(404) 870-6541 (fax)

### **HAWAII**

Aileen Deese  
PREVENT Child Abuse - HI  
Hawaii Chapter, NCPA  
1575 S. Beretania Street  
Suite 202  
Honolulu, HI 96826  
(808) 951-0200  
(808) 941-7004 (fax)

### **IDAHO**

Anna Sever, Child Protection  
Program Specialist  
FACTS - Third Floor  
Children's Service Bureau  
450 W. State Street  
Boise, ID 83720-0036  
(208) 334-5920  
(208) 334-6699 (fax)

### **ILLINOIS**

Robyn Gabel, Exec. Director  
Illinois Maternal & Child  
Health Coalition  
3411 W. Diversey, Suite 5  
Chicago, IL 60647  
(312) 384-8828  
(312) 384-3904 (fax)

### **INDIANA**

Patti Duwel  
Indiana Chapter of NCPA  
Jefferson Plaza  
One Virginia Avenue, Suite 401  
Indianapolis, IN 46204  
(317) 634-9282  
(317) 634-9295 (fax)

**IOWA**

John Holtkamp  
Iowa Chapter NCPA  
3829 71st Street, Suite A  
Des Moines, IA 50322  
(515) 252-0270  
(515) 252-0829 (fax)

**KANSAS**

Michelle Sinclair Lawrence  
(Brenda Sharpe)  
Child Abuse Prevention  
Coalition  
6811 W. 63rd Street, Suite 210  
Overland Park, KS 66202-4080  
(913) 831-2272  
(913) 831-0273 (fax)

**KENTUCKY**

Donna Overbee  
Program Director  
Kentucky Council on Child  
Abuse, Inc.  
2401 Regency Road, Suite 104  
Lexington, KY 40503  
(606) 276-1299  
(800) 432-9251  
(606) 277-1782 (fax)

**LOUISIANA**

Jacinta (Jay) Settoon  
LA Council on Child Abuse  
2351 Energy Drive, Suite 1010  
Baton Rouge, LA 70808  
(800) 348-KIDS (LA only)  
(504) 925-9520  
(504) 926-1319 (fax)

**MAINE**

Cheryl DiCara  
Maternal and Child Health  
Statehouse Station #11  
Augusta, ME 04333  
(207) 287-3311  
(207) 287-5355 (fax)

**MARYLAND**

Martha Elliott  
Director of Social Work  
Mt. Washington Pediatric Hosp.  
1708 Rogers Avenue  
Baltimore, MD 21209  
(410) 578-8600, ext. 4  
(410) 466-1715 (fax)

**MASSACHUSETTS**

Jetta Bernier, Exec. Director  
MA Committee for Children  
and Youth  
14 Beacon Street, Suite 706  
Boston, MA 02108  
(617) 742-8555  
(617) 742-7808 (fax)

**MICHIGAN**

Janice Long  
MI Children's Trust Fund  
P.O. Box 30037  
Lansing, MI 48909  
(517) 373-4320  
(517) 335-6177 (fax)

**MINNESOTA**

Carolyn Levitt, M.D.  
Midwest Children's Resource  
Center  
360 Sherman Street, Suite 200  
St. Paul, MN 55102  
(612) 220-6750  
(612) 220-6770 (fax)

Jane Swenson  
Midwest Children's Resource  
Center  
360 Sherman Street, Suite 200  
St. Paul, MN 55102  
(612) 220-6750  
(612) 220-6770 (fax)

**MISSISSIPPI**

Regan Marler Painter, Director  
MS Children's Trust Fund  
State Dept. of Human Services  
750 N. State Street  
Jackson, MS 39202  
(601) 359-4479  
(601) 359-4363 (fax)

**MISSOURI**

Nela Beetem  
Social Work Consultant  
MO Department of Health  
Bureau of Perinatal and Child  
Health  
1730 E. Elm Street  
Jefferson City, MO 65102  
(314) 751-6215  
(314) 526-5348 (fax)

**MONTANA**

Maryellen Bindel  
Cascade Co. CAP Council, Inc.  
2608 Second Avenue, North  
Great Falls, MT 59401  
(406) 761-1286

**NEBRASKA**

Terri Segal  
NE Dept. of Social Services  
301 Centennial Mall South  
Lincoln, NE 68509  
(402) 471-9196  
(402) 471-9455 (fax)

**NEVADA**

Dr. Paula R. Ford, Exec. Dir.  
Nevada NCPA  
We Can, Inc.  
3441 W. Sahara, Suite C-3  
Las Vegas, NV 89102  
(702) 368-1533  
(702) 368-1540 (fax)

**NEW HAMPSHIRE**

Audrey Knight, MSN, CPNP  
Child Health Nurse Consultant  
Bureau of Maternal & Child  
Health  
NH Division of Public Health  
Services  
6 Hazen Drive  
Concord, NH 03301  
(603) 271-4536  
(603) 271-3827 (fax)

**NEW JERSEY**

Susan White  
New Jersey Chapter, NCPA  
35 Halsey Street  
Newark, NJ 07012  
(201) 643-3710  
(201) 643-9222 (fax)

**NEW MEXICO**

Ellen Novak  
Children, Youth & Families  
Dept.  
Child Abuse Prevention Unit  
300 San Mateo N.E., Suite 602  
Albuquerque, NM 87108-1516  
(505) 841-2967  
(505) 841-2969 (fax)

**NEW YORK**

Judith Richards  
William B. Hoyt Memorial  
Children & Family Trust Fund  
40 N. Pearl Street, 11-D  
Albany, NY 12243  
(518) 474-9613  
(518) 474-9617 (fax)

**NORTH CAROLINA**

Jennifer Tolle, Exec. Director  
Prevent Child Abuse - NC  
3344 Hillsborough Street  
Suite 100D  
Raleigh, NC 27607  
(919) 829-8009  
(919) 832-0308 (fax)

**NORTH DAKOTA**

Sue Heinze  
Children's Hospital MeritCare  
720 4th Street North  
Fargo, ND 58122  
(701) 234-5737  
(701) 234-6965 (fax)

**OHIO**

Sharon Enright, Project Dir.  
GRADS  
65 S. Front Street, Room 909  
Columbus, OH 43215-4183  
(614) 466-3046  
(614) 644-5702 (fax)

Eve Pearl  
Council on Child Abuse of  
Southern Ohio, Inc.  
7374 Reading Road, Suite 105  
Cincinnati, OH 45237  
(513) 351-8005  
(513) 351-0226 (fax)

**OKLAHOMA**

John Stuemky, MD  
Oklahoma Emergency Medical  
Services for Children Project  
Children's Hospital of OK  
940 N.E. 13th Street  
Oklahoma City, OK  
73104-5066  
(405) 271-3307  
(405) 271-8709 (fax)

**OREGON**

Donna Merrill  
Children's Trust Fund  
800 N.E. Oregon Street  
Suite 1140  
Portland, OR 97232-2161  
(503) 731-4782  
(503) 731-8614 (fax)

**RHODE ISLAND**

Ted Whiteside, Exec. Director  
Rhode Island Committee to  
Prevent Child Abuse  
500 Prospect Street  
Pawtucket, RI 02860  
(401) 728-7920  
(401) 724-5850 (fax)

**SOUTH CAROLINA**

Sandra Jeter  
Office of Pub. Health/Soc. Work  
Department of Health and  
Environmental Control  
Robert Mills Complex  
Box 101106  
Columbia, SC 29211  
(803) 737-3950  
(803) 737-3946 (fax)

**SOUTH DAKOTA**

Merlin Weyer, Prog. Specialist  
Joyce Country, Prog. Specialist  
Office of Child Protection Svcs.  
700 Governor's Drive  
Kneip Building  
Pierre, SD 57501  
(605) 773-3227  
(605) 773-6834 (fax)

**TENNESSEE**

Dora Hemphill  
TN Dept. of Human Services  
400 Deaderick Street  
Nashville, TN 37248  
(615) 313-4764  
(615) 532-9956 (fax)

**TEXAS**

Janie Fields, Executive Director  
Claire Kriens  
Children's Trust Fund of Texas  
8929 Shoal Creek Boulevard  
Suite 200  
Austin, TX 78757-6854  
(512) 458-1281  
(512) 458-9471 (fax)

**UTAH**

Marilyn Sandberg  
Stacy Iverson  
Child Abuse Prevention Council  
of Ogden  
457 26th Street  
Ogden, UT 84401  
(801) 399-8430  
(801) 399-8016 (fax)

**VERMONT**

Linda Johnson, Exec. Director  
Vermont Chapter, NCPA  
141 Main Street  
P.O. Box 829  
Montpelier, VT 05601  
(802) 229-5724  
(802) 223-5567 (fax)

**VIRGINIA**

Diane Bell, Deputy Director  
SCAN of Northern Virginia,  
Inc.  
2210 Mount Vernon Avenue  
Alexandria, VA 22301  
(703) 836-1820  
(703) 836-1248 (fax)

**WASHINGTON**

Carol Mason  
Children's Protection Program  
Children's Hospital and  
Medical Center  
4800 Sand Point Way, N.E.  
P.O. Box 5371, MS CH-76  
Seattle, WA 98105-3071  
(206) 526-2194  
(206) 526-2246 (fax)

Carmen Ray, Exec. Director  
WA Council for Prevention of  
Child Abuse and Neglect  
318 First Avenue, South  
Suite 310  
Seattle, WA 98104  
(206) 464-6151  
(206) 464-6642 (fax)

**WEST VIRGINIA**

Victoria Schlak  
Children's Reportable Disease  
Coordinator  
1411 Virginia Street, East  
Charleston, WV 25301  
(304) 558-7996  
(304) 558-2183 (fax)

**WISCONSIN**

Christine Holmes  
Child Protection Center  
Outpatient Health Center  
1020 N. 12th Street  
Milwaukee, WI 53233  
(414) 277-8980  
(414) 277-8969 (fax)

**WYOMING**

Rick Robb  
Wyoming Department of  
Family Services  
Hathaway Building  
2300 Capitol Avenue  
Cheyenne, WY 82002  
(307) 777-7150  
(307) 777-3693 (fax)

**NATIONAL PROJECT  
DIRECTOR**

Jacy Showers, Ed.D.  
SBS Prevention Plus  
1907 Northmoor Terrace  
Pueblo, CO 81008  
(719) 583-2000  
(719) 583-2004 (fax)

## CHILDREN'S TRUST AND PREVENTION FUNDS

### ALABAMA

Kitty Trent  
Alabama CTF  
P.O. Box 4251  
Montgomery, AL 36103  
(334) 242-5710  
(334) 242-5711 (fax)

### ALASKA

Nila Rinehart  
Alaska CTF - Children's  
Cabinet  
P.O. Box 112100  
Juneau, AK 99811  
(907) 465-4870  
(907) 465-8638 (fax)

### ARIZONA

Valerie Roberson  
Arizona CTF  
Child Abuse Prevention Fund  
P. O. Box 6123, Site Code 940A  
Phoenix, AZ 85005  
(602) 542-0817  
(602) 542-3330 (fax)

### ARKANSAS

Sherri McLemore  
Arkansas CTF  
2915 Kavanaugh, Suite 416  
Little Rock, AR 72205  
(501) 374-9003  
(501) 372-5257 (fax)

### CALIFORNIA

Margery Winter  
California CTF  
Office of Child Abuse  
Prevention  
744 P Street, Mail Station 19-82  
Sacramento, CA 95814  
(916) 445-2862  
(916) 445-2898 (fax)

### COLORADO

Joyce Jennings  
Colorado CTF  
110 16th Street, 3rd Floor  
Denver, CO 80202  
(303) 446-8860  
(303) 640-5289 (fax)

### CONNECTICUT

Carol LaLiberte  
Connecticut CTF  
505 Hudson Street  
Hartford, CT 06106  
(860) 550-6473  
(860) 566-8022 (fax)

### DELAWARE

Richard Donges  
Delaware CTF  
P.O. Box 2363  
Wilmington, DE 19899  
(302) 836-8550  
(302) 836-2960 (fax)

### DISTRICT OF COLUMBIA

Carolyn Abdullah  
District of Columbia CTF  
1730 K Street, N.W., Suite 304  
Washington, DC 20006  
(202) 296-6656  
(202) 296-0942 (fax)

### FLORIDA

Admiral Henderson  
Florida CTF  
Dept. Health and Rehabilitative  
Services  
2811 C Industrial Plaza Drive  
Tallahassee, FL 32301  
(904) 488-8762  
(904) 488-9584 (fax)

### GEORGIA

Susan Phillips  
Georgia CTF  
Two Northside 75, Suite 125  
Atlanta, GA 30318  
(404) 352-6050  
(404) 352-6051 (fax)

### HAWAII

Steve Kaneshiro  
Hawaii CTF  
Hawaii Community Foundation  
222 Merchant Street  
Honolulu, HI 96813  
(808) 537-6333  
(808) 521-6286 (fax)

### IDAHO

Laura Rappaport  
Idaho CTF  
P.O. Box 2015  
Boise, ID 83701-2015  
(208) 386-9317  
(208) 334-6699 (fax)

### ILLINOIS

Ron Davidson  
Illinois CTF  
Dept. of Children & Family  
Services  
406 E. Monroe Street  
Station #225  
Springfield, IL 62701-1498  
(217) 524-2403  
(217) 524-3966 (fax)

### INDIANA

Vernell Miller  
Indiana CTF  
Child Abuse Prevention Fund  
402 W. Washington Street  
Room W364  
Indianapolis, IN 46204  
(317) 232-7116  
(317) 232-4436 (fax)



**IOWA**

Somma Ung  
Iowa CTF  
Iowa Dept. Human Services  
5th Floor  
Hoover State Office Building  
Des Moines, IA 50319-0114  
(515) 281-5246  
(515) 281-4597 (fax)

**KANSAS**

James Tramill  
Kansas CTF  
Family & Children's Trust Fund  
515 S. Kansas Avenue, Suite A  
Topeka, KS 66603  
(913) 296-3651  
(913) 296-4880 (fax)

**KENTUCKY**

John W. Patterson  
Kentucky CTF  
Child Victims' Trust Fund  
P.O. Box 2000  
Frankfort, KY 40602  
(502) 573-5900  
(502) 573-8315 (fax)

**LOUISIANA**

Judy Harrison  
Louisiana CTF  
P.O. Box 3318  
Baton Rouge, LA 70821  
(504) 342-2245  
(504) 342-2268 (fax)

**MAINE**

J. Terence Burns, President  
Maine CTF  
P.O. Box 2850  
Augusta, ME 04338  
(207) 623-5461

**MARYLAND**

J.C. Shay  
Maryland CTF  
301 W. Preston Street  
Suite 1502  
Baltimore, MD 21201  
(410) 225-4160  
(410) 333-7492 (fax)

**MASSACHUSETTS**

Suzin M. Bartley  
Massachusetts CTF  
294 Washington Street  
Suite 640  
Boston, MA 02108-4608  
(617) 727-8957  
(617) 727-8997 (fax)

**MICHIGAN**

Deborah Strong  
Michigan CTF  
P.O. Box 30037  
Lansing, MI 48909  
(517) 373-4320  
(517) 335-6177 (fax)

**MINNESOTA**

Maureen Cannon  
Minnesota CTF  
444 Lafayette Road  
Saint Paul, MN 55155-3839  
(612) 296-5436  
(612) 297-1949 (fax)

**MISSISSIPPI**

Regan Marler Painter  
Mississippi CTF  
Dept. Human Services  
750 N. State Street  
Jackson, MS 39202  
(601) 359-4479  
(601) 359-4363 (fax)

**MISSOURI**

Sarah Grim  
Missouri CTF  
P.O. Box 1641  
Jefferson City, MO 65102-1641  
(573) 751-5147  
(573) 751-0254 (fax)

**MONTANA**

Kirk Astroth  
Montana CTF  
Montana State University  
210 Taylor Hall  
Bozeman, MT 59717-0358  
(406) 994-3501  
(406) 994-5417 (fax)

**NEBRASKA**

Mary Jo Pankoke  
Nebraska CTF  
Child Abuse Prevention Fund  
301 Centennial Mall South  
Lincoln, NE 68508  
(402) 471-9320  
(402) 471-9455 (fax)

**NEVADA**

Joan Buchanan  
Nevada CTF  
505 E. King Street, Room 600  
Carson City, NV 89710  
(702) 687-5761  
(702) 687-4733 (fax)

**NEW HAMPSHIRE**

Fran Belcher  
New Hampshire CTF  
NH Charitable Foundation  
37 Pleasant Street  
Concord, NH 03301-4005  
(603) 225-6641  
(603) 225-1700 (fax)

**NEW JERSEY**

Donna Pincavage  
New Jersey CTF  
222 S. Warren Street, CN 700  
Trenton, NJ 08625-0700  
(609) 633-3992  
(609) 984-7380 (fax)

**NEW MEXICO**

Director  
New Mexico CTF  
300 San Mateo N.E. - 5th Floor  
Albuquerque, NM 87108  
(505) 841-6494  
(505) 841-6485 (fax)

**NEW YORK**

Judy Richards  
New York CTF  
Children & Family Trust Fund  
40 N. Pearl Street, 11 Floor  
Albany, NY 12243-0001  
(518) 474-9613  
(518) 474-9617 (fax)

**NORTH CAROLINA**

Dwight Whitted  
North Carolina CTF  
301 N. Wilmington Street  
Raleigh, NC 27601-2825  
(919) 715-1637  
(919) 715-0517 (fax)

**NORTH DAKOTA**

Beth Wosick  
North Dakota CTF  
600 E. Boulevard Avenue  
Bismarck, ND 58505-0250  
(701) 224-2301  
(701) 224-2359 (fax)

**OHIO**

Rhonda Reagh, Ph.D.  
Ohio CTF  
65 E. State Street, Suite 908  
Columbus, OH 43266-0423  
(614) 466-1822  
(614) 728-3504 (fax)

**OKLAHOMA**

Pamela Rollins  
Oklahoma CTF  
Child Abuse Prevention Fund  
1000 N.E. 10th  
Oklahoma City, OK  
73117-1299  
(405) 271-4471  
(405) 271-1011 (fax)

**OREGON**

Cynthia Thompson  
Oregon CTF  
800 N.E. Oregon Street  
Suite 1140  
Salem, OR 97232-2162  
(503) 731-4782  
(503) 731-8614 (fax)

**PENNSYLVANIA**

Scott Peters  
Pennsylvania CTF  
P.O. Box 2675  
Harrisburg, PA 17105-2675  
(717) 783-7287  
(717) 787-0414 (fax)

**RHODE ISLAND**

Nancy Herrington  
Rhode Island CTF  
Family & Children's Trust Fund  
610 Mount Pleasant Avenue  
Building 1  
Providence, RI 02908  
(401) 457-4519  
(401) 457-4511 (fax)

**SOUTH CAROLINA**

David Havin  
South Carolina CTF  
Partnership for S.C. Children  
2711 Middleburg Drive  
Suite 307  
Columbia, SC 29204  
(803) 929-1013  
(803) 779-4160 (fax)

**SOUTH DAKOTA**

Joyce Country  
South Dakota CTF  
700 Governor's Drive  
Pierre, SD 57501-2291  
(605) 773-3227  
(605) 773-4855 (fax)

**TENNESSEE**

Dora Hemphill  
Tennessee CTF  
Child Abuse Prevention Prog.  
400 Deaderick Street  
Nashville, TN 37248-9500  
(615) 313-4764  
(615) 532-9956 (fax)

**TEXAS**

Janie D. Fields  
Texas CTF  
8929 Shoal Creek Boulevard  
Suite 200  
Austin, TX 78757-6854  
(512) 458-1281  
(512) 458-9471 (fax)

**UTAH**

Consuelo Alires  
Utah CTF  
120 N. 200 West, Room 225  
Salt Lake City, UT 84103  
(801) 538-4535  
(801) 538-3993 (fax)

**VERMONT**

Linda Johnson  
Vermont CTF  
Children and Family Council  
103 S. Main Street  
Waterbury, VT 05671-0203  
(802) 241-2928  
(802) 241-2979 (fax)

**VIRGINIA**

Phyl Parrish  
Virginia CTF  
Family & Children's Trust Fund  
730 E. Broad Street  
Richmond, VA 23219  
(804) 692-1823  
(804) 692-1869 (fax)

**WASHINGTON**

Director  
Washington CTF  
Council for Prevention  
318 First Avenue South  
Suite 310  
Seattle, WA 98104  
(206) 464-6151  
(206) 464-6642 (fax)

**WEST VIRGINIA**

Barbara Merrill  
West Virginia CTF  
Gov. Cabinet on Children  
& Families  
Building 1, Room 9  
1900 Kanawaha Blvd., East  
Charleston, WV 25305  
(304) 558-1955  
(304) 558-0596 (fax)

**WISCONSIN**

Mary Ann Snyder  
Wisconsin CTF  
110 E. Main Street, Room 614  
Madison, WI 53703  
(608) 266-6871  
(608) 266-3792 (fax)

**WYOMING**

Carol Speight  
Wyoming CTF  
Dept. of Family Services  
Third Floor, Hathaway Building  
Cheyenne, WY 82002-0490  
(307) 777-6081  
(307) 777-7747 (fax)

***Developing Trust Fund:***

**PUERTO RICO**

Maria Carrillo de Sevilla  
Department of the Family  
GPO Box 15091  
San Juan, PR 00902  
(787) 724-7532  
(787) 721-1331 (fax)

## PARENTS ANONYMOUS, INC.

### ARIZONA

Michele Keal,  
President and CEO  
Parents Anonymous of AZ, Inc.  
2701 N. 16th Street, #316  
Phoenix, AZ 85006  
(602) 248-0428  
(602) 248-0496 (fax)  
*Family Lifeline* (800) 352-0528

### ARKANSAS

Linda Redden  
Parent Anonymous Coordinator  
SCAN Volunteer Services  
1400 W. Markham  
Little Rock, AR 72201  
(501) 372-7226  
(501) 375-7329 (fax)  
*Parents Anonymous*  
(501) 375-7321

### CALIFORNIA

Juanita Chavez,  
CA Coordinator  
Parents Anonymous, Inc.  
675 W. Foothill Blvd.  
Suite 220  
Claremont, CA 91711  
(909) 621-6184  
(909) 625-6304 (fax)

### COLORADO

Laura Fourzan, Coordinator  
Pikes Peak Family Connections,  
Inc.  
301 S. Union Boulevard  
Colorado Springs, CO 80910  
(719) 578-3210  
(719) 578-3192 (fax)  
*Family Connection*  
(719) 578-3206  
or (719) 495-4126

Jennifer Richardson,  
Coordinator  
Families First  
2760-R S. Havana Street  
P.O. Box 14190  
Aurora, CO 80014  
(303) 745-0327  
(303) 745-0115 (fax)  
*Parent Support Line*  
(303) 695-7996

### CONNECTICUT

Jane Bourns, Director  
Children's Clinical Services  
Wheeler Clinic  
91 Northwest Drive  
Plainville, CT 06062  
(860) 747-6801  
(860) 793-3520 (fax)  
*Parents Anonymous*  
(800) 841-4314

### DELAWARE

JoAnn Kasses & Karen  
DeRamos, Co-Directors  
Delawareans United to Prevent  
Child Abuse  
124 CD Senatorial Drive  
Wilmington, DE 19807  
(302) 654-1102  
(302) 655-5761 (fax)  
*PATH* (302) 654-1102; (302)  
674-1112; (302) 856-1737

### FLORIDA

Stephanie Meincke, Exec. Dir.  
The Family Source of Florida  
2728 Pablo Avenue, Suite B  
Tallahassee, FL 32308  
(904) 488-5437  
(904) 921-0322 (fax)  
*Parent Helpline* (800) 352-5683

### GEORGIA

Sandra Wood, Exec. Director  
GA Council on Child Abuse  
1375 Peachtree St. N.E., 200  
Atlanta, GA 30309  
(404) 870-6565  
(404) 870-6541(fax)  
*Helpline* (800) 532-3208

### ILLINOIS

Maureen Blaha  
Parents Anonymous Director  
Children's Home and Aid  
Society of Illinois  
125 S. Wacker Drive, 14<sup>th</sup> Flr.  
Chicago, IL 60606  
(312) 424-6822  
(312) 424-6800 (fax)  
*Parents Anonymous*  
(815) 968-0944; (618) 462-  
2714; (217) 359-8815; (708)  
837-6445; (312) 649-4879

### IOWA

Roberta Milinsky,  
Dir. of Program Activities  
Children & Families of Iowa  
1111 University  
Des Moines, IA 50314  
(515) 288-1981  
(515) 288-9109 (fax)  
*1st Call for Help*  
(515) 246-6555

### KENTUCKY

Mary Smith, Board Chair  
Parents Anonymous of Murray-  
Calloway County  
P.O. Box 1302  
Murray, KY 42071  
(502) 762-4627

**LOUISIANA**

Marketa Garner, Exec. Director  
LA Council on Child Abuse  
2351 Energy Drive  
Suite 1010  
Baton Rouge, LA 70808  
(504) 925-9520  
(800) 348-KIDS  
(504) 926-1319 (fax)

**MAINE**

Pam Marshall  
Parents Anonymous Coord.  
Parents Anonymous of Maine  
P.O. Box 284  
Cape Elizabeth, ME 04107  
(207) 767-5506  
(207) 767-0995 (fax)  
*Parent Talk Line*  
(800) 249-5506

**MARYLAND**

Frank Blanton, Exec. Director  
Parents Anonymous of MD  
733 W. 40th Street, Suite 20  
Baltimore, MD 21211  
(410) 889-2300  
(410) 889-2487 (fax)  
*Parent Stressline*  
(410) 243-7337

**MASSACHUSETTS**

Jeannette Atkinson  
Executive Director  
Parents Anonymous of MA  
140 Clarendon Street  
Boston, MA 02116  
(617) 267-8077  
(617) 351-7615 (fax),  
call first *Parents Anonymous*  
(800) 882-1250

**MICHIGAN**

Judy Ranger,  
Parent Aide Coordinator  
Family & Children's Services  
1608 Lake Street  
Kalamazoo, MI 49001  
(616) 344-0202  
(616) 344-0285 (fax)

**MINNESOTA**

Suzann Eisenberg Murray,  
Executive Director  
Parents Anonymous of MN  
1061 Rice Street  
Saint Paul, MN 55117  
(612) 487-2111  
(612) 487-6383 (fax)  
*Parents Anonymous*  
(507) 377-7665;  
(218) 736-5617

**MISSOURI**

Joyce Downing  
Parents Anonymous of Missouri  
10918 Elm Avenue  
Kansas City, MO 64134  
(816) 765-6600  
(816) 767-4101 (fax)  
*Parent Helpline* (800) 844-0192

**MONTANA**

Jeanne Kemis, Admin. Director  
Montana Council for Families  
P.O. Box 7533  
Missoula, MT 59807  
(406) 728-9449  
(406) 728-9459 (fax)  
*Parents Anonymous*  
(406) 728-5437;  
(406) 563-7983;  
(406) 252-9799;  
(406) 587-3840

**NEBRASKA**

Vicki Mack, Executive Director  
Parents Anonymous of Central  
Nebraska  
P.O. Box 1312  
Grand Island, NE 68802  
(308) 382-9117  
*Parent Stressline*  
(308) 389-0044

Lorena Murray, Chair,  
Board of Directors  
Hastings Area Parents  
Anonymous  
1832 W. Ninth Street  
Hastings, NE 68901  
(402) 463-4395

**NEVADA**

Sandy Soltz,  
Parents Anonymous Coord.  
WE CAN  
3441 W. Sahara, C-3  
Las Vegas, NV 89102  
(702) 368-1533  
(702) 368-1540 (fax)

**NEW HAMPSHIRE**

Monique Divine,  
Director of Communications  
New Hampshire Task Force to  
Prevent Child Abuse  
P.O. Box 607  
Concord, NH 03302  
(603) 225-5441  
(603) 228-5322 (fax)  
*PA Line* (800) 750-4494

**NEW JERSEY**

Kathleen Roe, Executive Dir.  
Parents Anonymous of NJ, Inc.  
12 Roszel Road, Suite A-103  
Princeton, NJ 08540  
(609) 243-9779  
(609) 243-0169 (fax)  
*Family Helpline*  
(800) THE-KIDS

**NEW MEXICO**

Chris Montano,  
Parent Anonymous Coordinator  
All Faiths Receiving Home  
P.O. Box 6573  
Albuquerque, NM 87197  
(505) 266-3506  
(505) 262-2877 (fax)

**NEW YORK**

Linda Murphy,  
Voc. Ed. Coordinator  
Yours, Ours, Mine Community  
Center, Inc.  
152 Center Lane  
Levittown, NY 11756  
(516) 796-6633  
(516) 796-6663 (fax)

Rosemary Taylor, Exec. Dir.  
YWCA  
44 Washington Avenue  
Schenectady, NY 12305  
(518) 374-3394  
(518) 374-3385 (fax)

**NORTH DAKOTA**

Beth Wosick, Exec. Dir.  
ND Children's Trust Fund  
600 East Boulevard  
Bismark, ND 58505  
(701) 328-2301  
(701) 328-2359 (fax)

**OHIO**

Carolyn Kurns  
Parents Anonymous of Canton  
Families First  
142 Arlington, NW  
Canton, OH 44708  
(330) 456-5470

Karen McCann  
Council on Child Abuse  
7374 Reading Road, Suite 1-A  
Cincinnati, OH 45237  
(513) 351-8005  
(513) 351-0226 (fax)

Marian Grisdale  
Bellflower Center  
11701 Shaker Boulevard  
Cleveland, OH 44120  
(216) 229-2420;  
(216) 229-2474

Bill McCulley,  
Parents Anonymous Director  
Catholic Social Services  
155 E. Patterson Avenue  
Columbus, OH 43202  
(614) 447-9192 (fax)  
*Parent Connection Line*  
(614) 447-9400

**OREGON**

Maureen Rozee, Parents  
Anonymous State Director  
Waverly Children's Home  
3550 S.E. Woodward  
Portland, OR 97202  
(503) 238-8819  
(503) 233-0187 (fax)  
*Parent Helpline* (800) 345-5044

**PENNSYLVANIA**

Angela Fogle, Exec. Director  
Parents Anonymous of PA  
2001 N. Front Street  
Building 1, Suite 314  
Harrisburg, PA 17102  
(717) 238-0937  
(717) 238-4315 (fax)  
*Parents Anonymous*  
(800) 448-4906

**RHODE ISLAND**

Mildred H. Bauer  
324 Oak Hill Avenue  
Attleboro, MA 02703  
(508) 222-6205  
(401) 434-1858 (fax)  
*Parents Anonymous*  
(800) 882-1250

**SOUTH CAROLINA**

Marty Banks, Exec. Director  
Parents Anonymous of SC  
P.O. Box 80099  
Charleston, SC 29416  
(803) 529-3200  
(803) 529-3211 (fax)  
*Helpline* (800) 326-8621

**TEXAS**

Rebecca Christie  
Executive Director  
Parents Anonymous of Texas  
7801 N. Lamar, Suite F-12  
Austin, TX 78752  
(512) 459-5490  
(512) 459-3058 (fax)  
*Texas Heartline*  
(800) 554-2323

**VERMONT**

Linda Johnson, Exec. Director  
Prevent Child Abuse-Vermont  
P.O. Box 829  
Montpelier, VT 05601  
(802) 229-5724  
(802) 223-5567 (fax)  
*Parent Stressline*  
(800) 639-4010

**VIRGINIA**

Karen Schrader,  
Director of Programs  
Prevent Child Abuse-Virginia  
P.O. Box 12308  
Richmond, VA 23241  
(804) 775-1777  
(804) 775-0019 (fax)  
*Warmline* (800) 257-8227

**WASHINGTON**

Sylvia Meyer, Exec. Director  
The Parent Trust for  
Washington Children  
1305 4th Avenue, Suite 310  
Seattle, WA 98101  
(206) 233-0156  
(206) 233-0604 (fax)  
*Family Helpline*  
(800) 932-HOPE

**WEST VIRGINIA**

Laurie McKeon, Coordinator  
Team for West Virginia  
Children  
824 Fifth Avenue, Suite 208  
Huntington, WV 25717  
(304) 523-9587  
(304) 523-9595 (fax)

**WISCONSIN**

Sally Casper,  
Executive Director  
Committee for Prevention of  
Child Abuse and Neglect  
214 N. Hamilton Street  
Madison, WI 53703  
(608) 256-3374  
(608) 256-3378 (fax); call first

Jackie Maggiore  
Executive Director  
The Parenting Network  
1717 S. Twelfth Street  
Suite 101  
Milwaukee, WI 53204  
(414) 671-5575  
(414) 671-1750 (fax)  
*Parent Stressline* (414) 671-  
0566

## NATIONAL COMMITTEE TO PREVENT CHILD ABUSE

### ALABAMA

Glenda Trotter, Exec. Director  
Greater AL Chapter, NCPA  
AL Council on Child Abuse Inc  
P.O. Box 230904  
2101 Eastern Boulevard  
Suite 26  
Montgomery, AL 36123-0904  
(334) 271-5105  
(334) 271-4349 (fax)  
HandsNet: HN4192

Joe Dean, President  
Greater AL Chapter, NCPA  
AL Council on Child Abuse Inc  
P.O. Box 848  
Opelika, AL 36803-0848  
(334) 749-5631  
(334) 749-5857 (fax)

Naomi Griffith, Exec. Director  
N. AL Chapter, NCPA  
Parents and Children Together  
P.O. Box 1247  
613 Lafayette NE  
Decatur, AL 35601  
(205) 355-7252  
(205) 351-0558 (fax)

Carol Bolding, President  
N. Alabama Chapter, NCPA  
Parents and Children Together  
P.O. Box 1247  
Decatur, AL 35602  
(205) 355-7252  
(205) 351-0558 (fax)

### ALASKA

Elizabeth Forrer, Exec. Dir,  
South Central Alaska Chapter,  
NCPA  
Anchorage Center for Families  
3745 Community Park Loop  
Suite 102  
Anchorage, AK 99508-3466  
(907) 276-4994  
(907) 276-6930 (fax)  
E-mail: acf@aonline.com

Joe Sonderleiter, President  
South Central Alaska Chapter,  
NCPA  
670 W. Fireweed Lane  
Anchorage, AK 99503  
(907) 265-4912  
(907) 265-4928 (fax)

Steve Krause, Exec. Director  
Fairbanks AK Chapter, NCPA  
Resource Center for Parents and  
Children  
1401 Kellum Street  
Fairbanks, AK 99701  
(907) 456-2866  
(907) 451-8125 (fax)

Christine Vaughan, President  
Fairbanks AK Chapter, NCPA  
Resource Center for Parents  
and Children  
1401 Kellum Street  
Fairbanks, AK 99701  
(907) 456-2866  
(907) 451-8125 (fax)

### ARIZONA

Carole Brazsky, Exec. Director  
Arizona Chapter, NCPA  
P.O. Box 63921  
Phoenix, AZ 85082-3921  
(602) 969-2308  
(602) 969-9277 (fax)

Deb Littler, President  
Arizona Chapter, NCPA  
c/o Child Crisis Center  
P.O. Box 4114  
Mesa, AZ 85211  
(602) 969-2308  
(602) 969-9277 (fax)

### CALIFORNIA

Julie Christine, Exec. Director  
California Chapter, NCPA  
CA Consortium to Prevent  
Child Abuse  
926 J Street, Suite 717  
Sacramento, CA 95814-2707  
(916) 498-8481  
(916) 498-0825 (fax)  
HandsNet: HN2300  
E-mail: ccpcax@ix.netcom.com

Cynthia Remmers, President  
California Chapter, NCPA  
CA Consortium to Prevent  
Child Abuse  
c/o Orrick, Herrington &  
Sutcliffe  
400 Capital  
Sacramento, CA 95814  
(916) 329-7909

### COLORADO

Bert Singleton, Exec. Director  
Colorado Chapter, NCPA  
Colorado Coalition for the  
Protection of Children  
950 S. Cherry, Suite 312  
Denver, CO 80222  
(303) 759-2383  
(303) 782-0850 (fax)

Linda Puckett, President  
Colorado Chapter, NCPA  
Colorado Coalition for the  
Protection of Children  
950 S. Cherry, Suite 312  
Denver, CO 80222  
(303) 782-9337  
(303) 782-0850 (fax)



**CONNECTICUT**

Jane Bourns, Director  
Connecticut Chapter, NCP  
CA  
Connecticut Center for  
Prevention of Child Abuse  
Wheeler Clinic  
91 Northwest Drive  
Plainville, CT 06062  
(860) 747-6801, ext. 244  
(860) 793-3520 (fax)  
E-mail: ccpca@connix.com

Ronald Bucchi, Chairperson  
Connecticut Chapter, NCP  
CA  
Connecticut Center for  
Prevention of Child Abuse  
Hyde & Bucchi  
200 Fisher Drive  
Avon Park North  
Avon, CT 06001  
(860) 678-0155  
(860) 676-0213 (fax)

**DELAWARE**

Karen de Rasmus/JoAnne Kasses  
Interim Co-Directors  
Delaware Chapter, NCP  
CA  
Delawareans United to Prevent  
Child Abuse  
Tower Office Park  
240 N. James Street, Suite 103  
Newport, DE 19804  
(302) 996-5444  
(302) 996-5425 (fax)  
HandsNet: HN2120  
E-mail: dupca@aol.com

Gay Lynch, President  
Delaware Chapter, NCP  
CA  
Delawareans United to Prevent  
Child Abuse  
Tower Office Park  
240 N. James Street, Suite 103  
Newport, DE 19804  
(302) 996-5444  
(302) 996-5425 (fax)

**DISTRICT OF COLUMBIA**

Barbara Lautman, Exec. Dir.  
Washington, D.C. Chapter,  
NCP  
CA  
D.C. Hotline, Inc.  
P.O. Box 57194  
1400 - 20th Street NW  
Washington, DC 20037  
(202) 223-0020  
(202) 296-4046 (fax)

Robert Yerman, President  
Washington, D.C. Chapter,  
NCP  
CA  
D.C. Hotline, Inc.  
9100 Falls Road  
Potomac, MD 20854  
(202) 822-4152

**FLORIDA**

Stephanie Meincke, Exec. Dir.  
Florida Chapter, NCP  
CA  
The Family Source  
2728 Pablo Street, Suite B  
Tallahassee, FL 32308  
(904) 488-5437  
(904) 921-0322 (fax)  
E-mail:  
familysource@nettally.com

Mary Oldiges, President  
Florida Chapter, NCP  
CA  
c/o Family Resource Center  
9500 S. Dadeland Boulevard  
Suite 350  
Miami, FL 33156  
(305) 670-7005  
(305) 670-7009 (fax)

**GEORGIA**

Sandra Wood, Exec. Director  
Georgia Chapter, NCP  
CA  
GA Council on Child Abuse Inc  
1375 Peachtree Street, N.E.  
Suite 200  
Atlanta, GA 30309  
(404) 870-6565  
(404) 870-6541 or 6587 (fax)  
HandsNet: HN1537  
Website: www.gcca.org

Paul Bowers, President  
Georgia Chapter, NCP  
CA  
GA Council on Child Abuse Inc  
c/o GA Power Company  
P.O. Box 4545  
Atlanta, GA 30302  
(404) 526-7386  
(404) 526-6877 (fax)

**HAWAII**

Charles Braden, Exec. Director  
Hawaii Chapter, NCP  
CA  
Prevent Child Abuse Hawaii  
1575 S. Beretania Street  
Suite 202  
Honolulu, HI 96826  
(808) 951-0200  
(808) 941-7004 (fax)  
E-mail: pciah@aloha.com

Wayne Suehisa, President  
Hawaii Chapter, NCP  
CA  
Prevent Child Abuse Hawaii  
2880 Kilihau Street  
Honolulu, HI 96819  
(808) 836-0888  
(808) 834-0652 (fax)

**ILLINOIS**

Don Schlosser, Exec. Director  
Illinois Chapter, NCP  
CA  
Prevent Child Abuse Illinois  
528 S. 5th Street, Suite 211  
Springfield, IL 62701  
(217) 522-1129  
(217) 522-0655 (fax)

Diana Stroud, President  
Illinois Chapter, NCP  
CA  
Prevent Child Abuse Illinois  
75 Lincoln Court  
Morton, IL 61550  
(309) 674-4125  
(309) 674-7029 (fax)

Roy Harley, Executive Director  
Quad Cities Affiliate, NCPA  
Child Abuse Council  
525 - 16th Street  
Moline, IL 61265  
(309) 764-7017  
(309) 757-8554 (fax)  
HandsNet: HN4040  
E-mail: harley@revealed.net

Larry McCallum, President  
Quad Cities Affiliate, NCPA  
Child Abuse Council  
1214 Pinehill Road  
Bettendorf, IL 52722  
(309) 794-7373 or 7300

#### **INDIANA**

Andie Marshall, Exec. Director  
Indiana Chapter, NCPA  
IN Chapter for Prevention of  
Child Abuse  
One Virginia Avenue, Suite 401  
Indianapolis, IN 46204  
(317) 634-9282  
(317) 634-9295 (fax)  
HandsNet: HN1700

Rebecca Goss, President  
Indiana Chapter, NCPA  
IN Chapter for Prevention of  
Child Abuse  
c/o Eli Lilly & Company  
Lilly Corporate Center  
Drop Code 1215  
Indianapolis, IN 46285  
(317) 276-2703  
(317) 276-9152 (fax)

#### **IOWA**

Steve Scott, Executive Director  
Iowa Chapter, NCPA  
3829 - 71st Street, Suite A  
Des Moines, IA 50322  
(515) 252-0270  
(515) 252-0829 (fax)  
E-mail: iowancpca@aol.com

Bill Ketch, President  
Iowa Chapter, NCPA  
1006 N. "C" Street  
Indianola, IA 50125  
(515) 246-4068 or 4000  
(515) 246-4068 (fax)

#### **KANSAS**

Robert L. Hartman, Exec. Dir.  
Kansas Chapter, NCPA  
KS Children's Service League  
1365 N. Custer Street  
P.O. Box 517  
Wichita, KS 67201  
(316) 942-4261  
(316) 943-9995 (fax)

Gwen Severt, President  
Kansas Chapter, NCPA  
KS Children's Service League  
9211 Lakepoint  
Wichita, KS 67226  
(316) 262-6834

Team Leader  
Prevention & Early Intervention  
Kansas Chapter, NCPA  
KS Children's Service League  
1365 N. Custer Street  
P.O. Box 517  
Wichita, KS 67201  
(316) 942-4261  
(316) 943-9995 (fax)

#### **KENTUCKY**

Jill Seyfred, Executive Director  
Kentucky Chapter, NCPA  
Kentucky Council on  
Child Abuse, Inc.  
2401 Regency Road, Suite 104  
Lexington, KY 40503  
(606) 276-1299 or 1399  
(606) 277-1782 (fax)

Gregory Schaaf, President  
Kentucky Chapter, NCPA  
KY Council on Child Abuse Inc  
c/o Greenebaum, Doll &  
McDonald  
P.O. Box 1808  
1400 Vine Center Tower  
Lexington, KY 40593-1637  
(606) 288-4621  
(606) 255-2742 (fax)

#### **LOUISIANA**

Marketa Garner, Exec. Director  
Louisiana Chapter, NCPA  
Louisiana Council on Child  
Abuse, Inc.  
2351 Energy Drive, Suite 1010  
Baton Rouge, LA 70808  
(504) 925-9520  
(504) 926-1319 (fax)  
HandsNet: HN1788

Helen Pope, Chairperson  
Louisiana Chapter, NCPA  
Louisiana Council on Child  
Abuse, Inc.  
P.O. Box 40990  
Baton Rouge, LA 70835-0990  
(504) 928-1160  
(504) 928-1161 (fax)

#### **MAINE**

Liz Kuhlman, Exec. Director  
Franklin County ME Chapter,  
NCPA  
Franklin County Children's  
Task Force  
69 N. Main Street  
Farmington, ME 04938  
(207) 778-6960  
(207) 778-0171 (fax)

Sue Taylor, Chairperson  
Franklin County ME Chapter,  
NCPA  
Franklin County Children's  
Task Force  
P.O. Box 500  
W. Farmington, ME 04992  
(207) 778-9442

Lucky Hollander, Exec. Dir.  
Greater Maine Chapter,  
NCPCA  
ME Assn. of CAN Councils  
P.O. Box 912  
211 Cumberland Avenue  
Portland, ME 04104  
(207) 874-1120  
(207) 874-1124 (fax)  
HandsNet: HN1113

Sheila Lovell, President  
Greater Maine Chapter,  
NCPCA  
ME Assn. of CAN Councils  
c/o Penquis CAP Council  
One Summer Street  
Dover Foxcroft, ME 04426  
(207) 564-7118  
(207) 564-2218 (fax)

Marilyn Staples, Exec. Director  
York County Chapter, NCPCA  
York County Child Abuse &  
Neglect Council, Inc.  
0 Dental Avenue, P.O. Box 568  
Biddeford, ME 04005  
(207) 284-1337  
(207) 284-1593 (fax)

Bill Hager, President  
York County Chapter, NCPCA  
York County Child Abuse &  
Neglect Council, Inc.  
c/o St. Louis Child Care  
P.O. Box 645  
116 Hill Street  
Biddeford, ME 04005  
(207) 282-3790

#### MARYLAND

Gloria Goldfaden, Exec. Dir.  
Maryland Chapter, NCPCA  
People Against Child Abuse Inc  
2530 Riva Road, Suite 3  
Annapolis, MD 21401  
(410) 841-6599  
(410) 224-3725 (fax)

Michael Reichel, M.D.,  
President  
Maryland Chapter, NCPCA  
People Against Child Abuse Inc  
7801 York Road, Suite 101  
Towson, MD 21204  
(410) 821-2810  
(410) 821-2804 (fax)

#### MASSACHUSETTS

Jetta Bernier, Exec. Director  
Massachusetts Chapter, NCPCA  
Massachusetts Committee for  
Children and Youth  
14 Beacon Street, Suite 706  
Boston, MA 02108  
(617) 742-8555  
(617) 742-7808 (fax)  
HandsNet: HN1126

Eli Newberger, President  
Massachusetts Chapter, NCPCA  
Massachusetts Committee for  
Children and Youth  
c/o The Children's Hospital  
300 Longwood Avenue  
Boston, MA 02115  
(617) 355-7982  
(617) 355-7979 (fax)  
E-mail:  
newberger@al.tch.harvard.edu

#### MICHIGAN

Jean Smith, Executive Director  
Michigan Contact  
P.O. Box 12096  
Lansing, MI 48901  
(517) 332-0482

#### MINNESOTA

Roy Garza, Executive Director  
Minnesota Chapter, NCPCA  
450 N. Syndicate Street  
Suite 290  
St. Paul, MN 55104  
(612) 641-1568  
(612) 641-0404 (fax)

Don Russell, President  
Minnesota Chapter, NCPCA  
1099 S. Snelling  
St. Paul, MN 55116  
(612) 582-3630  
(612) 582-3680 (fax)

#### MISSISSIPPI

Donna McLaurin, Exec. Dir.  
Mississippi Chapter, NCPCA  
Exchange Club Parent/Child  
Ctr. 2906 N. State, Suite 200  
Jackson, MS 39216  
(601) 366-0025  
(601) 366-0073 (fax)

Jane Emling, Chairperson  
Mississippi Chapter, NCPCA  
Exchange Club Parent/Child  
Center  
1931 Cherokee Drive  
Jackson, MS 39211-6509  
(601) 362-3995  
(601) 366-0073 (fax)

#### MISSOURI

Lucia Erickson-Kincheloe  
Executive Director  
Missouri Chapter, NCPCA  
Missouri Committee to Prevent  
Child Abuse  
308 E. High Street, Suite 303  
Jefferson City, MO 65101  
(573) 634-5223  
(573) 635-8499 (fax)  
HandsNet: HN2469

Dwain Hovis, President  
Missouri Chapter, NCPCA  
Missouri Committee to Prevent  
Child Abuse  
c/o Citibank EBT Services  
915 SW Boulevard, Suite L  
Jefferson City, MO 65109  
(573) 634-2724  
(573) 634-3407 (fax)

**MONTANA**

Jeanne Kemmis  
Executive Director  
Montana Chapter, NCPCA  
Montana Council for Families  
P.O. Box 7533  
127 E. Main, Suite 209  
Missoula, MT 59807  
(406) 728-9449  
(406) 728-9459 (fax)  
HandsNet: HN1780

Jeanne Kemmis, Exec. Director  
Jessica Stickney, President  
Montana Chapter, NCPCA  
Montana Council for Families  
2206 Main Street  
Miles City, MT 59301  
(406) 232-1100  
(406) 232-0799, Attn: Dr.  
Stickney (fax)

**NEVADA**

Dr. Paula Ford, Exec. Director  
Nevada Chapter, NCPCA  
We Can, Inc.  
3441 W. Sahara, Suite C-3  
Las Vegas, NV 89102  
(702) 368-1533  
(702) 368-1540 (fax)  
HandsNet: HN1699

Russell Shoemaker, President  
Nevada Chapter, NCPCA  
We Can, Inc.  
Las Vegas Metro Police Dept.  
8265 Hidden Crossing Lane  
Las Vegas, NV 89129  
(702) 438-3495  
(702) 229-3073 (fax)

**NEW HAMPSHIRE**

Monique Devine, Acting Dir.  
NH Chapter, NCPCA  
New Hampshire Task Force to  
Prevent Child Abuse  
P.O. Box 607, 44 Warren Street  
Concord, NH 03302  
(603) 225-5441  
(603) 228-5322 (fax)  
E-mail: tsmdevine@aol.com

Kevin Hamilton, President  
NH Chapter, NCPCA  
New Hampshire Task Force to  
Prevent Child Abuse  
c/o Porter, McGee PR  
1001 Elm Street  
Manchester, NH 03101  
(603) 669-8865  
(603) 669-8025 (fax)

**NEW JERSEY**

Sharon Copeland, Exec. Dir.  
New Jersey Chapter, NCPCA  
Prevent Child Abuse NJ, Inc.  
35 Halsey Street, Suite 300  
Newark, NJ 07102-3031  
(201) 643-3710  
(201) 643-9222 (fax)  
HandsNet: HN1874

Maura Somers Dughi, President  
New Jersey Chapter, NCPCA  
Prevent Child Abuse NJ, Inc.  
525 Valley Road  
Watchung, NJ 07060  
(201) 643-3710  
(908) 668-4321 (fax)

**NEW MEXICO**

Lori Campbell, Exec. Director  
New Mexico Chapter, NCPCA  
Prevent Child Abuse Santa Fe  
P.O. Box 15082  
Santa Fe, NM 87506  
(505) 471-6909  
(505) 983-2492 (fax)

Trish Steindler, President  
New Mexico Chapter, NCPCA  
Prevent Child Abuse Santa Fe  
P.O. Box 15082  
Santa Fe, NM 87506  
(505) 471-6909  
(505) 983-1583 (fax)

**NEW YORK**

James Cameron, Exec. Director  
National Chapter, NCPCA  
NY Committee to Prevent Child  
Abuse: NY State  
134 S. Swan Street  
Albany, NY 12210  
(518) 445-1273  
(518) 436-5889 (fax)  
HandsNet: HN1657  
E-mail: ncpcanys@aol.com  
Website:  
[http://child.cornell.edu/  
ncpca/home.html](http://child.cornell.edu/ncpca/home.html)

William Hayes, President  
New York Chapter, NCPCA  
National Committee to Prevent  
Child Abuse: NY State  
Bassett Health Care  
Atwell Road  
Cooperstown, NY 13326  
(607) 547-3456

**NORTH CAROLINA**

Jennifer Tolle, Exec. Director  
NC Chapter, NCPCA  
Prevent Child Abuse NC  
3344 Hillsborough Street  
Suite 100D  
Raleigh, NC 27607  
(919) 829-8009  
(919) 832-0308 (fax)  
HandsNet: HN2200  
Website:  
[www.pagecreator.com/~pca](http://www.pagecreator.com/~pca)

Lynn Lewis, President  
NC Chapter, NCPCA  
Prevent Child Abuse NC  
2140 Rolston Drive  
Charlotte, NC 27207  
(704) 347-2746

**NORTH DAKOTA**

Kathy Mayer, Exec. Director  
North Dakota Chapter, NCPCA  
ND Committee to Prevent  
Child Abuse  
P.O. Box 1213  
418 E. Rosser, Suite 303  
Bismarck, ND 58502-1213  
(701) 223-9052  
(701) 255-1904 (fax)

Jenny Buell, President  
North Dakota Chapter, NCPCA  
ND Committee to Prevent  
Child Abuse  
1231 E. Highland Acres Road  
Bismarck, ND 58501  
(701) 255-7399  
(701) 255-7167 (fax)

**OHIO**

Debbie Sendek, Exec. Director  
Ohio Chapter, NCPCA  
OH Committee to Prevent Child  
Abuse  
Timken Hall, Suite 130  
700 Children's Drive  
Columbus, OH 43205  
(614) 722-6800  
(614) 722-5510 (fax)  
E-mail: dsendek@chi.osu.edu

Sandra Mueller, Chairperson  
Ohio Chapter, NCPCA  
OH Committee to Prevent Child  
Abuse  
10424 Wellington Boulevard  
Powell, OH 43065  
(614) 766-6743

**OKLAHOMA**

Debbie Richardson, Exec. Dir.  
Oklahoma Chapter, NCPCA  
OK Committee to Prevent Child  
Abuse  
Citizen's Tower, Suite 340  
2200 Classen Boulevard  
Oklahoma City, OK 73106  
(405) 525-0688  
(405) 525-0689 (fax)  
E-mail: ocpc@juno.com

Rev. Mike Albert, President  
Oklahoma Chapter, NCPCA  
OK Committee to Prevent Child  
Abuse  
c/o Yale Avenue Christian  
Church  
3616 S. Yale Avenue  
Tulsa, OK 74135  
(918) 747-1304  
(918) 747-7175 (fax)

**PENNSYLVANIA**

Terry Ferrier, Interim Director  
Central PA Chapter, NCPCA  
Child Abuse Prevention  
Committee of Central PA  
P.O. Box 7664  
1917B Olde Homestead Lane  
Lancaster, PA 17604  
(717) 393-4511  
(717) 393-6801 (fax)

Jennifer Goldbach, President  
Central PA Chapter, NCPCA  
Child Abuse Prevention  
Committee of Central PA  
901 Jade Avenue  
Lancaster, PA 17621  
(717) 285-5848

Christine Linville, Interim Dir.  
Greater Philadelphia Chapter,  
NCPCA  
Child Abuse Prevention  
Committee of Greater PA  
260 S. Broad Street, 18th Floor  
Philadelphia, PA 19102  
(215) 985-6893  
(215) 864-1085 (fax)

Yvonne Ruiz, President  
Greater Philadelphia Chapter,  
NCPCA  
Child Abuse Prevention  
Committee of Greater PA  
1738 Pine Street, 4A  
Philadelphia, PA 19103  
(215) 686-8067

**RHODE ISLAND**

Ted Whiteside, Exec. Director  
Rhode Island Chapter, NCPCA  
RI Committee to Prevent Child  
Abuse  
500 Prospect Street  
Pawtucket, RI 02860  
(401) 728-7920  
(401) 724-5850 (fax)

Joe Murray, President  
Rhode Island Chapter, NCPCA  
RI Committee to Prevent Child  
Abuse  
86 King Phillip Court  
Warwick, RI 02886  
(401) 732-1224, ext. 354

**SOUTH CAROLINA**

Janice Bolin, Executive Director  
Low Country SC Chapter,  
NCPCA  
Exchange Club Center for  
Prevention of Child Abuse  
5055 Lackawanna Boulevard  
North Charleston, SC  
29406-4522  
(803) 747-1339  
(803) 529-3202 (fax)

Lee Stubblefield, President  
Low Country SC Chapter,  
NCPCA  
Exchange Club Center for  
Prevention of Child Abuse  
3 Carriage Lane  
Charleston, SC 29407  
(803) 766-5112  
(803) 766-1389 (fax)

Beebe James, Exec. Director  
Midlands Chapter, NCPCA  
Council on Child Abuse and  
Neglect  
1800 Main Street, Suite 3A  
Columbia, SC 29201  
(803) 733-5430  
(803) 779-7803 (fax)

Sidney Wait, President  
Midlands Chapter, NCPCA  
Council on Child Abuse and  
Neglect  
c/o Continuum of Care for  
Emotionally Handicapped  
Children  
220 Stoneridge Drive, Suite 300  
Columbia, SC 29210  
(803) 253-6272

Russell Smith, Exec. Director  
Piedmont Chapter, NCPCA  
Piedmont Council for  
Prevention of Child Abuse  
301 University Ridge  
Suite 5100  
Greenville, SC 29601-3671  
(864) 467-7680  
(864) 467-7699 (fax)

Jeff Ezell, President  
Piedmont Chapter, NCPCA  
Piedmont Council for  
Prevention of Child Abuse  
c/o Gibbes & Clarkson, PA  
330 Coffee Street  
Greenville, SC 29616  
(864) 271-9580

#### TENNESSEE

Lynne Luther, Exec. Director  
Tennessee Chapter, NCPCA  
Child Abuse Prevention of TN  
3010 Ambrose Avenue  
Nashville, TN 37207  
(615) 227-2273  
(615) 227-6846 (fax)

Ed Van Voorhees, President  
Tennessee Chapter, NCPCA  
Child Abuse Prevention of TN  
c/o United Warehouse, Inc.  
713 Overton Park  
Nashville, TN 37215  
(615) 254-3326

#### TEXAS

Wendell Teltow, Exec. Director  
Texas Chapter, NCPCA  
TX Committee to Prevent Child  
12701 Research, Suite 303  
Austin, TX 78759  
(512) 250-8438  
(512) 250-8733 (fax)

Grace Rank, President  
Texas Chapter, NCPCA  
TX Committee to Prevent Child  
3446 Flour Bluff Road  
Corpus Cristi, TX 78418  
(512) 289-6501, ext. 110  
(512) 289-1867 (fax)

#### UTAH

Executive Director  
Utah Chapter, NCPCA  
UT Committee to Prevent Child  
Abuse  
40 E. South Temple,  
Suite 350-12  
Salt Lake City, UT 84111-1003  
(801) 532-3404  
(801) 359-3662 (fax)  
HandsNet: HN1988  
E-mail: ewitker@bitcorp.net  
Website: www.bitcorp.net/ucpca

Jeff Hansen, President  
Utah Chapter, NCPCA  
UT Committee to Prevent  
Child Abuse  
Murdock Travel Management  
5383 S. 900 East  
Salt Lake City, UT 84117  
(801) 267-5831

#### VERMONT

Linda Johnson, Exec. Director  
Vermont Chapter, NCPCA  
Prevent Child Abuse Vermont  
P.O. Box 829  
141 Main Street  
Montpelier, VT 05601  
(802) 229-5724  
(802) 223-5567 (fax)

Bob Donnola, Vice-President  
Vermont Chapter, NCPCA  
21 Juniper Ridge  
Shelburne, VT 05482  
(802) 985-1149  
(802) 985-2497 (fax)

Gilman Rood, Vice-President  
Vermont Chapter, NCPCA  
161 Austin Drive  
Burlington, VT 05401  
(802) 229-5724

#### VIRGINIA

Barbara Rawn, Exec. Director  
Virginia Chapter, NCPCA  
Prevent Child Abuse Virginia  
P.O. Box 12308  
219 E. Broad Street, 10th Floor  
Richmond, VA 23241  
(804) 775-1777  
(804) 775-0019 (fax)  
HandsNet: HN1774

Michard Sterret, President  
Virginia Chapter, NCPCA  
Prevent Child Abuse Virginia  
c/o Director, North Hampton  
County Social Services  
P.O. Box 568  
Easterville, VA 23347  
(804) 678-5153

#### WASHINGTON

Executive Director  
Washington Chapter, NCPCA  
Child Abuse Prevention  
Association of Washington  
c/o Board of Directors, CAPAW  
Business Office/CAPR  
6314 W. 19th Street, Suite 3  
Tacoma, WA 98466

Bruce Garner, President  
Washington Chapter, NCPCA  
CAP Association of Washington  
c/o Department of Corrections  
1801 Grove Street, Unit D  
Marysville, WA 98270  
(360) 658-2164

**WEST VIRGINIA**

Lauri McKeown, Coordinator  
West Virginia Contact  
P.O. Box 1653  
Huntington, WV 25717  
(304) 523-9587  
(304) 523-9595 (fax)

**WISCONSIN**

Sally Casper, Exec. Director  
Wisconsin Chapter, NCPA  
WI Committee to Prevent Child  
Abuse  
214 N. Hamilton  
Madison, WI 53703  
(608) 256-3374  
(608) 256-3378 (fax)  
HandsNet: HN4758  
E-mail: wcpca@juno.com

Allen Jacobsen, President  
Wisconsin Chapter, NCPA  
WI Committee to Prevent Child  
Abuse  
8001 Excelsior Drive  
Madison, WI 53717  
(608) 827-6400

**WYOMING**

Rose Kor, Executive Director  
Wyoming Chapter, NCPA  
Prevent Child Abuse Wyoming  
1120 Logan Avenue  
Cheyenne, WY 82001  
(307) 637-8622  
(307) 637-8622 (fax)  
E-mail: pcawyo@juno.com

Jean Phelan, President  
Wyoming Chapter, NCPA  
Prevent Child Abuse Wyoming  
1404 E. 17th Street  
Cheyenne, WY 82001  
(307) 637-6162





## Appendix 5

### FBI Field Offices

#### Alabama

Federal Bureau of Investigation  
2121 8<sup>th</sup> Avenue North, Room 1400  
Birmingham, AL 35203-2396  
Telephone: (205) 326-6166

Federal Bureau of Investigation  
One St. Louis Centre  
1 St. Louis Street  
Mobile, AL 36602  
Telephone: (334) 438-3674

#### Alaska

Federal Bureau of Investigation  
101 East Sixth Avenue  
Anchorage, AK 99501-2524  
Telephone: (907) 276-4441

#### Arizona

Federal Bureau of Investigation  
201 East Indianola, Suite 400  
Phoenix, AZ 85012-2080  
Telephone: (602) 279-5511

#### Arkansas

Federal Bureau of Investigation  
10825 Financial Centre Parkway, Suite 200  
Little Rock, AR 72211-3552  
Telephone: (501) 221-9100

#### California

Federal Bureau of Investigation  
Federal Office Building  
11000 Wilshire Boulevard, Suite 1700  
Los Angeles, CA 90024-3672  
Telephone: (310) 477-6565

Federal Bureau of Investigation  
4500 Orange Grove Avenue  
Sacramento, CA 95841-4025  
Telephone: (916) 481-9110

Federal Bureau of Investigation  
9797 Aero Drive  
San Diego, CA 92123-1800  
Telephone: (619) 565-1255

Federal Bureau of Investigation  
450 Golden Gate Avenue  
San Francisco, CA 94102-9523  
Telephone: (415) 553-7400

#### Colorado

Federal Bureau of Investigation  
Federal Office Building  
1961 Stout Street, Suite 1823  
Denver, CO 80294-1823  
Telephone: (303) 629-7171

#### Connecticut

Federal Bureau of Investigation  
Federal Office Building  
150 Court Street, Room 535  
New Haven, CT 06510-2020  
Telephone: (203) 777-6311

#### Delaware

All queries should be directed to the FBI field office in Baltimore, Maryland.

#### Florida

Federal Bureau of Investigation  
7820 Arlington Expressway, Suite 200  
Jacksonville, FL 32211-7499  
Telephone: (904) 721-1211

Federal Bureau of Investigation  
16320 Northwest Second Avenue  
North Miami Beach, FL 33169  
Telephone: (305) 944-9101

**Florida - continued**

Federal Bureau of Investigation  
500 Zack Street, Room 610  
Tampa, FL 33602-3917  
Telephone: (813) 273-4566

**Georgia**

Federal Bureau of Investigation  
2635 Century Parkway Northeast, Suite 400  
Atlanta, GA 30345-3112  
Telephone: (404) 679-9000

**Hawaii**

Federal Bureau of Investigation  
300 Ala Moana Boulevard, Room 4307  
Honolulu, HI 96850-0053  
Telephone: (808) 521-1411

**Idaho**

All queries should be directed to the FBI field office in Salt Lake City, Utah.

**Illinois**

Federal Bureau of Investigation  
E.M. Dirksen Federal Office Building  
219 South Dearborn Street, Room 905  
Chicago, IL 60604-1702  
Telephone: (312) 431-1333

Federal Bureau of Investigation  
400 West Monroe Street, Suite 400  
Springfield, IL 62704-1800  
Telephone: (217) 522-9675

**Indiana**

Federal Bureau of Investigation  
575 North Pennsylvania Street, Room 679  
Indianapolis, IN 46204-1524  
Telephone: (317) 639-3301

**Iowa**

All queries should be directed to the FBI field office in Omaha, Nebraska.

**Kansas**

All queries should be directed to the FBI field office in Kansas City, Missouri.

**Kentucky**

Federal Bureau of Investigation  
600 Martin Luther King Place, Room 500  
Louisville, KY 40202-2231  
Telephone: (502) 583-3941

**Louisiana**

Federal Bureau of Investigation  
1250 Poydras Street, Suite 2200  
New Orleans, LA 70113-1829  
Telephone: (504) 522-4671

**Maine**

All queries should be directed to the FBI field office in Boston, Massachusetts.

**Maryland**

Federal Bureau of Investigation  
7142 Ambassador Road  
Baltimore, MD 21244-2754  
Telephone: (410) 265-8080

**Massachusetts**

Federal Bureau of Investigation  
One Center Plaza, Suite 600  
Boston, MA 02108  
Telephone: (617) 742-5533

**Michigan**

Federal Bureau of Investigation  
Federal Office Building  
477 Michigan Avenue  
Detroit, MI 48226  
Telephone: (313) 965-2323

**Minnesota**

Federal Bureau of Investigation  
111 Washington Avenue South, Suite 1100  
Minneapolis, MN 55401-2176  
Telephone: (612) 376-3200

**Mississippi**

Federal Bureau of Investigation  
100 West Capitol Street, Room 1553  
Jackson, MS 39269  
Telephone: (601) 948-5000

**Missouri**

Federal Bureau of Investigation  
U.S. Courthouse  
811 Grand Avenue, Room 300  
Kansas City, MO 64106-1926  
Telephone: (816) 221-6100

Federal Bureau of Investigation  
1520 Market Street, Room 2704  
St. Louis, MO 63103-2686  
Telephone: (314) 589-2500

**Montana**

All queries should be directed to the FBI field office in Salt Lake City, Utah.

**Nebraska**

Federal Bureau of Investigation  
10755 Burt Street  
Omaha, NE 68114-2000  
Telephone: (402) 493-8688

**Nevada**

Federal Bureau of Investigation  
700 East Charleston Boulevard  
Las Vegas, NV 89104-1545  
Telephone: (702) 385-1281

**New Hampshire**

All queries should be directed to the FBI field office in Boston, Massachusetts.

**New Jersey**

Federal Bureau of Investigation  
1 Gateway Center  
Market Street  
Newark, NJ 07102-9889  
Telephone: (201) 622-5613

**New Mexico**

Federal Bureau of Investigation  
415 Silver Street Southwest, Suite 300  
Albuquerque, NM 87102  
Telephone: (505) 224-2000

**New York**

Federal Bureau of Investigation  
445 Broadway, Fifth Floor  
Albany, NY 12207-2963  
Telephone: (518) 465-7551

Federal Bureau of Investigation  
One FBI Plaza  
Buffalo, NY 14202-2698  
Telephone: (716) 856-7800

Federal Bureau of Investigation  
26 Federal Plaza  
New York, NY 10278-0004  
Telephone: (212) 384-1000

**North Carolina**

Federal Bureau of Investigation  
400 South Tyron Street, Suite 900  
Charlotte, NC 28285-0001  
Telephone: (704) 377-9200

**North Dakota**

All queries should be directed to the FBI field office in Minneapolis, Minnesota.

**Ohio**

Federal Bureau of Investigation  
550 Main Street, Room 9000  
Cincinnati, OH 45273-8501  
Telephone: (513) 421-4310

Federal Bureau of Investigation  
Federal Office Building  
1240 East Ninth Street, Room 3005  
Cleveland, OH 44199-9912  
Telephone: (216) 522-1400

**Oklahoma**

Federal Bureau of Investigation  
50 Penn Place, Suite 1600  
Oklahoma City, OK 73118-1886  
Telephone: (405) 842-7471

**Oregon**

Federal Bureau of Investigation  
Crown Plaza  
1500 Southwest First Avenue  
Portland, OR 97201-5828  
Telephone: (503) 224-4181

**Pennsylvania**

Federal Bureau of Investigation  
600 Arch Street, Eighth Floor  
Philadelphia, PA 19106  
Telephone: (215) 418-4500

Federal Bureau of Investigation  
U.S. Post Office Building  
700 Grant Street, Suite 300  
Pittsburgh, PA 15219-1906  
Telephone: (412) 471-2000

**Rhode Island**

All queries should be directed to the FBI field office in Boston, Massachusetts.

**South Carolina**

Federal Bureau of Investigation  
1835 Assembly Street, Room 1357  
Columbia, SC 29201-2430  
Telephone: (803) 254-3011

**South Dakota**

All queries should be directed to the FBI field office in Minneapolis, Minnesota.

**Tennessee**

Federal Bureau of Investigation  
710 Locust Street, Suite 600  
Knoxville, TN 37902-2537  
Telephone: (423) 544-0751

Federal Bureau of Investigation  
225 North Humphreys Boulevard  
Memphis, TN 38120-2107  
Telephone: (901) 747-4300

**Texas**

Federal Bureau of Investigation  
1801 North Lamar, Room 300  
Dallas, TX 75202-1795  
Telephone: (214) 720-2200

Federal Bureau of Investigation  
700 East San Antonio Avenue, Suite C-600  
El Paso, TX 79901-7020  
Telephone: (915) 533-7451

Federal Bureau of Investigation  
2500 East TC Jester, Room 200  
Houston, TX 77008-1300  
Telephone: (713) 868-2266

Federal Bureau of Investigation  
615 East Houston Street, Room 200  
San Antonio, TX 78205-9998  
Telephone: (210) 225-6741

**Utah**

Federal Bureau of Investigation  
257 East 200 Street South, Suite 1200  
Salt Lake City, UT 84111-2048  
Telephone: (801) 579-1400

**Vermont**

All queries should be directed to the FBI field office in Albany, New York.

**Virginia**

Federal Bureau of Investigation  
150 Corporate Boulevard  
Norfolk, VA 23502-4999  
Telephone: (757) 455-0100

Federal Bureau of Investigation  
111 Greencourt Road  
Richmond, VA 23228-4948  
Telephone: (804) 261-1044

**Washington**

Federal Bureau of Investigation  
915 Second Avenue, Room 710  
Seattle, WA 98174-1096  
Telephone: (206) 622-0460

**Washington, D.C.**

Federal Bureau of Investigation  
Washington Metropolitan Field Office  
1900 Half Street SW.  
601 4<sup>th</sup> Street Northwest  
Washington, DC 20535-0002  
Telephone: (202) 252-7801

**West Virginia**

All queries should be directed to the FBI field office in Pittsburgh, Pennsylvania.

**Wisconsin**

Federal Bureau of Investigation  
330 East Kilbourn Avenue, Suite 600  
Milwaukee, WI 53202-6627  
Telephone: (414) 276-4684

**Wyoming**

All queries should be directed to the FBI field office in Denver, Colorado.

**Puerto Rico**

Federal Bureau of Investigation  
U.S. Courthouse and Federal Office Building  
150 Carlos Chardon Avenue, Room 526  
Hato Rey, PR 00918-1716  
Telephone: (809) 754-6000



## Appendix 6

### FBI Legal Attaches

**Athens**

Legal Attache  
American Embassy  
PSC 108, Box 45  
APO AE 09842  
Telephone:(011-30-1) 721-2951 ext.447

**Bangkok**

Legal Attache  
American Embassy-Box 67  
APO AP 96546  
Telephone:(011-66-2) 205-4366

**Bern**

American Embassy Bern  
Jubilaumstrasse 93  
CH 3005 Bern, Switzerland  
Telephone:(011-41-31) 357-7011

**Bogota**

US Embassy-Bogota  
Unit #5124-Legat  
APO AA 34038  
Telephone:(011-57-1) 315-0811 ext. 2575

**Bonn**

Off. Of the Legal Attache  
PSC 117, Box 310  
APO AA 09080  
Telephone:(011-49-228) 3391

**Bonn, Berlin Suboffice**

U.S.Embassy Off. Berlin-Legat  
PSC 120, Box 1000  
APO AE 09265  
Telephone:(011-49-30) 238-5174

**Bonn, Frankfurt Suboffice**

American Consulate-Frankfurt  
Office of Legat Attache  
PSC 115  
APO AE 09213  
Telephone:(011-49-69) 7535-3780

**Brazilia**

Telephone:(55-61) 321-7272

**Bridgetown**

Legal Attache  
American Embassy  
Bridgetown, Barbados  
FPO AA 34055  
Telephone:(246) 436-4950 ext. 2236

**Brussels**

Legal Attache  
LEG/EMB  
PSC 82, Box 002  
APO AE 09724  
Telephone:(011-32-2)  
508-2111 ext. 2551,2552

**Budapest International Law Enforcement**

**Agency**  
Budapest 1126  
Böszörményi út 21  
Hungary  
Telephone:(011-36-1) 267-4400

**Cairo**

American Embassy  
Unit 64900, Box 39  
APO AE 09839-4900  
Telephone:(011-202) 355-7371

**Canberra**  
US Embassy  
Legat  
APO AP 96549  
Telephone:(011-61-6) 270-5000 or  
5900 evenings, ext. 862,982

**Caracas**  
American Embassy Unit 4966  
APO AA 34037  
Telephone:(011-58-2) 977-2011

**Hong Kong**  
Legal Liaison Office  
American Consulate  
PSC 464, Box 30  
FPO AP 96522-0002  
Telephone:(011-852) 2841-2282  
2356, 2348

**Interpol**  
ICPO-Interpol General Secretariat  
200 Charles de Gaulle  
69006 Lyon, France  
Telephone:(011-33-4) 7244-7213

**Islamabad**  
Legal Attache Office  
American Embassy  
Unit 62219  
APO AE 09812-2219  
Telephone:(011-92-51) 826-161 ext.2205

**Kiev**  
American Embassy  
Department of State-Kiev  
Washington D.C. 20521-5850  
Telephone:(011-380) 44-244-7345  
ext. 237, 247

**London**  
American Embassy  
PSC 801 Box 02  
FPO AE 09498-4002  
Telephone:(011-44-171) 499-9000  
ext. 2478, 2479, 2475

**Madrid**  
PSC 61, Box 0001  
APO AE 09642  
Telephone:(011-34-1) 587-2200

**Manila**  
American Embassy  
Legat Attache  
FPO AP 96515  
Telephone:(011-63-2) 523-1323

**Mexico City**  
American Embassy  
P.O. Box 3087  
Laredo, Texas 78044-3087  
Telephone:(011-52-5) 211-0042  
ext. 3700 through 3703

**Mexico City, Guadalajara Suboffice**  
Telephone:(011-52-38) 25-2998

**Mexico City, Monterrey Suboffice**  
Telephone:(011-52-83) 43-2120  
ext. 469

**Montevideo**  
Unit 4503  
APO AA 34035  
Telephone:(011-598-2) 48-77-77  
Ask for Marines

**Moscow**  
American Embassy, Moscow  
PSC 77, Legat  
APO AE 09721  
Telephone:(011-7-095) 252-2459  
ext. 5222

**Ottawa**  
US Embassy-Canada  
P.O. Box 1711  
Ogdensburg, N.Y. 13669  
Telephone:(613) 238-5335 ext.206



**Panama City**

American Embassy Panama  
Unit 0945  
APO AA 34002  
Telephone:(011-507) 227-1777  
227-1377 evenings

**Paris**

Paris Embassy(LEG)  
PSC 116, A-324  
APO AE 09777  
Telephone:(011-33-1) 4312-2222  
ext. 2400

**Pretoria**

American Embassy, Pretoria  
U.S. Department of State  
Washington, D.C. 20521-9300  
Telephone:(011-27-12) 342-1048, ext. 2349

**Riyadh**

American Embassy  
AMEMB, Unit 61340  
APO AE 09803-1307  
Telephone:(011-966) 1488-3800 ext. 1555

**Rome**

PSC 59, Box 43  
APO AE 09624  
Telephone:(011-39-6) 4674-2710  
2711, 2392

**Santiago**

Office of the Legal Attache  
American Embassy-Santiago  
Unit 4131 (Legat)  
APO AA 34033  
Telephone:(011-56-2) 232-2600  
Ask for Marines

**Tallinn**

American Embassy  
PSC 78, Box T  
APO AE 09723  
Telephone:(011-372-6) 312-021 ext.210

**Tel Aviv**

US Embassy  
Legat  
Unit 7228  
APO AE 09830  
Telephone:(011-9723) 519-7575

**Tokyo**

American Embassy  
Unit 45004, Box 223  
APO AE 96337-0001  
Telephone:(011-81-3) 3224-5000

**Vienna**

American Embassy-Vienna  
DOS, Legat  
Washington D.C. 20521-9900  
Telephone:(011-43-1) 31-339

**Warsaw**

American Embassy-Warsaw  
Department of State  
Washington D.C. 20521-5010  
Telephone: (011-4822) 628-3041  
evenings: 628-0638

6-4



## Appendix 7

### Crime Victims Compensation/Assistance State Agencies and Programs

#### VICTIM COMPENSATION PROGRAMS

##### **ALABAMA**

Randy Helms, Executive Director  
Alabama Crime Victims Compensation  
100 N. Union Street  
P.O. Box 1548  
Montgomery, AL 36102-1548  
Telephone: (334) 242-4007

##### **ALASKA**

Susan Browne, Administrator  
Department of Public Safety  
Violent Crimes Compensation Board  
450 Whittier Street, Room 104  
Juneau, AK 99811-1200  
Telephone: (907) 465-3040

##### **ARIZONA**

Rita J. Yorke, Victim Services Coordinator  
Criminal Justice Commission  
1501 West Washington, Suite 207  
Phoenix, Arizona 85007  
Telephone: (602) 542-1928

##### **ARKANSAS**

Ginger B. Bailey, Director  
Crime Victims Reparations Board  
323 Center Street, Suite 200  
Little Rock, AR 72201  
Telephone: (501) 682-1323

#### VICTIM ASSISTANCE PROGRAMS

##### **ALABAMA**

Gilbert (Doug) Miller, Section Chief  
Department of Economic and Community  
Affairs  
Law Enforcement Planning Division  
401 Adams Avenue  
P.O. Box 5690  
Montgomery, AL 36103-5690  
Telephone: (334) 242-5843

##### **ALASKA**

Jayne E. Andreen, Executive Director  
Department of Public Safety  
Council on Domestic Violence and  
Sexual Assault  
P.O. Box 111200  
Juneau, AK 88911-1200  
(907) 465-4356

##### **ARIZONA**

Lynn Pirkle, Grant Coordinator  
Department of Public Safety  
2010 West Encanto Blvd.  
Phoenix, AZ 85005-6638  
Telephone: (602) 223-2465

##### **ARKANSAS**

Jerry Duran, Administrator  
Department of Finance & Administration  
P.O. Box 3278  
Little Rock, AR 72203  
Telephone: (501) 682-1071

**VICTIM COMPENSATION PROGRAMS**

**CALIFORNIA**

Ted Boughton, Deputy Executive Officer  
State of California  
State Board of Control  
P.O. Box 3036  
Sacramento, CA 95814  
Telephone: (916) 323-3432

**COLORADO**

Carol Poole, Deputy Director  
Division of Criminal Justice  
Department of Public Safety  
700 Kipling Street, Suite 1000  
Denver, CO 80215  
Telephone: (303) 239-4446

**CONNECTICUT**

Carole R. Watkins, Director  
Office of Victim Services  
Connecticut Judicial Branch  
1158 Silas Deane Highway  
Wethersfield, CT 06109  
Telephone: (860) 529-3089

**DELAWARE**

Ann L. DelNegro, Executive Director  
Violent Crimes Compensation  
Board  
1500 East Newport Pike, Suite 10  
Wilmington, DE 19804  
Telephone: (302) 995-8383

**DISTRICT OF COLUMBIA**

Laura Banks Reed, Director  
Crime Victims Compensation Program  
515 5th Street, Suite 503  
Washington D.C. 20001  
Telephone: (202) 879-4216

**VICTIM ASSISTANCE PROGRAMS**

**CALIFORNIA**

Kirby Everhart, Chief  
Victim Services & Violence Prevention  
Office of Criminal Justice Planning  
1130 K Street, Suite 300  
Sacramento, CA 95814  
Telephone: (916) 327-3687

**COLORADO**

Candace Grosz, VOCA Administrator  
Division of Criminal Justice  
Department of Public Safety  
700 Kipling Street, Suite 1000  
Denver, CO 80215  
Telephone: (303) 239-5703

**CONNECTICUT**

Carole R. Watkins, Director  
Office of Victim Services  
Connecticut Judicial Branch  
1158 Silas Deane Highway  
Wethersfield, CT 06109  
Telephone: (860) 529-3089

**DELAWARE**

Corrine Pearson, Program Manager  
Criminal Justice Council  
Carvel State Office Building  
820 North French, 4th Floor  
Wilmington, DE 19801  
Telephone: (302) 577-3697

**DISTRICT OF COLUMBIA**

Sandra R. Manning, Director  
D.C. Office of Grants Management  
717 14th Street N.W., Suite 400  
Washington, D.C. 20005  
Telephone: (202) 727-6537

## VICTIM COMPENSATION PROGRAMS

### **FLORIDA**

Mary Vancore, Chief  
Division of Victim Services and  
Criminal Justice Programs  
Office of the Attorney General  
Department of Legal Affairs  
The Capitol  
Tallahassee, FL 32399-1050  
Telephone: (904) 414-3301

### **GEORGIA**

Derek L. Marchman, Program Manager  
Crime Victim Compensation Program  
503 Oak Place, Suite 540  
Atlanta, GA 30349  
Telephone: (404) 559-4949

### **HAWAII**

Laraine Koga, Administrator  
Office of the Attorney General  
425 Queen Street, Room 221  
Honolulu, HI 96813  
Telephone: (808) 586-1282

### **IDAHO**

Mr. Fran Koch, Director  
Crime Victims Compensation Bureau  
c/o Idaho Industrial Commission  
P.O. Box 83720  
Boise, ID 83720-0041  
Telephone: (208) 334-6070

### **ILLINOIS**

Katherine Parker, Administrator  
Illinois Court of Claims  
Crime Victims Division  
Attorney General's Office  
100 W. Randolph, 13th Floor  
Chicago, Illinois 60601  
Telephone: (312) 814-2581

## VICTIM ASSISTANCE PROGRAMS

### **FLORIDA**

Cynthia Rogers, Chief  
Division of Victim Services and  
Criminal Justice Programs  
Office of the Attorney General  
Department of Legal Affairs  
The Capitol, PL- 01  
Tallahassee, FL 32399-1050  
Telephone: (904) 414-3300

### **GEORGIA**

John Cook, Grant Manager  
Criminal Justice Coordinating Council  
503 Oak Place, Suite 540  
Atlanta, GA 30349  
Telephone: (404) 559-4949

### **HAWAII**

Adrian Kwock, Planning Specialist  
Office of the Attorney General  
425 Queen Street, Room 221  
Honolulu, HI 96813  
Telephone: (808) 586-1282

### **IDAHO**

Celia V. Heady, Executive Director  
Department of Health & Welfare  
Council on Domestic Violence  
450 West State Street, 9th Floor  
Boise, ID 83720-0036  
Telephone: (208) 334-5580

### **ILLINOIS**

Candice M. Kane, Program Supervisor  
Criminal Justice Information Authority  
120 S. Riverside Plaza, 10th Floor  
Chicago, IL 60606  
Telephone: (312) 793-8550

## VICTIM COMPENSATION PROGRAMS

### **INDIANA**

Gwendolyn Allen, Program Director  
Violent Crime Compensation Fund  
Criminal Justice Institute  
302 West Washington Street, E209  
Indianapolis, IN 46204  
Telephone: (312) 233-3383

### **IOWA**

Kelly Brodie, Deputy Director  
Department of Justice  
Crime Victim Assistance Program  
Old Historical Building  
1125 East Grand Avenue  
Des Moines, IA 50319-0238  
Telephone: (515) 281-5044

### **KANSAS**

Frank Henderson, Director  
KS Crime Victims Compensation Board  
700 SW Jackson Street, Suite 400  
Topeka, KS 66603-3756  
Telephone: (913) 296-2359

### **KENTUCKY**

Jackie Howell, Executive Director  
Crime Victim Compensation Board  
115 Myrtle Avenue  
Frankfort, Kentucky 40601-3113  
Telephone: (502) 564-7986

### **LOUISIANA**

Robert Wertz, Program Manager  
Louisiana Commission on Law  
Enforcement  
1885 Wooddale Boulevard, Suite 708  
Baton, Rouge, LA 70806-1511  
Telephone: (504) 925-1998

## VICTIM ASSISTANCE PROGRAMS

### **INDIANA**

Kimberly I. Howell, Program Director  
Criminal Justice Institute  
302 West Washington Street, E209  
Indianapolis, IN 46204  
Telephone: (317) 233-3341

### **IOWA**

Virginia Beane, Administrator  
Department of Justice  
Crime Victim Assistance Program  
Old Historical Building  
1125 East Grand Avenue  
Des Moines, IA 50319-0238  
Telephone: (515) 281-5044

### **KANSAS**

Juliene A. Maska, Director  
Office of the Attorney General  
301 SW 10th Avenue  
Topeka, KS 66612-1597  
Telephone: (913) 296-2215

### **KENTUCKY**

Donna Langley, VOCA Program Mngr.  
Kentucky Justice Cabinet  
Bush Building  
403 Wapping Street, 2nd Floor  
Frankfort, KY 40601  
Telephone: (502) 564-7554

### **LOUISIANA**

Rosanna Marino, Program Manager  
Louisiana Commission on Law  
Enforcement  
1885 Wooddale Boulevard, Suite 708  
Baton Rouge, LA 70806-1442  
Telephone: (504) 925-1757

**VICTIM COMPENSATION PROGRAMS**

**MAINE**

Deborah Shaw-Rice, Director  
Office of the Attorney General  
Crime Victim Compensation Program  
State House Station 6  
Augusta, ME 04333  
Telephone: (297) 626-8589

**MARYLAND**

Esther Scaljon, Director  
Department of Public Safety  
and Correctional Services  
Criminal Injuries Compensation Board  
6776 Resisterstown Road, Suite 313  
Baltimore, MD 21215-2340  
Telephone: (410) 764-4214

**MASSACHUSETTS**

Judith E. Beals, Chief  
Office of the Attorney General  
Victim Compensation Division  
One Ashburton Place  
Boston, MA 02108-1698  
Telephone: (617) 727-2200

**MICHIGAN**

Michael J. Fullwood, Administrator  
Crime Victims Compensation Board  
P.O. Box 30026 - 320 South Walnut  
Lansing, MI 48909  
Telephone: (517) 373-0979

**MINNESOTA**

Marie Bibus, Executive Director  
Crime Victims Reparations Board  
Town Square, Suite 100-C  
444 Cedar Street  
St. Paul, MN 55101-2156  
Telephone: (612) 282-6267

**VICTIM ASSISTANCE PROGRAMS**

**MAINE**

Jeannette C. Talbot, Administrator  
Department of Human Services  
Bureau of Social Services  
State House Station 11  
Augusta, ME 04333  
Telephone: (207) 289-5060

**MARYLAND**

Adrienne Siegel, Assistant Director  
Office of Transitional Services  
MD Department of Human Resources  
311 West Saratoga Street, Room 272  
Baltimore, MD 21201-3521  
Telephone: (410) 767-7477

**MASSACHUSETTS**

Alyssa Kazin, Program Specialist  
Victim & Witness Assistance Board  
Office for Victims Assistance  
100 Cambridge Street, Room 1104  
Boston, MA 02202  
Telephone: (617) 727-5200

**MICHIGAN**

Leslie O'Reilly  
Grants Management Division  
Office of Contract Management  
P.O. Box 30026 - 320 South Walnut  
Lansing, MI 48909  
Telephone: (517) 373-1826

**MINNESOTA**

Emilie Tan-Graf, Grant Administrator  
Department of Corrections  
1450 Energy Park Drive  
Suite 200  
St. Paul, MN 55108-5129  
Telephone: (612) 642-0221

## VICTIM COMPENSATION PROGRAMS

### **MISSISSIPPI**

Sandra K. Morrison, Hearing Officer  
Department of Finance and  
Administration  
Box 267  
Jackson, MS 39205  
Telephone: (601) 359-6766

### **MISSOURI**

Sandy Wright, Program Manager  
Division of Workers' Compensation  
Crime Victims Compensation  
P.O. Box 504  
Jefferson City, MO 65102  
Telephone: (573) 526-3511

### **MONTANA**

Dara Lynn Smith, Program Officer  
Board of Crime Control Division  
Crime Victims Unit  
Scott Hart Building  
303 North Roberts, 4th Floor  
Helena, MT 59620-1408  
Telephone: (406) 444-3653

### **NEBRASKA**

Nancy Steeves, Federal Aid Administrator  
Crime Victims Reparation Board  
Commission on Law Enforcement  
and Criminal Justice  
P.O. Box 94946  
Lincoln, NE 68509  
Telephone: (402) 471-2194

### **NEVADA\***

Bryan Nix, Coordinator  
Victims of Crime Program  
NV Department of Administration  
555 E. Washington, Suite 3200  
Las Vegas, NV 89101  
Telephone: (702) 486-2740

## VICTIM ASSISTANCE PROGRAMS

### **MISSISSIPPI**

Ezzard C. Stamps, Program Manager  
Department of Public Safety  
Division of Public Safety & Planning  
401 North West Street, 8th Floor  
Jackson, MS 39225-3039  
Telephone: (601) 359-7880

### **MISSOURI**

Vicky Scott, Program Specialist  
Department of Public Safety  
Truman Building, Room 870  
P.O. Box 749 - 301 West High St.  
Jefferson City, MO 65102-0749  
Telephone: (573) 751-4905

### **MONTANA**

Wendy Sturn, Victim Coordinator  
Board of Crime Control Division  
Scott Hart Building  
303 North Roberts, 4th Floor  
Helena, MT 59501  
Telephone: (406) 444-3604

### **NEBRASKA**

Nancy Steeves, Federal Aid Administrator  
Crime Victims Reparation Board  
Commission on Law Enforcement  
and Criminal Justice  
P.O. Box 94946  
Lincoln, NE 68509  
Telephone: (402) 471-2194

### **NEVADA**

Chris S. Graham, Program Manager  
Department of Human Resources  
Division of Child & Family Services  
2655 Enterprise Road  
Reno, NV 89512  
Telephone: (702) 688-1628



**VICTIM COMPENSATION PROGRAMS**

**NEW HAMPSHIRE**

Susan Paige-Morgan  
NH Department of Justice  
33 Capitol Street  
Concord, NH 03301-6397  
Telephone: (603) 271-3658

**NEW JERSEY**

Jim Casserly  
Victims of Crime Compensation Board  
50 Park Place, 5th Floor  
Newark, NJ 07102  
Telephone: (201) 648-2107

**NEW MEXICO**

Larry Tackman, Director  
Crime Victims Reparation Commission  
8100 Mountain Road, N.E., Suite 106  
Albuquerque, NM 87110  
Telephone: (505) 841-9432

**NEW YORK**

Patricia Pouloupoulos, Administrative Officer  
New York Crime Victims Board  
845 Central Avenue, South 3, Suite 107  
Albany, NY 12206  
Telephone: (518) 457-8063

**NORTH CAROLINA**

Gary B. Eichelberger, Director  
Victims Compensation Commission  
Department of Crime Control and  
Public Safety  
P.O. Box 29588 - 512 North Salisbury St.  
Raleigh, NC 27611-7687  
Telephone: (919) 733-7974

**VICTIM ASSISTANCE PROGRAMS**

**NEW HAMPSHIRE**

Gale Dean  
NH Department of Justice  
33 Capitol Street  
Concord, NH 03301-6397  
Telephone: (603) 271-7987

**NEW JERSEY**

Kathleen A. Kauker-Lawrie  
Department of Law and Public Safety  
Division of Criminal Justice  
Office of Victim/Witness Advocacy  
25 Market Street, CN 085  
Trenton, New Jersey 08625-0085  
Telephone: (609) 984-7347

**NEW MEXICO**

Larry Tackman, Director  
Crime Victims Reparation Commission  
8100 Mountain Road, N.E., Suite 106  
Albuquerque, NM 87110  
Telephone: (505) 841-9432

**NEW YORK**

Peggy Donnelly, Assistant Director  
New York Crime Victims Board  
845 Central Avenue  
Albany, NY 12206  
Telephone: (518) 457-1779

**NORTH CAROLINA**

Barry Bryant, Criminal Justice Planner  
Governor's Crime Commission  
Department of Crime Control & Public Safety  
3824 Barrett Drive  
Raleigh, NC 27609-7220  
Telephone: (919) 571-4736

**VICTIM COMPENSATION PROGRAMS**

**NORTH DAKOTA**

Paul J. Coughlin, Administrator  
Division of Parole & Probation  
North Dakota Department of Corrections  
Crime Victims Reparations  
3303 E. Main - Box 5521  
Bismarck, ND 58502-5521  
Telephone: (701) 328-6195

**OHIO**

Miles C. Durfey, Clerk  
Victims of Crime Compensation Program  
Court of Claims of Ohio  
65 East State Street, Suite 1100  
Columbus, Ohio 43215  
Telephone: (614) 466-8439

**OKLAHOMA**

Suzanne K. Breedlove, Administrator  
Crime Victims Compensation Board  
2200 Classen Blvd., Suite 1800  
Oklahoma City, OK 73106-5811  
Telephone: (405) 557-6704

**OREGON**

Mary Ellen Johnson, Director  
Department of Justice  
Crime Victims' Compensation Program  
1162 Court Street, N.E.  
Salem, OR 97310  
Telephone: (503) 378-5348

**PENNSYLVANIA**

Carol Lavery, Director  
Pennsylvania Commission on Crime  
and Delinquency  
Bureau of Victims Services  
Victims Compensation Division  
P.O.ox 1167  
Harrisburg, PA 17108-1167  
Telephone: (717) 787-2040

**VICTIM ASSISTANCE PROGRAMS**

**NORTH DAKOTA**

Paul J. Coughlin, Administrator  
Division of Parole & Probation  
North Dakota Department of Corrections  
Crime Victim Reparations  
3303 E. Main - Box 5521  
Bismarck, ND 58502-5521  
Telephone: (701) 328-6195

**OHIO**

Sharon Boyer, Administrator  
Ohio Office of the Attorney General  
Crime Victim Assistance Office  
65 East State Street, 8th Floor  
Columbus, OH 43215-4321  
Telephone: (614) 466-5610

**OKLAHOMA**

Suzanne K. Breedlove, Administrator  
District Attorneys Council  
2200 Classen Boulevard, Suite 1800  
Oklahoma City, OK 73106-5811  
Telephone: (405) 557-6704

**OREGON**

Mary Ellen Johnson, Director  
Department of Justice  
Crime Victims' Assistance Section  
1162 Court Street, N.E.  
Salem, OR 97310  
Telephone: (503) 378-5348

**PENNSYLVANIA**

John H. Kunkle, Program Manager  
Pennsylvania Commission on Crime  
and Delinquency  
P.O. Box 1167 - 2nd & Chestnut Sts.  
Federal Square Station  
Harrisburg, PA 17108-1167  
Telephone: (717) 787-8559 x 3031

**VICTIM COMPENSATION PROGRAMS**

**RHODE ISLAND**

Barbara Boden, Program Administrator  
General Treasurer's Office  
Crime Victims Compensation Program  
49 Fountain Street, 7th Floor  
Telephone: (401) 277-2212

**SOUTH CAROLINA**

Renee Graham, Program Manager  
Division of Victim Assistance  
Office of the Governor, Room 401  
1205 Pendleton Street, Edgar Brown Bldg.  
Columbia, SC 29201  
Telephone: (803) 734-1930

**SOUTH DAKOTA**

Ann M. Holzhauser, Administrator  
Office of Adult Service  
Crime Victims' Compensation Commission  
700 Governors Drive  
Pierre, SD 57501-2291  
Telephone: (605) 773-6317

**TENNESSEE**

Susan P. Clayton, Program Director  
Treasury Department  
Division of Claims Administration  
9th floor, Andrew Jackson Bldg.  
Nashville, TN 37243-0243  
Telephone: (615) 741-2734

**TEXAS**

Richard Anderson, Director  
Crime Victims Compensation Division  
Office of the Attorney General  
P.O. Box 12548, Capitol Station  
Austin, TX 78711-2548  
Telephone: (512) 936-1200

**VICTIM ASSISTANCE PROGRAMS**

**RHODE ISLAND**

Joseph L. Persia, Grant Administrator  
Governor's Justice Commission  
One Capitol Hill  
4th Floor  
Providence, RI 02903-5803  
Telephone: (401) 277-2620

**SOUTH CAROLINA**

Barbara Jean Nelson, VOCA Program Coord.  
Division of Public Safety Programs  
5400 Broad River Road  
Columbia, South Carolina 29210  
Telephone: (803) 896-8712

**SOUTH DAKOTA**

Susan Sheppick, Administrator  
Department of Social Services  
Office of the Adult Services  
700 Governors Drive  
Pierre, SD 57501-2291  
Telephone: (605) 773-4330

**TENNESSEE**

Cresa L. Bailey, VOCA Specialist  
Department of Human Services  
400 Deaderick Street  
Citizens Plaza Building  
Nashville, TN 37248-9500  
Telephone: (615) 313-4767

**TEXAS**

Carol Funderburgh, Program Coordinator  
Criminal Justice Division  
Office of the Governor  
P.O. Box 12428  
Austin, TX 78701  
Telephone: (512) 463-1919

## **VICTIM COMPENSATION PROGRAMS**

### **UTAH**

Dan R. Davis, Director  
Office of Crime Victim Reparations  
350 E. 500 South, Suite 200  
Salt Lake City, UT 84111  
Telephone: (801) 533-4000

### **VERMONT**

Lori E. Hayes, Executive Director  
Vermont Center for Crime Victim Services  
Crime Victims Compensation Program  
103 South Main Street  
Waterbury, VT 05671-2001  
Telephone: (802) 241-1250

### **VIRGINIA**

Robert W. Armstrong, Director  
Division of Crime Victims' Compensation  
1000 DMV Drive  
Richmond, VA 23220-2036  
Telephone: (804) 367-8686

### **VIRGIN ISLANDS**

Ruth D. Smith, Administrator  
Criminal Victims Compensation Commission  
Department of Human Services  
Office of the Commissioner  
The Knud Hansen, Complex Building A  
1303 Hospital Grounds  
Charlotte Amalie, Virgin Islands 00802  
Telephone: (809) 774-1166

### **WASHINGTON**

Cletus Nnanabu, Program Manager  
Department of Labor & Industries  
Crime Victims Compensation Program  
7373 Linderson Way, SW - POB 44520  
Olympia, WA 98504-4520  
Telephone: (360) 902-5340

## **VICTIM ASSISTANCE PROGRAMS**

### **UTAH**

Christine Watters, Program Coordinator  
Office of Crime Victim Reparations  
350 E. 500 South, Suite 200  
Salt Lake City, UT 84111  
Telephone: (801) 533-4000

### **VERMONT**

Lori E. Hayes, Executive Director  
Vermont Center for Crime Services  
103 South Main Street  
Waterbury, Vermont 05671-2001  
Telephone: (802) 241-1250

### **VIRGINIA**

Mandie Patterson, Program Manager  
Department of Criminal Justice Services  
805 East Broad Street, 10th Floor  
Richmond, VA 23219  
Telephone: (804) 786-3923

### **VIRGIN ISLANDS**

Maria Brady, Director  
Law Enforcement Planning Commission  
8172 Sub Base, Suite 3  
St. Thomas, VI 00802  
Telephone: (809) 774-6400

### **WASHINGTON**

Susan Hannibal, Program Manager  
Department of Social and  
Health Services  
P.O. Box 45710, 12th & Jefferson  
Olympia, WA 98504-5710  
Telephone: (206) 753-3395

**VICTIM COMPENSATION PROGRAMS**

**WEST VIRGINIA**

Cheryle M. Hall, Clerk  
West Virginia Court of Claims  
Crime Victims Compensation Fund  
Room 6, Building 1, 1900 Kanawha Blvd. E.  
Charleston, WV 25305-0291  
Telephone: (304) 347-4850

**WISCONSIN**

Susan Goodwin, Executive Director  
Office of Crime Victims Services  
Department of Justice  
P.O. Box 7951 - 222 State Street  
Madison, WI 53707-7951  
Telephone: (608) 266-6470

**WYOMING**

Sylvia Bagdonas, Program Manager  
Crime Victims Compensation Commission  
Office of the Attorney General  
1700 Westland Road  
Cheyenne, WY 82002  
Telephone: (307) 635-4050

**VICTIM ASSISTANCE PROGRAMS**

**WEST VIRGINIA**

Melissa B. Crawford, Program Manager  
Criminal Justice & Highway Safety Div.  
Dept. of Military Affairs & Public Safety  
1204 Kanawha Boulevard, East  
Charleston, WV 25301  
Telephone: (304) 558-8814

**WISCONSIN**

Steve Derene, Program Manager  
Office of Crime Victims Services  
Department of Justice  
P.O. Box 7951 - 222 State Street  
Madison, WI 53707-7951  
Telephone: (608) 267-2251

**WYOMING**

Sylvia Bagdonas, Program Manager  
Office of Crime Compensation Commission  
Office of the Attorney General  
1700 Westland Road  
Cheyenne, WY 82002  
Telephone: (307) 635-4050

## VICTIM ASSISTANCE TERRITORY PROGRAMS

### VICTIM COMPENSATION PROGRAMS

#### **AMERICAN SAMOA**

No compensation program

#### **GUAM**

No compensation program

#### **NORTHERN MARIANA ISLANDS**

No compensation program

#### **PUERTO RICO**

No compensation program

#### **PALAU**

No compensation program

### VICTIM ASSISTANCE PROGRAMS

#### **AMERICAN SAMOA**

Laauli A. Filoialii, Director  
Criminal Justice Planning Agency  
American Samoa Government  
Pago Pago, AS 96799  
Telephone: (011) (684) 633-5221

#### **GUAM**

Gloria J. Duenas Cruz  
Department of Law  
Government of Guam  
2-200E Guam Judicial Center  
120 West O'Brien Drive  
Agana, GU 96910  
Telephone: (011) (671) 475-3406

#### **NORTHERN MARIANA ISLANDS**

Joaquin T. Ogumoro, Executive Director  
Criminal Justice Planning Agency  
P.O. Box 1133 CK, Saipan MP  
Saipan, CM 96950  
Telephone: (011) (670) 322-9350

#### **PUERTO RICO**

Lizzette Traversoi, Acting Director  
Department of Justice  
P.O. Box 192  
San Juan, PR 00902  
Telephone: (809) 723-4949

#### **PALAU**

Yusim Sato, VOCA Program Coordinator  
Ministry of Health  
P.O. Box 6027  
Koror, Palau 96940  
Telephone: (680) 488-2813/2553

\*\*\*Nevada's victim compensation program does not received VOCA funds.

## Appendix 8

### Interpol State Liaison Offices

A point of contact has been established in each of the 50 States and the District of Columbia for local and State authorities to receive assistance from INTERPOL on international investigations to include child abductions/ kidnappings. This point of contact is known as the INTERPOL State Liaison Office. Local and State law enforcement can forward requests for assistance through the liaison office, which will then forward the request to the USNCB for transmission to appropriate foreign police authorities. The following is a listing of INTERPOL State Liaison Offices through which local/State police authorities can obtain assistance on child abduction investigations:

Alabama/INTERPOL Liaison Office  
Alabama Bureau of Investigation  
Criminal Information Center  
Alabama Department of Public Safety  
2720-A West Gunter Park Drive  
Montgomery, AL 36109  
Telephone: (334) 260-1170  
FAX: (334) 260-8788

California/INTERPOL Liaison Office  
California Department of Justice  
Bureau of Investigation  
Organized Crime Unit  
P. O. Box 163029  
Sacramento, CA 95816-3029  
Telephone: (916) 227-4186  
FAX: (916) 227-4097

Alaska/INTERPOL Liaison Office  
Alaska State Troopers  
101 East 6th Avenue  
Anchorage, AK 99501  
Telephone: (907) 265-9583  
FAX: (907) 274-0851

Colorado/INTERPOL Liaison Office  
Colorado Bureau of Investigation  
Crime Information Center  
690 Kipling Street, Suite 3000  
Denver, CO 80215-5865  
Telephone: (303) 239-4310  
FAX: (303) 238-6714

Arizona/INTERPOL Liaison Office  
Arizona Department of Public Safety  
P.O. Box 6638  
Phoenix, AZ 85005-6638  
Telephone: (602) 223-2608  
FAX: (602) 223-2911

Connecticut/INTERPOL Liaison Office  
Central Criminal Intelligence Unit  
294 Colony Street  
Meriden, CT 06451  
Telephone: (203) 238-6561  
FAX: (203) 238-6410

Arkansas/INTERPOL Liaison Office  
Arkansas State Police  
Crime Analysis Section  
3 Natural Resources Drive  
P. O. Box 5901  
Little Rock, AR 72215  
Telephone: (501) 221-8213  
FAX : (501) 224-5006

Delaware/INTERPOL Liaison Office  
Delaware State Police  
P.O. Box 430  
Dover, DE 19901  
Telephone: (302) 739-5998  
FAX: (302) 739-2459

District of Columbia/INTERPOL Liaison Office  
Washington Metropolitan Police Department  
Intelligence Division - Room 5067  
300 Indiana Ave., NW  
Washington, D.C. 20001  
Telephone: (202) 724-1426  
FAX: (202) 727-0588

Florida/INTERPOL Liaison Office  
Florida Department of Law Enforcement  
DCI/ISB  
P.O. Box 1489  
Tallahassee, FL 32302  
Telephone: (904) 488-6933  
FAX: (904) 488-7863

Georgia/INTERPOL Liaison Office  
Georgia Bureau of Investigation  
P.O. Box 370808  
Decatur, GA 30037-0808  
Telephone: (404) 244-2554  
FAX: (404) 244-2798

Honolulu/INTERPOL Liaison Office  
Department of the Attorney General  
425 Queen St.  
Honolulu, HI 96813  
Telephone: (808) 586-1249  
FAX: (808) 586-1371

Idaho/INTERPOL Liaison Office  
Idaho State Police  
Idaho Bureau of Investigation  
P.O. Box #700  
Meridian, ID 83680-0700  
Telephone: (208) 884-7110  
FAX: (208) 884-7191

Illinois/INTERPOL Liaison Office  
Illinois State Police  
Division of Criminal Investigation  
500 Iles Park Place Room 400  
Springfield, IL 62718  
Telephone: (217) 782-8760  
FAX: (217) 785-3328

Indiana/INTERPOL Liaison Office  
Indiana State Police  
Crime Information Center  
100 Senate Avenue  
Indianapolis, IN 46206-2404  
Telephone: (317) 232-7796  
FAX: (317) 232-0652

Iowa/INTERPOL Liaison Office  
Iowa Department of Public Safety  
Intelligence Bureau  
Wallace State Office Building  
Des Moines, IA 50319-0049  
Telephone: (515) 242-6124  
FAX: (515) 281-6108

Kansas/INTERPOL Liaison Office  
Kansas Bureau of Investigation  
1620 Tyler  
Topeka, KS 66612  
Telephone: (913) 296-8261  
FAX: (913) 296-6781

Kentucky/INTERPOL Liaison Office  
Kentucky State Police Intelligence Section  
1240 Airport Road  
Frankfort, KY 40601  
Telephone: (502) 227-8708  
FAX: (502) 564-4931

Louisiana/INTERPOL Liaison Office  
Louisiana State Police  
P.O. Box 66614  
Baton Rouge, LA 70896  
Telephone: (504) 925-6213  
FAX: (504) 925-4766

Maine/INTERPOL Liaison Office  
Maine State Police  
Gardiner Annex  
State House Station 164  
Augusta, ME 04333-0164  
Telephone: (207) 624-8787  
FAX: (207) 624-8765



Maryland/INTERPOL Liaison Office  
Maryland State Police  
Criminal Intelligence Division  
7175 Columbia Gateway Drive, Suite D  
Columbia, MD 21045  
Telephone: (410) 290-0780  
FAX: (410) 290-0752

Massachusetts/INTERPOL Liaison Office  
Massachusetts State Police  
Criminal Information Section  
470 Worcester Road  
Framingham, MA. 01702  
Telephone: (508) 820-2129  
FAX: (508) 820-2128

Michigan/INTERPOL Liaison Office  
Michigan State Police  
Criminal Intelligence Unit  
4000 Collins Road  
PO Box 30637  
Lansing, MI 48909-8137  
Telephone: (517) 336-6235  
FAX: (517) 333-5399

Minnesota/INTERPOL Liaison Office  
Minnesota State Bureau of Criminal Apprehension  
1246 University Avenue  
St. Paul, MN 55104-4197  
Telephone: (612) 642-0610  
FAX: (612) 642-0618

Mississippi/INTERPOL Liaison Office  
Mississippi Department of Public Safety  
Division of Criminal Investigation  
P.O. Box 958  
Jackson, MS. 39205  
Telephone: (601) 987-1592  
FAX: (601) 987-1579

Missouri/INTERPOL Liaison Office  
Missouri State Highway Patrol  
P.O. Box 568  
Jefferson City, MO 65102  
Telephone: (573) 751-3452  
FAX: (573) 526-5577

Montana/INTERPOL Liaison Office  
Montana Department of Justice  
Law Enforcement Services Division  
P.O. Box 201417  
Helena, MT 59620-1417  
Telephone: (406) 444-3874  
FAX: (406) 444-2759

Nebraska/INTERPOL Liaison Office  
Nebraska State Patrol  
State House  
P. O. Box 94907  
Lincoln, NE 68509  
Telephone: (402) 479-4957  
FAX: (402) 479-4002

Nevada/INTERPOL Liaison Office  
Nevada Division of Investigation  
555 Wright Way  
Carson City, NV 89711-0100  
Telephone: (702) 687-3346  
FAX: (702) 687-1668

New Hampshire/INTERPOL Liaison Office  
New Hampshire State Police  
Intelligence Unit  
10 Hazen Drive  
Concord, NH 03305  
Telephone: (603) 271-2663  
FAX: (603) 271-2520

New Jersey/INTERPOL Liaison Office  
New Jersey State Police  
Intelligence Bureau  
P. O. Box 7068  
West Trenton, NJ 08628-0068  
Telephone: (609) 882-2000 x 2642  
FAX: (609) 883-5576

New Mexico/INTERPOL Liaison Office  
New Mexico Department of Public Safety  
Criminal Intelligence Section  
400 Gold Ave. SW - Suite 300  
Albuquerque, NM 87102  
Telephone: (505) 841-8053  
FAX: (505) 841-8062

New York/INTERPOL Liaison Office  
New York State Police  
1220 Washington Avenue - BLDG #30  
Albany, NY 12226-3000  
Telephone: (518) 485-1518  
FAX: (518) 485-2000

Inter-City Correspondence Unit  
Police Headquarters  
1 Police Plaza, Room 703  
New York, NY 10038-1497  
Telephone: (212) 374-5030  
FAX: (212) 374-2485

North Carolina/INTERPOL Liaison Office  
North Carolina State Bureau of Investigation  
Intelligence and Technical Services Section  
P. O. Box 29500  
Raleigh, NC 27626  
Telephone: 1-800-334-3000  
FAX: (919) 662-4483

North Dakota/INTERPOL State Liaison Office  
Bureau of Criminal Investigation  
P. O. Box 1054  
Bismark, ND 58502-1054  
Telephone: (701) 221-5500  
FAX: (701) 328-5510

Ohio/INTERPOL Liaison Office  
Criminal Intelligence Unit  
Ohio BCI&I  
P.O. Box 365  
London, OH 43140  
Telephone: (800) 282-3784, Ext. 223  
FAX: (614) 852-1603

Oklahoma/INTERPOL Liaison Office  
Oklahoma State Bureau of Investigation  
6600 N. Harvey, Suite 300  
Oklahoma City, OK 73116  
Telephone: (405) 848-6724  
FAX: (405) 843-3804

Oregon State Police  
Criminal Investigation Division  
400 Public Service Building  
Salem, Oregon 97310  
Telephone: (503) 378-3720  
FAX: (503) 363-5475

Pennsylvania/INTERPOL Liaison Office  
PA Attorney General Intelligence Unit  
State Police Headquarters  
1800 Elmerton Avenue  
Harrisburg, PA 17110  
Telephone: (717) 787-0834  
FAX: (717) 787-0846

Rhode Island/INTERPOL Liaison Office  
Rhode Island State Police Headquarters  
P.O. Box 185  
N. Scituate, RI 02857  
Telephone: (401) 444-1006  
FAX: (401) 444-1133

South Carolina/INTERPOL Liaison Office  
South Carolina Law Enforcement Division  
P. O. Box 21398  
Columbia, SC 29221-1398  
Telephone: (803) 896-7008  
FAX: (803) 896-7041

South Dakota/INTERPOL Liaison Office  
Division of Criminal Investigation  
Criminal Justice Training Center  
E.Hwy. 34 c/o 500 E. Capitol Avenue  
Pierre, SD 57501-5070  
Telephone: (605) 773-3331  
FAX: (605) 773-4629

Tennessee/INTERPOL Liaison Office  
Tennessee Bureau of Investigation  
Cooper Hall 1148 Foster Avenue  
Nashville, TN 37210  
Telephone: (615) 741-0430  
FAX: (615) 532-8315

Texas/INTERPOL Liaison Office  
Texas Department of Public Safety  
Special Crimes Service  
P. O. Box 4087 N.A.S.  
Austin, TX 78773-0001  
Telephone: (512) 424-2200  
FAX: (512) 424-5715

Utah/INTERPOL Liaison Office  
Utah DPS/Division of Investigations  
5272 South College Drive - Suite 200  
Murray, UT 84123-2611  
Telephone: (801) 284-6200  
FAX: (801) 284-6300

Vermont/INTERPOL Liaison Office  
Vermont State Police  
Criminal Division  
103 South Main Street  
Waterbury, VT 05671  
Telephone: (802) 244-8781  
FAX: (802) 244-1106

Virginia/INTERPOL Liaison Office  
Virginia Department of State Police  
808 Moorefield Drive Suite 300  
Richmond, VA 23236-3683  
Telephone: (804) 323-2493  
FAX: (804) 323-2021

Washington/INTERPOL Liaison Office  
Washington State Patrol  
Investigative Assistance Division  
P. O. Box 2347, Mail Stop 42634  
Olympia, WA 98507-2347  
Telephone: (206) 753-3277  
FAX: (360) 586-8231

West Virginia/INTERPOL Liaison Office  
West Virginia State Police  
725 Jefferson Road  
South Charleston, WV 25309  
Telephone: (304) 558-3324  
FAX: (304) 746-2246

Wisconsin/INTERPOL Liaison Office  
Wisconsin Department of Justice  
Division of Criminal Investigation  
P. O. Box 7857  
Madison, WI 53707-7857  
Telephone: (608) 266-1671  
FAX: (608) 267-2777

Wyoming/INTERPOL Liaison Office  
Wyoming Division of Criminal Investigation  
316 West 22nd Street  
Cheyenne, WY 82002-0150  
Telephone: (307) 777-6615  
FAX: (307) 777-7252

INTERPOL/U.S. American Samoa  
P.O. Box 4567  
Pago Pago, American Samoa 96799  
Telephone: (684) 633-2827  
FAX: (684) 633-2979

INTERPOL-Special Invest. Bureau  
Puerto Rico Dept. of Justice  
P.O. Box 9023899  
San Juan, Puerto Rico 00902-3899  
Telephone: (787) 729-2068  
FAX: (787) 722-0809

INTERPOL Liaison Office  
Virgin Islands Police Department  
Insular Investigation Unit  
Patrick Sweeney Headquarters  
RR 02 Kings Hill  
St. Croix, U.S. Virgin Islands 00850  
Telephone: (809) 778-6601  
FAX: (809) 773-7272



## Appendix 9

### U.S. Department of State Bureau of Consular Affairs

#### Office of Children's Issues Abduction and Custody Information Checklist

Name: \_\_\_\_\_

Address: \_\_\_\_\_

(Please place a check beside your choice)

#### GENERAL INFORMATION:

- Office of Children's Issues Brochure
- International Parental Child Abduction Booklet\*, +
- International Parental Kidnaping Crime Act of 1993
- Tips for Travelers to the Middle East and North Africa\*  
(Provides country specific information)

#### HAGUE CONVENTION ON INTERNATIONAL PARENTAL CHILD ABDUCTION:

- Hague Parties (List of Hague Countries)
- Hague Convention - French/English Text
- Hague: Scope of the Convention

#### COUNTRY SPECIFIC INFORMATION

- |                                                 |                                                            |
|-------------------------------------------------|------------------------------------------------------------|
| <input type="checkbox"/> Australia              | <input type="checkbox"/> Pakistan                          |
| <input type="checkbox"/> Canada                 | <input type="checkbox"/> Pakistan - Child Custody Law      |
| <input type="checkbox"/> Canada - Legal Aid Act | <input type="checkbox"/> Pakistan - Sunni Muslim Law       |
| <input type="checkbox"/> Denmark                | <input type="checkbox"/> Philippines*                      |
| <input type="checkbox"/> Germany*               | <input type="checkbox"/> Poland                            |
| <input type="checkbox"/> Greece                 | <input type="checkbox"/> Portugal                          |
| <input type="checkbox"/> India                  | <input type="checkbox"/> Saudi Arabia*                     |
| <input type="checkbox"/> Iran*                  | <input type="checkbox"/> Saudi Arabia = Marriage to Saudis |
| <input type="checkbox"/> Islamic Family Law     | <input type="checkbox"/> Spain                             |
| <input type="checkbox"/> Japan                  | <input type="checkbox"/> Sweden                            |
| <input type="checkbox"/> Jordan*                | <input type="checkbox"/> Syria                             |
| <input type="checkbox"/> Kuwait                 | <input type="checkbox"/> Thailand                          |
| <input type="checkbox"/> Mexico                 | <input type="checkbox"/> United Kingdom                    |
| <input type="checkbox"/> Mexico - Child Custody |                                                            |

\* - Available by Autofax

+ - Available by Internet

**Office of Children's Issues  
Adoption Information Checklist**

Name: \_\_\_\_\_

Address: \_\_\_\_\_

(Please place a check beside your choice)

**GENERAL INFORMATION FLYERS:**

\_\_\_\_ International Adoptions\*

\_\_\_\_ The Immigration of Adopted and Prospective Adoptive Children (M-249Y)

**COUNTRY SPECIFIC INFORMATION:**

\_\_\_\_ Albania  
\_\_\_\_ Antingua  
\_\_\_\_ Argentina  
\_\_\_\_ Austria  
\_\_\_\_ Bahamas  
\_\_\_\_ Barbados  
\_\_\_\_ Belarus  
\_\_\_\_ Belize  
\_\_\_\_ Bolivia  
\_\_\_\_ Brazil  
\_\_\_\_ Bulgaria  
\_\_\_\_ Chile  
\_\_\_\_ China  
\_\_\_\_ Columbia  
\_\_\_\_ Costa Rica  
\_\_\_\_ Czech Republic  
\_\_\_\_ Dominica  
\_\_\_\_ Dominican Republic  
\_\_\_\_ Ecuador  
\_\_\_\_ El Salvador  
\_\_\_\_ Georgia  
\_\_\_\_ Germany  
\_\_\_\_ Greece  
\_\_\_\_ Grenada

\_\_\_\_ Guatemala  
\_\_\_\_ Guyana  
\_\_\_\_ Haiti  
\_\_\_\_ Honduras  
\_\_\_\_ Hong Kong  
\_\_\_\_ Hungary  
\_\_\_\_ India  
\_\_\_\_ Iran  
\_\_\_\_ Ireland  
\_\_\_\_ Israel  
\_\_\_\_ Jamaica  
\_\_\_\_ Japan  
\_\_\_\_ Jordan  
\_\_\_\_ Korea  
\_\_\_\_ Latvia  
\_\_\_\_ Lebanon  
\_\_\_\_ Lithuania  
\_\_\_\_ Marshall Islands  
\_\_\_\_ Mexico  
\_\_\_\_ Moldova  
\_\_\_\_ Morocco  
\_\_\_\_ Nepal  
\_\_\_\_ Nicaragua  
\_\_\_\_ Pakistan

\_\_\_\_ Panama  
\_\_\_\_ Paraguay  
\_\_\_\_ Peru  
\_\_\_\_ Philippines  
\_\_\_\_ Poland  
\_\_\_\_ Portugal  
\_\_\_\_ Romania  
\_\_\_\_ Russia  
\_\_\_\_ Slovakia  
\_\_\_\_ Sri Lanka  
\_\_\_\_ St. Lucia  
\_\_\_\_ St. Kitts  
\_\_\_\_ St. Vincent  
\_\_\_\_ Syria  
\_\_\_\_ Taiwan  
\_\_\_\_ Thailand  
\_\_\_\_ Trinidad  
\_\_\_\_ Ukraine  
\_\_\_\_ Uruguay  
\_\_\_\_ Uzbekistan  
\_\_\_\_ Vietnam  
\_\_\_\_ Former Yugoslavia  
\_\_\_\_ Venezuela

Office of Children's Issues  
Overseas Citizens Services  
Bureau of Consular Affairs  
U.S. Department of State  
Washington, D.C. 20520

Telephone: (202) 647-2699  
Fax: (202) 647-2835  
Autofax (202) 647-3000  
Recorded Info:  
(202) 647-7000  
Internet Address:  
<http://travel.state.gov>

## Appendix 10

### U.S. Customs Service Field Offices

#### Alabama

|             |                |
|-------------|----------------|
| Birmingham  | (205) 290-7193 |
| Gulf Shores | (205) 981-5711 |
| Mobile      | (205) 441-6146 |

#### Alaska

|           |                |
|-----------|----------------|
| Anchorage | (907) 271-2880 |
|-----------|----------------|

#### Arizona

|           |                |
|-----------|----------------|
| Douglas   | (602) 364-1218 |
| Flagstaff | (602) 556-7384 |
| Nogales   | (602) 761-2075 |
| Phoenix   | (602) 640-2036 |
| Sells     | (602) 387-7640 |
| Tucson    | (602) 670-6026 |
| Yuma      | (602) 344-0088 |

#### Arkansas

|             |                |
|-------------|----------------|
| Little Rock | (501) 324-7345 |
|-------------|----------------|

#### California

|                     |                |
|---------------------|----------------|
| El Centro           | (619) 353-9090 |
| Fresno              | (209) 487-5351 |
| Los Angeles         | (310) 514-6231 |
| Los Angeles Airport | (310) 215-2200 |
| Oceanside           | (619) 722-6616 |
| Orange County       | (714) 836-2293 |
| Oxnard              | (805) 988-8690 |
| Riverside           | (909) 276-6664 |
| Sacramento          | (916) 978-4411 |
| San Diego           | (619) 557-6850 |
| San Francisco       | (415) 705-4070 |
| San Jose            | (408) 291-7861 |
| San Ysidro          | (619) 428-7115 |

#### Colorado

|        |                |
|--------|----------------|
| Denver | (303) 784-6480 |
|--------|----------------|

**Connecticut**  
New Haven (203) 773-2155

**District of Columbia**  
Washington, D.C. (703) 709-9700

**Florida**  
Cocoa Beach (407) 452-3700  
Fort Lauderdale (305) 590-7384  
Fort Myers (813) 433-7773  
Fort Pierce (407) 461-1293  
Jacksonville (904) 356-4701  
Key Largo (305) 664-2955  
Key West (305) 294-3877  
Miami (305) 597-6000  
Naples (813) 643-4554  
Orlando (407) 648-6847  
Panama City (904) 763-8418  
Pensacola (904) 434-6648  
Sarasota (813) 953-2920  
Tallahassee (904) 942-8802  
Tampa (813) 225-7638  
West Palm Beach (407) 659-4606

**Georgia**  
Atlanta (770) 994-2230  
Savannah (912) 652-4341

**Illinois**  
Chicago (312) 353-8450

**Indiana**  
Indianapolis (317) 248-4151

**Louisiana**  
Baton Rouge (504) 389-0433  
Belle Chase (504) 589-2291  
Houma (504) 851-0179  
Lafayette (318) 262-6619  
Lake Charles (318) 477-2112  
New Orleans (504) 589-6499  
Shreveport (318) 676-3350

**Maine**  
Houlton (207) 532-6198  
Portland (207) 773-8959



|                                                                                                                 |                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Maryland</b><br>Baltimore                                                                                    | (410) 962-2620                                                                                           |
| <b>Massachusetts</b><br>Boston                                                                                  | (617) 565-7400                                                                                           |
| <b>Michigan</b><br>Detroit<br>Grand Rapids                                                                      | (313) 226-3166<br>(616) 235-3936                                                                         |
| <b>Minnesota</b><br>Minneapolis                                                                                 | (612) 348-1300                                                                                           |
| <b>Mississippi</b><br>Gulfport<br>Jackson                                                                       | (601) 864-1274<br>(601) 965-5234                                                                         |
| <b>Missouri</b><br>Kansas City<br>St. Louis                                                                     | (816) 374-6426<br>(314) 539-6740                                                                         |
| <b>Montana</b><br>Great Falls                                                                                   | (406) 727-8750                                                                                           |
| <b>Nevada</b><br>Las Vegas<br>Reno                                                                              | (702) 388-6042<br>(702) 784-5727                                                                         |
| <b>New Jersey</b><br>Newark                                                                                     | (201) 645-3770                                                                                           |
| <b>New Mexico</b><br>Albuquerque<br>Deming<br>Las Cruces                                                        | (505) 766-2807<br>(505) 546-2759<br>(505) 526-4643                                                       |
| <b>New York</b><br>Albany<br>Buffalo<br>John F. Kennedy Airport<br>Long Island<br>New York City<br>Rouses Point | (518) 472-2211<br>(716) 551-4375<br>(718) 553-1824<br>(516) 563-3040<br>(212) 466-2906<br>(518) 297-6661 |
| <b>North Carolina</b><br>Charlotte<br>Wilmington                                                                | (704) 527-0151<br>(910) 343-4899                                                                         |

|                       |                |
|-----------------------|----------------|
| <b>North Dakota</b>   |                |
| Grand Forks           | (701) 746-1157 |
| <b>Ohio</b>           |                |
| Cincinnati            | (606) 578-4600 |
| Cleveland             | (216) 522-4292 |
| Columbus              | (614) 469-5705 |
| <b>Oklahoma</b>       |                |
| Oklahoma City         | (405) 231-4279 |
| <b>Oregon</b>         |                |
| Astoria               | (503) 325-4644 |
| Coos Bay              | (503) 269-7521 |
| Portland              | (503) 326-2711 |
| <b>Pennsylvania</b>   |                |
| Harrisburg            | (717) 782-4047 |
| Philadelphia          | (215) 597-4305 |
| Pittsburgh            | (412) 644-4970 |
| <b>Rhode Island</b>   |                |
| Providence            | (401) 528-5025 |
| <b>South Carolina</b> |                |
| Charleston            | (803) 745-9290 |
| Columbia              | (803) 765-5430 |
| Greenville            | (803) 235-0519 |
| <b>Tennessee</b>      |                |
| Memphis               | (901) 544-4140 |
| Nashville             | (615) 781-5473 |
| <b>Texas</b>          |                |
| Alpine                | (915) 837-5889 |
| Austin                | (512) 482-5502 |
| Brownsville           | (210) 542-7831 |
| Corpus Christi        | (512) 888-3501 |
| Dallas                | (214) 767-2011 |
| Del Rio               | (210) 703-2000 |
| Eagle Pass            | (210) 773-7877 |
| El Paso               | (915) 540-5700 |
| Falcon Dam            | (210) 848-5243 |
| Galveston             | (409) 766-3791 |
| Houston               | (713) 985-0500 |
| Laredo                | (210) 726-2210 |
| McAllen               | (210) 682-1366 |

**Texas - continued**

Port Arthur (409) 839-2401  
Presidio (915) 229-3960  
San Angelo (915) 942-6900  
San Antonio (210) 229-4561

**Utah**

Salt Lake City (801) 524-5884

**Vermont**

Burlington (802) 863-3458  
Derby Line (802) 873-3609

**Virginia**

Norfolk (804) 441-6533

**Washington**

Blaine (206) 332-6725  
Port Angeles (206) 452-4122  
Seattle (206) 553-7531  
Spokane (509) 353-3130

**Wisconsin**

Milwaukee (414) 297-3231

**Bahamas**

Nassau (809) 325-5322

**Guam**

Guam (700) 550-7265

**Puerto Rico**

Fajardo (809) 865-5303  
Mayaguez (809) 831-3346  
Ponce (809) 841-3108  
San Juan (809) 729-6975

**Virgin Islands**

St. Thomas (809) 774-7409



# Appendix 11

## U.S. Postal Inspection Service Division Boundaries



For assistance with postal-related problems of a law enforcement nature, please contact your nearest Inspection Service Division.

**Atlanta Division**  
P.O. Box 16489  
Atlanta, GA 30321-0489  
404/608-4500  
Fax: 404/608-4505

**Boston Division**  
425 Summer Street, 7th Floor  
Boston, MA 02210-1736  
617/464-8000  
Fax: 617/464-8123

**Buffalo Division**  
1200 Main Place Tower  
Buffalo, NY 14202-3796  
716/853-5300  
Fax: 716/846-2372

**Charlotte Division**  
2901 South I-85 Service Road  
Charlotte, NC 28228-3000  
704/329-9120  
Fax: 704/357-0039

**Chicago Division**  
433 W. Harrison Street, Room 50190  
Chicago, IL 60669-2201  
312/983-7900  
Fax: 312/983-6300

**Cincinnati Division**  
895 Central Avenue, Suite 200  
Cincinnati, OH 45202-5748  
513/684-8000  
Fax: 513/684-8009

**Cleveland Division**  
P.O. Box 5726  
Cleveland, OH 44101-0726  
216/443-4000  
Fax: 216/443-4509

**Denver Division**  
1745 Stout Street, Suite 900  
Denver, CO 80202-3034  
303/313-5320  
Fax: 303/313-5351

**Detroit Division**  
P.O. Box 330119  
Detroit, MI 48232-6119  
313/226-8184  
Fax: 313/226-8220

**Ft. Worth Division**  
P.O. Box 162929  
Ft. Worth, TX 76161-2929  
817/317-3400  
Fax: 817/317-3430

**Houston Division**  
P.O. Box 1276  
Houston, TX 77251-1276  
713/238-4400  
Fax: 713/238-4460

**Kansas City Division**  
3101 Broadway, Suite 850  
Kansas City, MO 64111-2416  
816/932-0400  
Fax: 816/932-0490

**Los Angeles Division**  
P.O. Box 2000  
Pasadena, CA 91102-2000  
818/405-1200  
Fax: 818/405-1207

**Memphis Division**  
P.O. Box 3180  
Memphis, TN 38173-0180  
901/576-2077  
Fax: 901/576-2085

**Miami Division**  
3400 Lakeside Drive, 6th Floor  
Miramar, FL 33027-3242  
954/436-7200  
Fax: 954/436-7282

**Newark Division**  
P.O. Box 509  
Newark, NJ 07101-0509  
201/693-5400  
Fax: 201/645-0600

**New York Division**  
P.O. Box 555  
New York, NY 10116-0555  
212/330-3844  
Fax: 212/330-2720

**Philadelphia Division**  
P.O. Box 7500  
Philadelphia, PA 19101-9000  
215/895-8450  
Fax: 215/895-8470

**Phoenix Division**  
P.O. Box 20666  
Phoenix, AZ 85036-0666  
602/223-3660  
Fax: 602/258-1705

**Pittsburgh Division**  
1001 California Avenue, Room 2101  
Pittsburgh, PA 15290-9000  
412/359-7900  
Fax: 412/359-7682

**Richmond Division**  
P.O. Box 25009  
Richmond, VA 23260-5009  
804/418-6100  
Fax: 804/418-6150

**St. Louis Division**  
1106 Walnut Street  
St. Louis, MO 63199-2201  
314/539-9300  
Fax: 314/539-9306

**St. Paul Division**  
P.O. Box 64558  
St. Paul, MN 55164-0558  
612/293-3200  
Fax: 612/293-3384

**San Francisco Division**  
P.O. Box 882528  
San Francisco, CA 94188-2528  
415/778-5800  
Fax: 415/778-5822

**San Juan Division**  
P.O. Box 363667  
San Juan, PR 00936-3667  
787/749-7600  
Fax: 787/782-8296

**Seattle Division**  
P.O. Box 400  
Seattle, WA 98111-4000  
206/442-6300  
Fax: 206/442-6304

**Tampa Division**  
P.O. Box 22526  
Tampa, FL 33622-2526  
813/281-5200  
Fax: 813/289-8003

**Washington Division**  
P.O. Box 96096  
Washington, DC 20066-6096  
202/636-2300  
Fax: 202/636-2287

**Headquarters**  
U.S. Postal Inspection Service  
475 L'Enfant Plaza SW  
Washington, DC 20260-2100  
Fax: 202/268-4563



**U.S. Department of Defense –  
Legal Assistance Offices**

**Army Legal Assistance Office**

DAJA-LA  
Office of the Judge  
Advocate General  
Room 2C463  
Pentagon  
Washington, DC 20310-2200  
Telephone: (703) 697-3170

**Navy Legal Assistance Office**

Legal Assistance (Code 36)  
Office of the Judge  
Advocate General  
Department of the Navy  
9S25 Hoffman II Building  
200 Stovall Street  
Alexandria, VA 22332-2400  
Telephone: (703) 325-7928

**U.S. Department of Health  
and Human Services –  
Family and Youth Services Bureau**

**Family and Youth  
Services Bureau**

U.S. Department of Health  
and Human Services  
P.O. Box 1882  
Washington, DC 20013  
Telephone: (202) 205-8102  
Fax: (202) 260-9333

**National Clearinghouse  
on Families and Youth**

P.O. Box 13505  
Silver Spring, MD 20911-3505  
Telephone: (301) 608-8098  
Fax: (301) 608-8721

**National Runaway  
Switchboard Hotline**

Telephone: 1-800-621-4000

**U.S. Department of Justice –  
Child Exploitation and  
Obscenity Section**

**Child Exploitation and  
Obscenity Section**

Criminal Division  
U.S. Department of Justice  
1331 F Street NW.  
6th Floor  
Washington, DC 20530  
Telephone: (202) 514-5780  
Fax: (202) 514-1793

**U.S. Department of Justice –  
Office for Victims of Crime**

**Office for Victims of Crime**

U.S. Department of Justice  
810 7th Street NW.  
Washington, DC 20531  
Telephone: (202) 307-5983  
Fax: (202) 514-6383

Gopher to: ncjrs.aspensys.com  
World Wide Web:  
<http://www.ojp.usdoj.gov/OVC/>

**Air Force Legal  
Assistance Office**  
AFLSA/JACA  
1420 Air Force Pentagon  
Washington, DC 20330-1420  
Telephone: (202) 697-0413

**Marine Corps Legal  
Assistance Office**  
Legal Assistance Office  
Judge Advocate Division  
Headquarters, USMC  
301 Henderson Hall  
Southgate Road and Orme St.  
Arlington, VA 22214  
Telephone: (703) 614-1266



**U.S. Department of Defense –  
Family Advocacy Program**

**Army Family Advocacy Program**

Army Family Advocacy Program Manager  
HQDA, CFSC-FSA, Department of the Army  
Hoffman #1, Room 1407  
Alexandria, VA 22331-0521  
Telephone: (703) 325-9390  
Fax: (703) 325-5924

**Air Force Family Advocacy Program**

Chief, Family Advocacy Division  
HQ AFMOA/SGPS  
8901 18th Street, Suite 1  
Brooks Air Force Base, TX 78235-5217  
Telephone: (210) 536-2031  
Fax: (210) 536-9032

**Navy Family Advocacy Program**

Director, Family Advocacy Program  
BUPERS 661  
Department of the Navy

Washington, DC 20370-5000  
Telephone: (703) 697-6616/8/9  
Fax: (703) 697-6571

**U.S. Department of Education –  
Safe and Drug-Free Schools Program**

**Safe and Drug-Free  
Schools Program**

U.S. Department of Education  
600 Independence Avenue SW.  
Room 604, Portals Building  
Washington, DC 20202-6123  
Telephone: (202) 260-3954  
Fax: (202) 260-7767  
E-mail: <http://www.ed.gov/offices/OESE/SDFS>

**U.S. Department of Health and  
Human Services – National Center  
on Child Abuse and Neglect**

**National Center on  
Child Abuse and Neglect**

Administration on Children,  
Youth and Families  
U.S. Department of Health  
and Human Services  
P.O. Box 1182  
Washington, DC 20013-1182  
Telephone: (202) 205-8586  
Fax: (202) 260-9351

**National Clearinghouse  
on Child Abuse and  
Neglect Information**

P.O. Box 1182  
Washington, DC 20013-1182  
Telephone: 1-800-FYI-3366  
Fax: (703) 385-3206  
E-mail: [nccanch@calib.com](mailto:nccanch@calib.com)

**U.S. Department of Justice –  
Federal Bureau of Investigation/  
Child Abduction and Serial Killer Unit**

Contact your local FBI Office (see inside front cover of your local telephone directory for the number) or:

**Child Abduction and  
Serial Killer Unit  
Federal Bureau of Investigation**

Quantico, VA 22135  
Telephone: (540) 720-4700  
Fax: (540) 720-4790

**Morgan P. Hardiman Task  
Force on Missing and  
Exploited Children**

Federal Bureau of Investigation  
Quantico, VA 22135  
Telephone: (540) 720-4760  
Fax: (540) 720-4792

**Marine Corps Family Advocacy  
Program**

Marine Corps Family Advocacy  
Program Manager  
Headquarters USMC  
Human Resources Division (Code MHF)  
Washington, DC 20380-0001  
Telephone: (703) 696-2066 or 696-1188  
Fax: (703) 696-1143

**Defense Logistics Agency  
Family Advocacy Program**

Family Advocacy Program Manager  
Quality of Life Program CAAPQ  
Defense Logistics Agency  
8725 John J. Kingman Road, STE 2533  
Fort Belvoir, VA 22060-6221  
Telephone: (703) 767-5372  
Fax: (703) 767-5374

**FBI Headquarters**

Special Investigations and Initiatives Unit  
Office of Crimes Against Children  
Office of Indian Country Investigations  
935 Pennsylvania Avenue NW.  
Washington, DC 20535-0001  
Telephone: (202) 324-3666  
Fax: (202) 324-2731

**U.S. Department of Justice –  
Missing and Exploited  
Children's Program**

**Missing and Exploited Children's Program**

Office of Juvenile Justice and Delinquency Prevention  
810 7th Street NW.  
Washington, DC 20531  
Telephone: (202) 616-3637  
Fax: (202) 307-2819  
World Wide Web: <http://www.ncjrs.org/ojjhome.htm>

**U.S. Department of State – Office  
of Children's Issues**

**Office of Children's Issues**  
Room 4811  
Overseas Citizens Services  
Bureau of Consular Affairs  
U.S. Department of State  
Washington, DC 20520-4818  
Telephone: (202) 736-7000  
Fax: (202) 647-2835  
Autofax: (202) 647-3000

Consular Affairs  
Electronic Bulletin Board:  
(202) 647-9225  
(modem number)  
Internet Address:  
<http://travel.state.gov>

**U.S. Department of Treasury –  
U.S. Secret Service**

**U.S. Secret Service**

Forensic Services Division  
1800 G Street NW.  
Suite 929  
Washington, DC 20223  
Telephone: (202) 435-5926  
Fax: (202) 435-5603

**National Center for Missing  
and Exploited Children**

**National Center for Missing  
and Exploited Children**  
2101 Wilson Boulevard  
Suite 550  
Arlington, VA 22201-3052  
Hotline: 1-800-THE-LOST  
(1-800-843-5678), for the  
United States, Canada,  
and Mexico

Telephone (Business): (703) 235-3900  
TTD: 1-800-826-7653  
Fax: (703) 235-4067  
World Wide Web:  
<http://www.missingkids.com>  
Internet e-mail:  
[77431.177@CompuServe.com](mailto:77431.177@CompuServe.com)  
Cyber Tipline:  
<http://www.missingkids.com/cybertip>

1

2

3

4

5

6



**U.S. Department of Justice –  
INTERPOL**

**INTERPOL**

U.S. National Central Bureau  
U.S. Department of Justice  
Bicentennial Building  
Room 600  
600 E Street NW.  
Washington, DC 20530

MAIN NUMBER (202) 616-9000  
Deputy Chief (202) 616-9000  
Admin Support (202) 616-9000  
Criminal (202) 616-7220

Financial Fraud (202) 616-3850  
State Liaison (202) 616-1051  
Chief (202) 616-9000  
General Counsel (202) 616-7280  
Alien/Fugitive (202) 616-7260  
Drug (202) 616-7230  
Invest Support (202) 616-3900  
State Toll-Free (800) 743-5630

**FAX NUMBERS**

Main Fax Number (202) 616-8400  
Interpol Cryptofax (202) 616-7999

**U.S. Department of Treasury –  
U.S. Customs Service**

**U.S. Customs Service**

International Child Pornography Investigation and Coordination Center  
45365 Vintage Park Road

Suite 250

Sterling, VA 20166

Telephone: (703) 709-9700, ext. 353

Fax: (703) 709-8286

**U.S. Postal Service – U.S. Postal  
Inspection Service**

**U.S. Postal Inspection Service**

Office of Criminal Investigations  
475 L'Enfant Plaza West SW.  
Room 3141  
Washington, DC 20260-2166  
Telephone: (202) 268-4286  
Fax: (202) 268-4563

**U.S. Department of Justice -  
U.S. Immigration and  
Naturalization Service**

U.S. Immigration and Naturalization Service

Office of Inspections (HQINS)

425 I Street NW

Washington, DC 20536

Telephone: (202) 514-3019

Fax: (202) 514-8345

After Hours: (202) 616-5000 (INS Command Center, 7 x 24)



—

|

|

|

—