

COMMITTEE ON THE JUDICIARY

HENRY J. HYDE, Illinois, *Chairman*

F. JAMES SENSENBRENNER, JR.,
Wisconsin
BILL McCOLLUM, Florida
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVEN SCHIFF, New Mexico
ELTON GALLEGLY, California
CHARLES T. CANADY, Florida
BOB INGLIS, South Carolina
BOB GOODLATTE, Virginia
STEPHEN E. BUYER, Indiana
SONNY BONO, California
ED BRYANT, Tennessee
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
ASA HUTCHINSON, Arkansas
EDWARD A. PEASE, Indiana
CHRISTOPHER B. CANNON, Utah

JOHN CONYERS, JR., Michigan
BARNEY FRANK, Massachusetts
CHARLES E. SCHUMER, New York
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey

THOMAS E. MOONEY, *Chief of Staff-General Counsel*
JULIAN EPSTEIN, *Minority Staff Director*

SUBCOMMITTEE ON CRIME

BILL McCOLLUM, Florida, *Chairman*

STEVEN SCHIFF, New Mexico
STEPHEN E. BUYER, Indiana
STEVE CHABOT, Ohio
BOB BARR, Georgia
ASA HUTCHINSON, Arkansas
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina

CHARLES E. SCHUMER, New York
SHEILA JACKSON LEE, Texas
MARTIN T. MEEHAN, Massachusetts
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey

PAUL J. McNULTY, *Chief Counsel*
GLENN R. SCHMITT, *Counsel*
DANIEL J. BRYANT, *Counsel*
NICOLE R. NASON, *Counsel*
DAVID YASSKY, *Minority Counsel*

11915188

LC Control Number



00 300941

KF27
J858
1997
COPY
LL

CONTENTS

HEARING DATE

	Page
November 7, 1997	1
OPENING STATEMENT	
McCollum, Hon. Bill, a Representative in Congress from the State of Florida, and chairman, Subcommittee on Crime	1
WITNESSES	
Cleaver, Cathy, Director of Legal Policy, Family Research Council	32
Ellison, Carol, Senior Editor, HomePC Magazine	18
Rehman, D. Douglas, Special Agent, Florida Department of Law Enforcement	21
Reid, Paul J., Detective, Arlington County Police Department	37
Wiley, Stephen R., Chief of the Violent Crimes and Major Offenders Section of the Federal Bureau of Investigation	4
LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING	
Cleaver, Cathy, Director of Legal Policy, Family Research Council: Prepared statement	35
Ellison, Carol, Senior Editor, HomePC Magazine: Prepared statement	20
Rehman, D. Douglas, Special Agent, Florida Department of Law Enforcement: Prepared statement	23
Reid, Paul J., Detective, Arlington County Police Department: Prepared state- ment	40
Wiley, Stephen R., Chief of the Violent Crimes and Major Offenders Section of the Federal Bureau of Investigation: Prepared statement	6
APPENDIX	
Material submitted for the record	49

CRIMES AGAINST CHILDREN: THE NATURE AND THREAT OF SEXUAL PREDATORS ON THE INTERNET

FRIDAY, NOVEMBER 7, 1997

**HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME,
COMMITTEE ON THE JUDICIARY,
*Washington, DC.***

The subcommittee met, pursuant to notice, at 10:06 a.m., in room 2237, Rayburn House Office Building, Hon. Bill McCollum (chairman of the subcommittee) presiding.

Present: Representatives Bill McCollum, Steve Buyer, Steve Chabot, and Asa Hutchinson.

Also present: Paul J. McNulty, chief counsel; Aerin Bryant, professional staff member, and Kara Norris, staff assistant.

OPENING STATEMENT OF CHAIRMAN MCCOLLUM

Mr. MCCOLLUM. [presiding] This hearing of the Subcommittee on Crime will come to order. This morning we will examine the nature and threat of pedophiles on the Internet and other related dangers posed to children on the Internet.

Recently, highly publicized news accounts in which pedophiles have used the Internet to seduce or persuade children to meet them to engage in sexual activity, have sparked vigorous debate about the wonders and perils of the information superhighway. One report indicates that almost half of all children ages 12 to 17 use the Internet. Another study claims that 10 million children have access to the Internet. That number is expected to more than double in the next 5 years.

With the advent of ever-growing computer technology, law enforcement officials are discovering that criminals roam the Internet just as they roam the streets. While parents strive to warn their children about the dangers outside the home, they may be failing to warn their children about the dangers within on the World Wide Web. Cyber-predators often cruise the Internet in search of lonely, rebellious, and trusting young people. The anonymous nature of the online relationship allows users to misrepresent their age, gender, and interests to reach into the home and befriend a child.

Today, we will hear from witnesses who will demonstrate the ease in which children can be exploited through online chat rooms and bulletin boards designed for and frequented by children. These online forums allow computer users to exchange typed messages about a particular subject and to engage in conversations with like-

minded souls, often perfect strangers. In this environment, a middle-aged man could actually be masquerading as a 12-year-old girl. Clever pedophiles manage to befriend and gain the trust of youngsters who may eventually agree to a face-to-face meeting. In recent cases, youths who have agreed to such meetings have been photographed for child pornography, raped, beaten, robbed, and worse. The use of the Internet by pedophiles to seduce and lure children for such illicit purposes is a horrifying trend. The stories which are appearing more and more frequently in the papers are astounding.

While there are currently no estimates as to the number of children victimized in cyberspace, the rate at which Federal, State, and local law enforcement are confronted with these types of cases is growing at a rapid pace. As we usher in the computer age, law enforcement will be confronted with even newer challenges. There are virtually dozens of issues pertaining to crimes against children, and the Subcommittee intends to examine many of them over the coming months. The purpose of this hearing is to gain an understanding of the nature and extent of the problem. Other issues such as child pornography and child exploitation, Federal efforts to find missing children, the adequacy of Federal laws pertaining to sexual assault against children, and solutions to these problems will be the subjects of further consideration. I expect one or more hearings related to these important topics after the first of the year. I also expect that we will identify several gaps or shortcomings in Federal law and will need to consider some legislation next year on this issue.

Some of the testimony we will hear today will identify specific changes. Children must be protected from becoming victims of sexual predators. I intend to make it a priority of the Crime Subcommittee to ensure that we are doing all we can to protect our society's most vulnerable members from exploitation and abuse in the computer age. Today's witnesses should provide a full discussion of these issues, and I look forward to hearing their testimony.

I want to recognize Mr. Hutchinson if he wishes to make an opening comment.

Mr. HUTCHINSON. I just want to thank the chairman for showing a great deal of leadership on this issue. The law must keep up with technological advances. We start with the hearing process. This is very important what the witnesses have to say today, and I look forward to working with the Chair and with this committee on any future legislation that might be necessary.

Mr. MCCOLLUM. Thank you very much, Mr. Hutchinson. Our panel today is a distinguished panel, indeed. I will introduce each one of the witnesses, and then we'll proceed to take their testimony.

The Subcommittee's first witness today is Steven Wiley. Currently, Mr. Wiley serves as the Chief of the Violent Crimes and Major Offenders Section of the Federal Bureau of Investigation. Prior to his employment with the FBI, Mr. Wiley served in the United States Marine Corp from April, 1967 to May, 1973, attaining the rank of Staff Sergeant. He entered on duty with the FBI as a Special Agent in 1976, and upon completion of training was assigned to the Alexandria, Virginia Division. Mr. Wiley has served in the FBI in various capacities throughout the years, including as

a supervisor in Counterterrorism Planning with the Counterterrorism Section of the Criminal Investigation Division and as a Chief of the Violent Crimes Fugitive Unit at the FBI Headquarters. From August, 1995 until assuming his current position, he was an Assistant Special Agent-in-Charge of the Atlanta Division. The FBI has agreed to provide a simulated online demonstration of a chat room discussion taken from a previous Federal case. Joining us from the FBI's Innocent Images Task Force will be Supervisory Special Agent Linda Hooper and Special Agent Rick Potocek. They will be assisting Mr. Wiley with this demonstration.

Next, the Subcommittee will hear testimony from Carol Ellison. Ms. Ellison is a senior editor of Home PC Magazine, a position she's held for the past 4 years. She is the founder and director of Home PC Kids' Lab where she works with some 60 children, ages 2 to 16, on software testing and issues related to children's computing. She is co-author of two books, *Parents, Kids and Computers*, and *The Kid's Computer Book*, and her articles on children and technology have appeared in most major computer magazines and many newspapers, including PC Magazine, PC Computing, and the Washington Post Education Review. Ms. Ellison is widely regarded as an authority on children's computing. Ms. Ellison is presently working with the Suffolk County District Attorney's Task Force on Child Safety and the Internet which was established following the arrest of a Long Island man implicated in the Manzie case in New Jersey.

Our third witness today is Dr. D. Douglas Rehman. Special Agent Rehman has been with the Florida Department of Law Enforcement for the past 9 years. Prior to joining FDLE he was with the Illinois State Police, the Port Richey, Florida Police Department, and the Clearwater, Florida Police Department. Special Agent Rehman has spent the past 12 years in the field of electronic surveillance and high-tech investigations including computer crimes. In the past 4 years, he has specialized in the investigation of child exploitation via the computer. Special Agent Rehman is a founding member of the FBI's anti-child exploitation Innocent Images Task Force. He also founded the Central Florida Child Exploitation Task Force, regularly instructs at the FBI Academy, and is the president of the 400-member Florida Association of Computer Crime Investigators. He's spent more than 1,000 hours online in an undercover capacity as a child victim and as an adult pedophile.

Our next witness is Ms. Cathy Cleaver. Ms. Cleaver currently serves as Director of Legal Policy for the Family Research Council where she guides the pro-family organization's approach to cutting edge legal issues. Before joining the Family Research Council, she was the legal counsel and program director for the National Law Center for Children and Families, a legal center founded to strengthen and defend laws against obscenity, child pornography, and sexual exploitation. In this role, Ms. Cleaver advised State and Federal lawmakers on the constitutionality of pornography-related legislation and participated in training conferences across the country for prosecutors and investigators of obscenity and child pornography. Ms. Cleaver also drafted legal briefs in cases before the Supreme Court and Federal Courts of Appeal with the National Law Center. Ms. Cleaver earned her Bachelor's Degree from the Univer-

sity of South Florida and her Juris Doctor from the Georgetown University Law Center. She is also a National Institute for Trial Advocacy graduate.

Our final witness appearing before this Subcommittee today is Paul Reid. Detective Reid is a 17-year veteran of the Arlington County, Virginia Police Department. He's been assigned to the criminal investigations division of the police department for 12 years and the sex crimes unit for the past 7 years where he has been an integral part of numerous investigations involving the exploitation of children by pedophiles. Detective Reid has received extensive training in the field of child abuse, ranging from domestic abuse to exploitation on the Internet. He is a two-time recipient of the United to Save America Diamond Award for his efforts pertaining to investigations of pedophiles exploiting children. He has, in recent years, been assigned to the FBI Innocent Images Task Force. He's also sat on committees for the National Center for Missing and Exploited Children in reference to exploitation of children on the Internet.

For all of the witnesses, without objection, your entire written testimony will be submitted into the record. Hearing no objection, it's so ordered. We have the potential for considerable interruption today with votes. I hope it isn't like yesterday, but I'm afraid it may be because we have a lot of procedural votes. So, I ask you to please be concise in what you say. We want to hear everything you have to say fully, but if you could summarize and direct us to the most important parts of your testimony it would be helpful. We'll start in the order in which I introduced you. Mr. Wiley, if you would proceed; you are recognized first.

**STATEMENT OF STEPHEN R. WILEY, CHIEF OF THE VIOLENT
CRIMES AND MAJOR OFFENDERS SECTION OF THE FED-
ERAL BUREAU OF INVESTIGATION**

Mr. WILEY. Thank you. Good morning, Mr. Chairman and members of the subcommittee. I appreciate this opportunity to discuss the serious problem of crimes against children facilitated by the Internet. Our children are our Nation's most valued resource, and they are the most vulnerable members of our society. There's no greater outrage in our society than when we hear of a child who has been mistreated, sexually abused, or murdered. It is paramount that, as a society, we protect our Nation's children, and keep them from becoming victims of crime.

Advances in computer and telecommunications technology have allowed our children to broaden their horizons, thus increasing their knowledge and cultural experiences. This technology, however, has also allowed our Nation's children to become vulnerable to exploitation and harm by pedophiles and other sexual predators.

Commercial online services and the Internet provide the opportunity for pedophiles and other sexual predators to meet and converse with children. Our investigative efforts have shown that pedophiles often utilize chat rooms to contact children. These chat rooms offer users the advantage of instant communication throughout the United States and abroad, and they provide the pedophile an anonymous means of identifying and recruiting children into sexually illicit relationships. Through the use of chat rooms, chil-

dren can chat for hours with unknown individuals, often without the knowledge or approval of their parents. A child does not know if he or she is chatting with a 14-year-old or a 40-year-old. The FBI has investigated more than 70 cases involving pedophiles traveling interstate to meet juveniles or undercover agents and officers posing as juveniles for the purpose of engaging in an illicit sexual relationship.

The FBI is attacking the proliferation of child pornography on the Internet and online services and the problem of pedophiles establishing sexual, illicit relationships with minors through the use of the Internet through a comprehensive initiative focusing on crimes against children.

One facet of the FBI's Crimes Against Children program is the Innocent Images initiative which was initiated based upon information developed during a child abduction investigation. The FBI's national initiative on child pornography focuses on those who indicate a willingness to travel for purposes of engaging in sexual activity with a child; those who produce and or distribute child pornography, and those who post illegal images onto the online services and the Internet. Through this initiative, FBI Agents and task force officers go online in an undercover capacity to identify and investigate those individuals who are victimizing children through the Internet and online service providers.

The Innocent Images national initiative is coordinated through the Baltimore Division of the FBI. This initiative provides for a coordinated FBI response to a nationwide problem by collating and analyzing information and images obtained from numerous sources to avoid duplication of effort by all FBI field offices. The Baltimore's Division investigative operation involves commitment and dedication of Federal, State, and local law enforcement agencies, working together in a task force environment. The FBI believes that law enforcement agencies should work together, in a coordinated effort, to address crimes against children facilitated by the Internet. It is this sharing of manpower and resources that will ultimately provide the most effective tool in combating this crime problem.

The FBI has taken the necessary steps to ensure that the Innocent Images national initiative remains viable and productive. These efforts include the use of new technology and sophisticated investigative techniques and the coordination of this national investigative effort with other Federal agencies that have statutory investigative authority including the U.S. Customs Service, United States Postal Inspection Service, the Department of Justice Child Exploitation Obscenity Section, which is part of the Criminal Division, and the National Center for Missing and Exploited Children and numerous commercial and independent online service providers.

The FBI also conducts an outreach program to inform the public and local law enforcement agencies about this national initiative. In the past 2 years, the FBI has addressed a number of civic, judicial, prosecutive, and law enforcement organizations concerning this initiative and the assistance the FBI can provide in investigating crimes against children facilitated by the Internet.

The FBI is currently in the process of assigning a supervisory Special Agent on a full time basis to the National Center for Missing and Exploited Children. The FBI strongly believes that it must work closely with the center, a national resource for child protection, to locate and recover missing children, and raise public awareness about ways to prevent child abduction, molestation, and sexual exploitation.

As I mentioned earlier, the FBI has investigated more than 70 cases involving pedophiles traveling interstate to meet minors for the purpose of engaging in illicit, sexual relationships. In one case investigated by the FBI in Maryland and Florida, in conjunction with the Clearwater, Florida Police Department, a subject was arrested in November, 1995 after traveling from his home in Minneapolis, Minnesota to Tampa, Florida for the purpose of having sex with what he thought was a 13-year-old girl whom he had met through an online chat room. In reality, the victim in the case was an undercover FBI Agent. This subject, who was married and the parent of three children, was convicted in Federal court.

Another example of a traveler case involved a resident of Rockville, Maryland who plead guilty to two counts of interstate travel to engage in sexual activity with a minor. Through investigation, this individual was found to have traveled from his Maryland home to Springfield, Virginia for the purpose of meeting a 12-year-old female in order to have sex. After this subject's arrest, a review of his Internet email messages revealed that the subject had been posing as a 16-year-old and had communicated with a number of other girls, between the ages of 10 and 15, attempting to meet them for sex.

Crimes against children are among the most emotional and demanding cases that investigators and prosecutors must face. The FBI will continue to work closely with other law enforcement agencies, the National Center for Missing and Exploited Children, and the Department of Justice to investigate, arrest, and convict those individuals who prey upon our Nation's children.

Mr. Chairman, this concludes my prepared remarks, and at this time, we have a demonstration available. It's an actual case. The information has been redacted to a limited degree, and if I could introduce Rick Potocek who is an Agent assigned to our Innocent Images Task Force in Baltimore.

[The prepared statement of Mr. Wiley follows:]

PREPARED STATEMENT OF STEPHEN R. WILEY, CHIEF OF THE VIOLENT CRIMES AND MAJOR OFFENDERS SECTION OF THE FEDERAL BUREAU OF INVESTIGATION

Good morning, Mr. Chairman and Members of the Subcommittee. I appreciate this opportunity to discuss the serious problem of crimes against children facilitated by the Internet. Our children are our nation's most valued resource and they are the most vulnerable members of our society. There is no greater outrage in our society than when we hear of a child who has been mistreated, sexually abused, or murdered. It is paramount that, as a society, we protect our nation's children and keep them from becoming victims of crime.

Advances in computer and telecommunications technology have allowed our children to broaden their horizons, thus increasing their knowledge and cultural experiences. This technology, however, has also allowed our nation's children to become vulnerable to exploitation and harm by pedophiles and other sexual predators.

Commercial on-line services and the Internet provide the opportunity for pedophiles and other sexual predators to meet and converse with children. Our investigative efforts have shown that pedophiles often utilize "chat rooms" to contact

children. These "chat rooms" offer users the advantage of instant communication throughout the United States and abroad, and they provide the pedophile an anonymous means of identifying and recruiting children into sexually illicit relationships. Through the use of "chat rooms," children can "chat" for hours with unknown individuals, often without the knowledge or approval of their parents. A child does not know if he/she is "chatting" with a 14 year old or a 40 year old. The FBI has investigated more than 70 cases involving pedophiles traveling interstate to meet undercover agents or officers posing as juveniles for the purpose of engaging in an illicit sexual relationship.

The advancement and availability of computer telecommunications also demands that all of us—public officials, law enforcement, parents, educators, commerce and industry leaders—be more vigilant and responsible by teaching our children how to avoid becoming victims of sexual predators. Parents must talk to their children about the potential dangers they may encounter through the Internet and on-line services. Several groups, to include the National Center for Missing and Exploited Children (NCMEC), have issued guidelines for parents on safeguarding children who use computers linked to the information highway. I have attached a copy of those guidelines to this statement. I urge parents to review these guidelines and discuss them with their children. Schools that offer computer classes and access to the Internet should include appropriate discussion of this problem in their curriculum. Creating awareness of the problem is a first step toward reducing a child's vulnerability to sexual predators.

Blocking mechanisms for Internet access are available for parents to restrict access to sexually-oriented Internet and on-line bulletin boards, chat rooms and web sites. These mechanisms can help reduce, but will not totally eliminate, the vulnerability of children. It is possible that children, such as teenagers, may be able to circumvent the restrictions of the blocking mechanism or that pedophiles will still be able to meet children through what may at first appear to be innocent non-interactive activity, such as responding to a newsgroup or web site posting.

The FBI and other law enforcement agencies must continue to develop innovative investigative strategies for dealing with crimes committed in cyberspace and build strong legal precedent to support these investigations and prosecutions.

The FBI is attacking the proliferation of child pornography on the Internet and on-line services and the problem of pedophiles establishing sexually illicit relationships with minors through use of the Internet, through a comprehensive initiative focusing on crimes against children. This initiative encompasses several major crime problems, including: the sexual exploitation of children; child abductions; child abuse on government and Indian reservations; and parental/family non-custodial kidnappings. In May 1997, each of the FBI's 56 field offices designated two special agents as Crimes Against Children coordinators. These coordinators have been tasked with developing multi-agency teams of law enforcement, prosecutive and social service professionals capable of effectively investigating and prosecuting child victim crimes that cross legal and geographical jurisdictional boundaries and which enhance the interagency sharing of intelligence and information. The FBI has and will continue to aggressively address all crimes against children facilitated by the Internet.

One facet of the FBI's Crimes Against Children Program is the "Innocent Images" initiative which was initiated based upon information developed during a child abduction investigation.

In May 1993, the disappearance of ten year old George Stanley Burdyski, Jr., led Prince George's County, Maryland police detectives and FBI agents to two suspects who had sexually exploited numerous juvenile males over a 25 year period. Investigation into the activities of these two suspects determined that adults were routinely utilizing computers to transmit images of minors showing frontal nudity or sexually explicit conduct, as well as to luring minors into illicit sexual activity. It was through this investigation that the FBI recognized that the utilization of computer telecommunications was rapidly becoming one of the most prevalent techniques by which pedophiles and other sexual predators shared sexually explicit photographic images of minors, and identified and recruited children for sexually illicit relationships. The illicit activities being investigated by the FBI are conducted by users of both commercial and private online services, as well as the Internet.

The FBI's national initiative on child pornography focuses on those who indicate a willingness to travel for the purpose of engaging in sexual activity with a child; those who produce and/or distribute child pornography and those who post illegal images onto the online services and the Internet. Through this initiative, FBI agents and task force officers go on-line, in an undercover capacity, to identify and investigate those individuals who are victimizing children through the Internet and on-

line service providers. There are currently 55 field offices assisting and conducting investigations as a result of the "Innocent Images" initiative.

The "Innocent Images" national initiative is coordinated through the Baltimore Division of the FBI. This initiative provides for a coordinated FBI response to a nationwide problem by collating and analyzing information and images obtained from numerous sources to avoid duplication of effort by all FBI field offices.

The Baltimore Division's investigative operation involves the commitment and dedication of federal, state and local law enforcement agencies, working together in a task force environment. The FBI believes that law enforcement agencies should work together, in a coordinated effort, to address crimes against children facilitated by the Internet. It is this sharing of manpower and resources that will ultimately provide the most effective tool in combating this crime problem.

Although the "Innocent Images" initiative is coordinated through the FBI field office at Baltimore, this operation has been franchised to include the Los Angeles field office. The Los Angeles Division also works in a task force environment and is a part of the Southern California Sexual Assault and Exploitation Felony Enforcement Team (the SAFE team).

The FBI has taken the necessary steps to ensure that the "Innocent Images" national initiative remains viable and productive. These efforts include the use of new technology and sophisticated investigative techniques and coordination of this national investigative effort with other federal agencies that have statutory investigative authority, including the United States Customs Service, the United States Postal Inspection Service; the Department of Justice's Child Exploitation and Obscenity Section (part of the Criminal Division); the NCMEC; and numerous commercial and independent on-line service providers.

The FBI also conducts an outreach program to inform the public and local law enforcement agencies about this national initiative. In the past two years, the FBI has addressed a number of civic, judicial, prosecutive and law enforcement organizations concerning this initiative and the assistance the FBI can provide in investigating crimes against children facilitated by the Internet. The FBI is currently in the process of assigning a Supervisory Special Agent, on a full-time basis, to the NCMEC. The FBI strongly believes that it must work closely with the NCMEC, a national resource center for child protection, to locate and recover missing children and raise the public awareness about ways to prevent child abduction, molestation and sexual exploitation. I believe that the assignment of this FBI agent will enhance coordination between the two organizations and benefit the nation in our fight to combat crimes against children.

As I mentioned earlier, the FBI has investigated more than 70 cases involving pedophiles traveling interstate to meet minors for the purpose of engaging in illicit sexual relationships. In one case investigated by the FBI in Maryland and Florida, in conjunction with the Clearwater, Florida, police department, a subject was arrested in November 1995, after traveling from his home in Minneapolis, Minnesota, to Tampa, Florida, for purposes of having sex with what he thought was a 13-year-old girl whom he had met through an on-line chat room. In reality, the "victim" in this case was an undercover FBI agent. This subject, who was married and the parent of three children, was convicted in federal court.

Another example of a traveler case involved a resident of Rockville, Maryland, who pled guilty to 2 counts of interstate travel to engage in sexual activity with a minor (Title 18, USC, Section 2423). Through investigation, this individual was found to have traveled from his Maryland home to the Springfield, Virginia, public library for the purpose of meeting a 12 year old female in order to have sex. After this subject's arrest, a review of his Internet e-mail messages revealed that the subject had been posing as a 16 year old and had communicated with a number of other girls, between the ages of 10-15, attempting to meet them for sex.

Crimes against children are among the most emotional and demanding cases that investigators and prosecutors must face. The FBI will continue to work closely with other law enforcement agencies, NCMEC and the Department of Justice's CEOS to investigate, arrest and convict those individuals who prey upon our nation's children.

This concludes my prepared remarks.

Mr. MCCOLLUM. Certainly, please do so.

Mr. POTOCEK. Mr. Chairman, this is an adjudicated case that occurred last year, and it involves an individual who was the CEO of a manufacturing company in Columbia, Maryland that employed 250 people. On April 11th, 1996 he signed on to America Online, and entered a public chat room using the screen name Xderalte,

and the screen name is, in the days of CB radios, would be like a handle. There may be some identifying information in there about the person; there may not be. While in this chat room, the subject initiated an online conversation with another America Online subscriber, "JulieJ1982." In chat room parlance, by reading that screen name, you might draw the conclusion that Julie J. was born in 1982 and, in fact, "JulieJ1982" was an undercover Agent and had created that name to give that impression; that Julie was born in 1982.

The subject initiated the conversation, first contact with Julie J., who he believed to be a 14-year-old. "Hello, Julie. You must look lovely nude. Glad to find you in this chat room." On that same date, he transmitted two images depicting child pornography to "JulieJ1982." A week later, April 18th, an undercover Agent utilizing the same screen name engaged in an online conversation with the same defendant in a private chat room, and the subject sent another image of child pornography. On May 1st, 1996, the subject transmitted two additional images of child pornography to "JulieJ1992," and on May 20th, 1996, he initiated another online conversation with Julie, and in this conversation discussed meeting Julie at a shopping mall in Tysons Corner, Virginia. It's that conversation that we have here as an example. It is redacted. It's shortened, and some of the language has been substituted with the word "expletive." The subject discusses in sexually explicit detail what he wanted to do with Julie, and on May 21st, the subject transmitted another image depicting child pornography. We found in these cases that the subjects will often send child pornography to reduce the victim's apprehensions about it. It's kind of test balloon; if the victim doesn't recoil or stop conversing, the subject feels like he's making some headway. On May 21st, 1996, the same undercover Agent signed onto America Online using a different screen name, BlueBoy987.

Typically, in these cases, what we'll do is arrange the meeting, and if the subject travels and shows up, we arrest him. The undercover Agent in this case used a different tact, and what he did was when he contacted Xderalte, he said, "I may be able to procure the services of a 14-year-old female for sexual purposes." The subject bit immediately on that. They made an arrangement to meet at a hotel in Arlington, Virginia. The subject traveled from his home in Columbia, Maryland to Arlington, Virginia. He met an undercover Agent; paid the undercover Agent \$180. The scenario was that the girl was in the room next door. In fact, there were several FBI Agents in the room next door. After the payment was made, he was taken into the other room and was arrested. He was charged and he later plead guilty to one count of traveling interstate for the purpose of having sex with a minor. He was sentenced to 1 month in jail, 5 months home detention, and 2 years probation and a \$6,000 fine.

I'm going to run through the conversation here. It is—there are misspellings as there are in a typical chat conversation; people are typing very quickly. Grammar and spelling don't count in chat rooms. I'm going to ignore that as I read through it. Again, it is shortened. There are areas where there was conversation that really wasn't pertinent, and for the purposes of this hearing we elected

to take it out. I think you may have received the full unedited version of the text.

Mr. MCCOLLUM. We do have that for the record, thank you.
[The information referred to follows:]

INNOCENT IMAGES CASE STUDY

"XDERALTE"

On April 11, 1996, the CEO of a manufacturing company employing 250 people based in Columbia, Maryland, signed onto America Online and entered a public "chat" room utilizing the screen name "XDERALTE". While in this chat room the subject initiated an online conversation with another America Online subscriber, JULIEJ1982. JULIEJ1982 was in fact an undercover FBI Agent. The subject initiated the conversation as follows: "Hello, Julie you must look lovely nude. Glad to find you in this chat room". On the same date, he transmitted two images depicting child pornography.

On April 18, 1996, an undercover agent utilizing screen name JULIEJ1982 engaged in an online conversation with the defendant in a private chat room and the subject subsequently sent another image depicting child pornography.

On May 1, 1996, subject transmitted two additional images of child pornography to the screen name JULIEJ1982. On May 20, 1996, he initiated another online conversation with JULIEJ1982 and in this conversation discussed meeting JULIEJ1982 at a shopping mall in Tysons Corner, Virginia. The subject discusses in sexually explicit detail what he wanted to do with JULIEJ1982. On May 21, 1996, the subject transmitted another image depicting child pornography.

On May 21, 1996, the same undercover agent signed onto America Online utilizing the screen name "BLUBOY987". The agent contacted subject online and advised that he (BLUBOY987) could possibly arrange for the subject to purchase the sexual services of minor females. The subject agreed to purchase the services of a 14 year old female.

On June 6, 1996, the subject traveled from the state of Maryland to a hotel located in Arlington, Virginia and paid an undercover agent \$180.00 to have sex with a 14 year old female in a hotel room. He was arrested, charged and later plead guilty to one count of traveling interstate for the purpose of having sex with a minor. He was sentenced to one month in jail, 5 months home detention, 2 years probation and a \$6,000.00 fine.

U404-001

OnlineHost: *** You are in "Julian". ***
 OnlineHost:
 XderAlte: Hello again.
 JULIEJ1982: Hi
 JULIEJ1982: have you been chatting with anyone interesting
 XderAlte: How are you dressed tonight .. I have been
 getting ready to go out just showered
 JULIEJ1982: i just got in from softball practice, jeans and
 sweatshirt
 XderAlte: I have not been doing more than surfing..
 no one really to talk to
 JULIEJ1982: you seem alot younger than your age, what is your
 real age
 XderAlte: Do you mind my being in just my jocky
 shorts
 JULIEJ1982: no not all, where are going?
 XderAlte: I really am 56, Julie.. I have to meet my
 wife later .. she'll be coming from
 work... working late.
 JULIEJ1982: what does she do
 XderAlte: I think talking with you keeps me young :)
 JULIEJ1982: Oh your too sweet
 XderAlte: She is a lawyer// What does your Mom do ?
 JULIEJ1982: :-)
 JULIEJ1982: She works as a nurse
 XderAlte: I'm going to have to capture that tongue in
 my mouth when I kiss you when we
 meet
 JULIEJ1982: I thought you might like my smiling face
 XderAlte: Are you alone now.. ?? Can you chat freely ??
 JULIEJ1982: thanks again for those neat pictures
 JULIEJ1982: Yes, I am home alone
 XderAlte: I love you especially when you smile.
 JULIEJ1982: are you alone at home?
 XderAlte: It makes me want to give you an especially
 big hug.
 XderAlte: Yes, alone till son may come home.
 JULIEJ1982: how old is your son
 JULIEJ1982: i luv hugs
 XderAlte: He is 35, ectually my stepson..He came with
 my second wife who passed away.
 XderAlte: I am married for the third time.
 JULIEJ1982: how long thi stime
 XderAlte: When my daughters were still home we hugged a
 lot..
 XderAlte: Almost 8 years.
 JULIEJ1982: you sound like a very nice father
 XderAlte: Why thank you.. I tried to be..
 XderAlte: Do you get to see yours much ?
 JULIEJ1982: did you ever cheat on your wife

JULIEJ1982: I never see my father
XderAlte: The truth is yes..
XderAlte: I find myself talking very truthfully with
you as I did my own girls.
JULIEJ1982: well i guess sometimes you can be very truthful
and open with strangers
XderAlte: If I asked you a question would you tell
me the truth?? My girls were never
XderAlte: strangers with me .
JULIEJ1982: you can asked me anything, i will tell you the
truth
XderAlte: Have you ever played around in real life
as we did on line ?
JULIEJ1982: I messed around some
JULIEJ1982: did you ever met up with someone you met on line
XderAlte: You know if you were really here I would
want to kiss you all over :)
XderAlte: No I have never actually met anyone I met
on line. Most were far away,
XderAlte: not anywhere near as close as you are in
VA..
JULIEJ1982: exactly what would be all over, is it what I think
XderAlte: Have you ever actually met anyone you met
on line ??
JULIEJ1982: no not exactly
XderAlte: Yes I did mean all over
XderAlte: What do you mean not exactly.,
JULIEJ1982: I was going to met somebody once, but chickened
out
XderAlte: Would you chicken out if we had plans for
lunch, do you think..? I might :)
XderAlte: Are you there, Julie, didn't mean to have that
question upeet you
JULIEJ1982: i don't think so, I in school during lunch
JULIEJ1982: I had to go to the bathroom
JULIEJ1982: the meeting sounds very nice Julian
XderAlte: I would very much enjoy that
XderAlts: I would give you a very gentle hug when we
met!
JULIEJ1982: that would nice
XderAlte: Do you drive ? How would I meet you ? Is
there a restaurant you like very much
JULIEJ1982: no i don't drive, but i have friends who do
XderAlte: I think if we meet it should be someplace
where you would feel safe.
JULIEJ1982: but then what would i do with my friend, what
about a mall
JULIEJ1982: how long do you think we would need
XderAlte: A mall sounds very good.
XderAlte: I thni the first time we meet it should
be just long enough for us to get to
know each other better.. no strings attached
XderAlte: and just see how we are together.
JULIEJ1982: and if we hit it off?

XderAlte: And if we hit it off and we want to meet again we can arrange that after.

JULIEJ1982: hey, before i forget and more cool pictures you can send me

JULIEJ1982: okay what mall

XderAlte: What is convenient for you. I drive.

JULIEJ1982: I know where tysons corner mall is, do you

XderAlte: Yes, I do.. That's a big mall..Perhaps we need a special place in the mall /

JULIEJ1982: what kind of car do you drive

JULIEJ1982: do you know where that would be

XderAlte: I drive a Jeep Grand Cherokee, sand colored

JULIEJ1982: i luv those kind

JULIEJ1982: my mom has vanity plates, do you, i was going to get them when i am old enough to drive

JULIEJ1982: do you like them?

XderAlte: Is there an Eddie Bauer store in that mall

JULIEJ1982: I don't know

XderAlte: I will do a little checking and I will let you know when we decide when it should

JULIEJ1982: okay, your in charge

XderAlte: be,, I have to check my office schedule .

XderAlte: All right darling.. I'll make the suggestions and you can tell me if the dates and times are okay.

XderAlte: that sounds great

JULIEJ1982: I'm looking for a nice gif for you :)

XderAlte: Julian, tell me who you look like the most

XderAlte: Just sent a gif

XderAlte: Did you get it ??

JULIEJ1982: I got it, looks like tonya harding the ice skater. the guy was pretty nice

XderAlte: I'll be back in a second Julia.

JULIEJ1982: any other kids my age?

XderAlte: Yes I was looking for them

JULIEJ1982: did you leave because your wife is home

XderAlte: No .. Had a phone

XderAlte: did you get the second??

JULIEJ1982: no did you send it

XderAlte: I can send yo a picture that was taken of me in my office. I look very stern

JULIEJ1982: i wish i had one of me to send, but i would like to see what you look like

XderAlte: and surely not handsome. I'm afraid after you see it you won't want to talk t

JULIEJ1982: let me decide

XderAlte: Ok, the AOL says you received but did not read the second pic I sent

XderAlte: Now I'll send the one of me.

JULIEJ1982: i would check again, hold on

OnlineHost: *** You are in "Lobby 84". ***

OnlineHost:

OnlineHost:

OnlineHost:

OnlineHost: *** You are in "Julian". ***
OnlineHost:
JULIEJ1982: sorry, i back, did you get my reply
XderAlte: Hello again. I sent the pic of me I'll go
look for your reply now.
JULIEJ1982: Julka
JULIEJ1982: you look alot younger than 66
XderAlte: Hello again.. I think she is 14'15..
XderAlte: Why thank you.. you are sweet to me..
XderAlte: I try to take care of myself.
XderAlte: It will be fun walking around the mall witha
daughter.
JULIEJ1982: nice picture you sent last time, i wonder does it
hurt doing that way, she look like she was
having fun
JULIEJ1982: do you think of me only as your daughter
JULIEJ1982: Ithink she was really enjoying it . There
XderAlte: are lots of different positions.. depe
XderAlte: depends on what you find out you like :)
XderAlte: Would it surprise you if I told you that I
have lots of feelings about you. ??
JULIEJ1982: tell me all about your feelings, remember we are
telling the truth today
XderAlte: And differnt kinds.. But then I had different
feelings about my middle daughter to
JULIEJ1982: tell me how do you know what positions feel good
XderAlte: I feel that I want to hold you and cuddle
you,, but then when I do I have a
JULIEJ1982: what did you do about your feelings for your
daughter
XderAlte: very physical reaction to thhat and just
thinking of holding you and kissing y
JULIEJ1982: what kind of reaction?
XderAlte: you I I get a hard penis almost right away.
XderAlte: And I want to love to in a more mature
way.. I want to kiss your breasts
XderAlte: and play with the nipples with my tongue. I
want to caress your thighs
XderAlte: and feel how smooth and firm they are.
XderAlte: I want to feel my hand removing your
panties..
XderAlte: and feel my fingers opening up the lips
between your legs.
XderAlte: I want my thumb and finger playing with the
clit,, amaking the juices come down .
XderAlte: And feel your hips moving toward me as I
do.
JULIEJ1982: wow
XderAlte: Does it bothar you that I have those
feelings. ??
JULIEJ1982: no problem here, what do you want to do
XderAlte: I guess I want to arrange the meeting with
you..
JULIEJ1982: still in a mall

XderAlte: What I might want and what is best for us are sometimes two different things.

XderAlte: What do YOU want Julie. ?? Tell me what you want of me.. ??

JULIEJ1982: Julian tell me what you want, i will decide what is best

XderAlte: Sitting here at a computer, I want to make you come , to have a grand orgasm

JULIEJ1982: did you have an orgasm

XderAlte: No.. I don't masturbate while I am on line.

XderAlte: Julie, you are still a virgin. !!!

JULIEJ1982: yes I am

XderAlte: It is one thing to use my tongue on you and inside you to make you come and taste your come and have you hold me tight as you do and another thing for me to take your virginity.

XderAlte: Would you really want me inside you ??

JULIEJ1982: will you be gentle?

XderAlte: I will be gentle in everything we do together. !!

JULIEJ1982: when do you want to do this?

XderAlte: I will e-mail you next Monday afternoon when I can get the day to come .

JULIEJ1982: great, still at tysons

XderAlte: That seems like the best place.

JULIEJ1982: i need to know how long will it be since i need someone to drop me off and pick me up.

XderAlte: I have to go off line now.. ..Love you. I'll look for you tomorrow.

XderAlte: I think we should TALK and make friends for real for about 2 hours at our first meeting..

XderAlte: bye, send me more pictures when you can, they are pretty neat

JULIEJ1982: okay Julian, is that really your name?

XderAlte: I'll try to find more for you.

XderAlte: Yes it is., Is Julie yours??

JULIEJ1982: yes Julie Pierce

XderAlte: I love you Julie.. Bye for now

JULIEJ1982: bye sweet dreams

XderAlte: You too.....

OnlineHost: XderAlte has left the room.

Mr. POTOCEK. The very first line—or the second line, online host is—this was on America Online, and that's a system message that Julie has entered a room, a private room, called Julian. This was a room that the subject created for the purpose of this meeting—this cyberspace meeting. Xderalte states, "Hello, again." Julie responds, "Hi. Have you been chatting with anyone interesting?" Xderalte states, "How are you dressed tonight. I've been getting ready to go out; just showered." Julie responds, "I just got in from softball practice, jeans and a sweatshirt." Xderalte, "I have not been doing more than surfing. No one really to talk to." Julie states, "You seem a lot younger than your age. What is your real age?"

Often in these conversations people are typing and sending the message, and the person on the other end hasn't responded to the first question, so you'll see at some points the conversation is a little bit delayed. Xderalte says, "Do you mind my being just in my jockey shorts?" Julie says, "No, not at all. Where are you going?" Xderalte states, "I am really am 66, Julie. I have to meet my wife

later. She'll be coming from work, working late." Julie asks, "What does she do?" Xderalte states, "I think talking with you keeps me young." And Julie responds, "Oh, you're too sweet." Xderalte responding to Julie's first question about his wife, "She's a lawyer. What does your mom do?" And Julie responds, "She works as a nurse." Xderalte says, "I'm going to have to capture that tongue in my mouth when I kiss you when we meet."

The conversation continues to go back and forth. Xderalte then says, "If I ask you a question, would you tell me the truth? My girls were never strangers with me." Apparently, this subject had several daughters who are now grown, and in prior conversations he had talked to Julie about his daughters. Julie says, "You can ask me anything. I will tell you the truth." He asks, "Have you ever played around in real life as we did online?" Julie says, "I messed around some. Did you ever meet with someone you met online?" Xderalte says, "You know, if you were really here, I would want to kiss you all over. No I have never actually met anyone I met online. Most were far away." Undercover Agents will typically do that to find out the extent of this person's activity. When it comes time for a search warrant and an interview we might be looking for other victims, and if in the chat he states that he has met other people, we know to push a little hard in that area. Xderalte, "No, I've never actually met anyone I met online. Most were far away; not anywhere near as close as you are in Virginia." Julie says, "Exactly what would be all over? Is it what I think?" Xderalte says, "Have you ever actually met anyone you met online?" And Julie says, "No, not exactly." Xderalte says, "Yes, I did mean all over, and what do you mean 'not exactly?'"

And the conversation goes back and forth. This is the point where Xderalte starts asking Julie about a meeting, and he starts with something that would sound innocent, lunch at a restaurant. Xderalte says, "Would you chicken out if we had plans for lunch? Do you think?" "I might." He asks if she drives? "How would I meet you? Is there a restaurant you like very much?" Julie says, "No, I don't drive, but I have friends who do." Xderalte, "I think, if we meet it should be some place where you would feel safe." Julie says, "But then what would I do with my friend? What about a mall? How long do you think we would need?" Xderalte says, "A mall sounds very good. I think the first time we meet it should be just long enough for us to get to know each other better. No strings attached, and just see how we are together."

The conversation, again, continues. Xderalte asks, "What is convenient for you; I drive." Julie says, "I know where Tyson's Corner Mall is. Do you?" Xderalte responds that he does. He states, "That's a big mall. Perhaps, we need a special place in the mall." Julie asks what kind of car he drives? And, "Do you know where that would be?" Xderalte responds, "I drive a Jeep Grand Cherokee, sand colored." And Julie says, "I love those kind. My mom has vanity plates. Do you? I was going to get them when I am old enough to drive." I think the undercover Agent, here, was looking for what the license plate was so we could further identify this individual. Julie asked, "Do you like them?" Xderalte asks, "Is there an Eddie Bauer store in that mall?" Julie says, "I don't know." And Xderalte says, "I will do a little checking and will let you know when we de-

cide when it should." And Julie responds, "Okay, you're in charge." The conversation goes back and forth.

Xderalte has sent several pictures via email to Julie, and Julie received them and looked at them—the undercover Agent looked at them—and responds, "Nice picture you sent last time. I wonder, does it hurt doing it that way? She looks like she was having fun. Do you think of me only as your daughter?" Xderalte says, "I think she was really enjoying it. There are lots of different positions. It depends on what you find out you like. Would it surprise you if I told you that I have lots of feelings about you?" Julie responds, "Tell me all about your feelings, and remember, we are telling the truth today." Xderalte says, "And different kinds, but then I had different feelings about my middle daughter too." The undercover Agent says, "Tell me, how do you know what positions feel good?" Xderalte says, "I feel that I want to hold you and cuddle you, but then when I do I have an—" Julie's conversation breaks in. Here, the undercover Agent is suspecting, maybe, there was something that had gone on with his middle daughter, so he's probing that area a little bit. "What did you do about your feelings for your daughter?" Xderalte responds, "Very physical reaction to that, and just think of holding you and kissing you." Julie says, "What kind of reaction?" And it gets graphic here. I've substituted the graphic words with expletive. "You and I get a hard expletive almost right away, and I want to love, too, in a more mature way. I want to kiss your expletive, and play with the expletive with my tongue. I want to caress your thighs and feel how smooth and firm they are. I want to feel my hand removing your panties and feel my fingers opening up the expletive between your legs." I'll skip through the rest. You can read it if you like. Julie responds to all of that with, "Wow." And Xderalte says, "Does it bother you that I have those feelings?" The conversation continues. Julie asks if he'll be gentle? Xderalte says, "I will be gentle in everything we do together."

They discuss what day and what time and how long it will take. Julie, the undercover Agent, is really trying to figure out when and where he has to assemble agents for the arrest. Xderalte says he has to go offline now, "Love you. I'll look for you tomorrow. I think we should talk and make friends for real for about 2 hours at our first meeting." And then, there is a little more conversation. Xderalte then signs off the computer, and that was the end of that conversation.

Mr. MCCOLLUM. Unfortunately, we are going to have to take a break at this point. We have a vote on, and there may be some technical votes. I will announce that we will come back, and I will try to continue the hearing as regularly as possible because we don't want to condense this—we want to have a full hearing. So, this hearing's in recess until we return from the vote on the floor.

[Recess.]

Mr. MCCOLLUM. The Subcommittee on Crime will come to order. I don't know if the presentation was completed at the time we took our recess. Mr. Wiley, Mr. Potocek, do we have more?

Mr. POTOCEK. Yes, sir, I am finished with my presentation.

Mr. MCCOLLUM. Mr. Wiley, do you have more?

Mr. WILEY. No, sir, I don't, Mr. Chairman.

Mr. McCOLLUM. Then, I will recognize Ms. Ellison. You may give us a summarization of your testimony. We look forward to hearing from you.

STATEMENT OF CAROL ELLISON, SENIOR EDITOR, HOMEPC MAGAZINE

Ms. ELLISON. Thank you, Mr. Chairman. It's a pleasure to appear before the committee, today. For the last 4 years I've worked with a group of youngsters at the HomePC Kids' Lab. When we started, these kids were considered exceptional. They were the lucky kids who had access to computers at home and at our office. Today, they are the norm. According to recent reports, nearly half of the 35.3 million family households in this country either have kids online or expect their kids to be online in the very near future, and the number is really growing at an astonishing rate. It's projected that by the year 2002, more than 45 million children will be online. I think that's very good.

Computers and online communications are the tools that kids really will need to succeed in the 21st century, but the power and complexity of the technology also exposes these children unlike any that we've seen before. Just as the Internet allows kids to communicate directly with NASA scientists, and puts photos from Mars at their fingertips, it also exposes them to pedophiles, pornographers, and child predators. Everything from pornographic photos to live teleconferenced orgies can be seen on the computers in family rooms and children's bedrooms today.

Talk to kids about all of this and you'll find that it's so pervasive most of them regard it as a fact of life online. Perhaps, more astonishing but heartening, is that kids, themselves, are often the ones providing the first line of defense against abuse. There's a tremendous informal support network of teens out there. When I've logged on to America Online chat rooms, I've been met by teens who have clued me to the pitfalls I would encounter—thinking that I was a teen—and have offered me advice on how to avoid them. Some of the best advice I've heard on how to get off pornographic email lists came from an 11-year-old boy who works with me in the kids' lab, and a group of teens I know from Long Island recently got together to create their own website; organize their own online games and chats, specifically, because they did not want intrusions by strangers. But these are kids who are relatively trouble-free and who want to keep their lives that way. Children who are feeling alienated and having difficulty socializing at home and at school, are the ones most susceptible to predators.

If the number of calls I receive from reporters, investigators, individual parents, and community groups seeking help with this issue is any indication, incidence of exploitation facilitated by the Internet and the fear they cause in families is on the rapid rise.

It is important as we explore this issue to recognize that the Internet, itself, is not the abuser; it is simply a vehicle no more responsible for other's crimes than the automobile is responsible for a bank heist when a getaway car is used or the telephone is responsible for obscene phone calls. It is impossible to discuss pedophilia and pornography as we are today without feeling deep revulsion, but we cannot lose sight of the fact that all of the Inter-

net tools used to facilitate crimes against children pack tremendous benefit when used by the many who have no hidden agenda.

Chat rooms, online forums, where groups of people gather to talk about almost anything, make wonderful meeting places for clubs, organizations, and support groups. They are also place where teens come together to meet other teens, and, as a result, they have become the favorite of pedophiles who recognize that fact. Private chat rooms, which are not visible to the general public, can be set up by teachers who want their students to chat uninterrupted with scientists or even Members of the House of Representatives, but they can and are being used by pedophiles who invite children into them for their own private conversations.

And there's email, which I think we're all familiar with. In its worse form, however, it arrives as spam mail with live links to pornographic websites and toll free numbers that kids can call, or anyone can call, for a free half hour of hot chat. Named for the Monty Python skit in which diners were repeatedly offered spam no matter how many times they refused it, electronic spam blankets the mailboxes of millions of Internet users each day with no regard to the age, sex, or sensitivities of the recipient.

Parental control software can effectively restrict young children's use of the Internet, but these software-based parental controls are impaired by the fact that they rely on human intervention to make them work. Their use is not particularly high. The parents I know aren't comfortable enough with the technology to set them up, and they believe that their technically savvy kids will find a way around them anyway. Practically speaking, by the age of 12, children begin demanding their independence and the right to make their own decisions. For kids between the ages of 13 and 18, the groups, perhaps, most at risk, parental control software can create more strife than benefit within a family.

What's a parent to do? I am certain that each member of this committee has been asked that question as many times as I have. I'm not certain that Federal legislation is necessarily the answer. Much of the confusion that exists stems from parents not understanding the technology; not knowing what their kids are doing online, and not knowing where to turn when problems arise. We do need improved mechanisms for reporting crime, better education for parents, and for the law enforcement community about what to do when it's suspected. We must clear family and official confusion about how to proceed in these cases, and make the appropriate response for families as well known and clear cut as what they should do when they receive pornography through the mail or obscene phone calls on the phone.

Finally, I shared the pain of many in America who saw the Barbara Walters with the Manzie family on 20/20 last week. This is the family of the 15-year-old boy in New Jersey charged in the murder of an 11-year-old. Sam Manzie, himself, was abused by a man that he met on the Internet. The confusion and stress caused by the tangle of jurisdictions in that case contributed to an already troubled situation. Since so many of these cases do cross State lines and do involve many different legal authorities, attention should be given to streamlining the investigative and prosecutorial processes so that they are more sensitive to the victims and their families.

I welcome your attention to these issues, and will be happy to answer any questions you may have.

[The prepared statement of Ms. Ellison follows:]

PREPARED STATEMENT OF CAROL ELLISON, SENIOR EDITOR, HOMEPC MAGAZINE

Carol Ellison is Education Editor of HomePC, a publication of CMP Media. She is the founder and director of HomePC Kids' Lab where she works with some 60 children, ages 2 to 16, on software testing and issues related to children's computing and has held that position for the last four years. She is co-author of two books, *Parents, Kids & Computers* (Random House, 1992) and *The Kids Computer Book* (Compute Books, 1994) and her articles on children and technology have appeared in most major computer magazines and many newspapers, including PC Magazine, PC/Computing, Compute, The Network Star-Ledger, The Washington Post Education Review, and the Christian Science Monitor. Ms. Ellison is widely regarded as an authority on children's computing. In January, she appeared as an industry expert on Oprah's show on "Strangers on the Internet" and she has been interviewed frequently by the New York Times, USA Today, and numerous other local and national newspapers and cable news programs for stories regarding child safety on the Internet. Ms. Ellison is presently working with the Suffolk County (Long Island, New York) District Attorney's Taskforce on Child Safety and the Internet which was established following the arrest of the Long Island man implicated in the Manzie case in New Jersey. HomePC's Online Safety Resource Center was developed in cooperation with that Taskforce and the Suffolk County District Attorney. It can be found at HomePC's website, www.homepc.com.

Thank you. It is a pleasure to appear before this committee today. For the last four years, I have worked with a group of about 60 technically-savvy youngsters at the HomePC Kids' Lab. When we started, these kids were considered exceptional. They were the lucky ones who had access to computers and to the Internet. Today they are the norm.

According to a recent report from FIND/SVP's Emerging Technologies Research Group and Grunwald Associates, nearly half of the 35.3 million family households in this country either have kids online or expect their children to be online in the very near future. And that number is growing at an astonishing rate. The Group projects that by the year 2002 more than 45 million children will be online.

And that is good. Computers and online communications are tools that kids will need to succeed in the 21st century. But the power and complexity of this technology also exposes children to risks unlike any we've ever seen before. Just as the Internet allows kids to communicate directly with NASA scientists and puts photos from Mars at their fingertips, it also exposes them to pedophiles, pornographers and child predators. Everything from pornographic photos to live teleconferenced orgies can be seen on computers in family rooms and children's bedrooms.

Talk to kids about all of this and you'll find it is so pervasive they regard it as a fact of life online. More astonishing but heartening is that the kids themselves are often the ones providing the first line of defense against abuse. There is a tremendous informal support network of teens out there. When I logged onto America Online as a 14-year-old girl in preparation for an appearance on the Oprah Winfrey show earlier this year, I was met by teens who clued me to the pitfalls I would encounter and offered sound advice on how to avoid them. Some of the best advice I've heard on how to get off pornographic mail lists came from an 11-year-old boy who works with me in the Kids' Lab. And a group of teens I know from a high school on Long Island recently got together to create their own web site and organize their own online games and chats, specifically to avoid intrusions by strangers.

But these are kids whose lives are relatively trouble-free and who want to keep it that way. Children who are feeling alienated and are having difficulty socializing at home and at school are the ones most susceptible to predators. If the number of calls I receive from reporters, investigators, individual parents, and community groups seeking help with this issue is any indication, incidents of exploitation facilitated by the Internet and the fear they cause is on the rise.

It is important, as we explore this issue, to recognize that the Internet itself is not the abuser. It is simply a vehicle, an more responsible for others' crimes than the automobile is responsible for a bank heist when a getaway car is used or the telephone is responsible for obscene calls. It is impossible to discuss pedophilia and pornography, as we are today, without feeling deep revulsion. But we cannot lose sight of the fact that all of the Internet tools used to facilitate crimes against children pack tremendous benefit when used by the many who have no hidden agenda.

Chatrooms, online forums where groups of people gather to talk about just about anything, make wonderful meeting places for clubs, organizations, and support groups. They are also places where teens come together to meet other teens. They have, likewise, become favorite haunts of pedophiles who recognize that fact.

Private chatrooms, which are not visible to the general public, can be set up by teachers who want their students to chat uninterrupted with a scientist or a Member of the House of Representatives. They also can, and are, being set up by pedophiles who invite children into them for their own private conversations.

And there's e-mail which we're all familiar with. In its worst form, however, it arrives as "spam mail" with live links to pornographic web sites and toll-free numbers to call for a free half-hour of hot chat. Named for the Monty Python skit in which diners were repeatedly offered spam no matter how many times they refused it, electronic spam blankets the mailboxes of millions of Internet users each day with no regard to the age, sex or sensitivities of the recipient.

Parental control software can and does effectively restrict young children's use of the Internet. But these software-based parental controls are impaired by the fact that they rely on human intervention to make them work. Their use is not high. Few parents are comfortable enough with technology to set them up. They believe their technically savvy kids will find a way around them anyway. And, practically speaking, by the age of 12 children begin demanding their independence and the right to make their own decisions. For kids between the ages of 13 and 18, the group that's perhaps most at risk, parental controls can create more strife than benefit within a family.

What's a parent to do? I am certain that each member of this committee has been asked that question as many times I have. I do not know that federal legislation is necessarily the answer. Much of the confusion stems from parents not understanding the technology, not knowing what their kids are doing online and not knowing where to turn when problems arise. We need improved mechanisms for reporting crime and better education for the parents and the law enforcement community. We must clear family and official confusion about how to proceed in these cases and make the appropriate response as well-known and clear-cut to families as what to do when they receive pornography through the mail and obscene calls on the phone.

Finally, I shared the pain of many in America who watched Barbara Walters' interview with the Manzie family on 20/20 last week. This is the family of the 15-year-old boy, charged in the murder of an 11-year-old, who himself was abused by a man he met on the Internet. The confusion and stress caused by the tangle of jurisdictions in that case contributed to an already troubled situation. Since so many of these cases do cross state lines and do involve many different legal authorities, attention needs to be given to streamlining the investigative and prosecutorial processes so that they are more sensitive to the victims and their families. I welcome your attention to these issues and will be happy to answer any questions you may have.

Mr. McCOLLUM. Thank you, Ms. Ellison. Mr. Rehman.

**STATEMENT OF D. DOUGLAS REHMAN, SPECIAL AGENT,
FLORIDA DEPARTMENT OF LAW ENFORCEMENT**

Mr. REHMAN. Mr. Chairman and members of the subcommittee, thank you for this opportunity to address you.

Never before in the history of the world has there been a better time to be a pedophile than today. Both child pornography and child victims are readily available via computer. Advances in computer technology allow for the easy creation and exchange of child pornographic computer image files. Child pornographic magazines from the 1970's as well as a wealth a modern photographs have been converted into computer image files. I routinely seize computer child pornography of two girls that were actually victimized and photographed in Orlando some two decades ago.

Children spend countless unsupervised hours online in chat rooms. Pedophiles look for children that are loners; the children that are apart from the others. The child that's last to be picked for a team; the child alone in their bedroom, online.

The online child exploitation is self perpetuating. I've arrested computer pedophiles that would most likely never have engaged in child exploitation had they not gone online. They go online, and they encounter large numbers of computer pedophiles who extol the virtues of sex with children, and who provide child pornography. This psychological validation begins their downward spiral into child exploitation themselves.

Through the course of numerous Federal prosecutions that I've been involved in, deficiencies in the Federal statutes have come to light. Most can be easily remedied. Additionally, sentences, particularly for repeat offenders, must be increased to reflect the true severity of the offenses. In my written testimony, I've set out 19 needed changes. Child exploitation must be fought by a combined force of Federal, State, and local law enforcement officers. No one level of government can be successful on its own. Together, the Federal agencies and the State and local agencies have the needed resources and experience to combat this child exploitation.

There is, however, a significant need for a national clearinghouse for child exploitation intelligence and evidence as well as investigative coordination. As more agencies and task forces begin independent computer pedophile investigations, the amount of lost intelligence information and evidence that could lead to convictions will become staggering. Likewise, law enforcement agencies will waste valuable resources investigating each other.

The FBI's Operation Innocent Images has amassed a substantial amount of intelligence and evidence. Funding slated for this fiscal year will significantly enhance their capabilities for collecting and analyzing this. Innocent Images should be evolved into this national clearinghouse in order to provide the coordination for child exploitation investigations nationwide.

A recent investigation illustrates what the establishment of a national clearinghouse could accomplish. The FBI office in New York City received a tip that an individual in Florida was trading child pornographic computer images via the Internet that he had made from videotapes of his having sex with girls under the age of 10. This information was immediately provided to the FBI's Innocent Images who in turn provided it to me. Within 36 hours of the tip a multi-agency strike force executed a search warrant on the defendant's residence, and he was in custody. Evidenced seized resulted in the defendant being charged with 42 counts of capital sexual battery for crimes against the two preteen girls. A third victim had not yet been sexually battered, however, the defendant was in the course of building up to it, and would most likely have progressed to the stage within a week or two. This case was successful because a relationship already existed between Innocent Images and the Florida Department of Law Enforcement.

There is a great need to hold a national conference of law enforcement officers and prosecutors who are actively investigation and prosecuting computer pedophiles. This conference would be the foundation for the creation of a national clearinghouse as well as allowing for the exchange of techniques, intelligence, and ideas.

Training must be developed and funded so that large numbers of investigators, nationwide, can become knowledgeable and proficient

in pedophile investigations. Likewise, training for both State and Federal prosecutors must be instituted.

The Tampa to Orlando I-4 corridor is in the process of being designated as a high intensity drug trafficking area and will receive more than \$1 million annually for the establishment and operation of a multi-agency task force to combat drugs. A funding bill for the current fiscal year will provide \$2.4 million for the establishment of child exploitation task forces. This money, however, is for the entire Nation. Countless millions of dollars are spent annually in anti-drug efforts. Only a fraction of that is spent on eliminating child exploitation.

The number of full-time investigators nationwide assigned to conduct proactive pedophile investigations on a full-time bases is less than the number of drug investigators in a typical city. Unlike drug trafficking, there is no one looking to take the place of an arrested pedophile. A concentrated effort at all levels aimed at pedophiles engaged in child exploitation could have a significant impact on the problem. For many years we have been waging a war against illegal drugs. The time has come for a declaration of war against child exploitation in this country. Thank you, sir.

[The prepared statement of Mr. Rehman follows:]

PREPARED STATEMENT OF D. DOUGLAS REHMAN, SPECIAL AGENT, FLORIDA
DEPARTMENT OF LAW ENFORCEMENT

I have been a Special Agent with the Florida Department of Law Enforcement (FDLE) for the past nine and one half years. While attending the University of South Florida in 1984, I began my law enforcement career as a Part-Time Police Officer with the City of Clearwater, Florida. After receiving a Bachelor's Degree in Criminal Justice, I worked as a Police Officer for the City of Port Richey, Florida for one year. Prior to FDLE, I was an Inspector with the Illinois State Police for two and one half years. For the past 12 years, I have been involved in electronic surveillance and high tech crimes.

FDLE is a state law enforcement agency having approximately 350 Special Agents who investigate multi-jurisdictional crimes and provide assistance to other law enforcement agencies.

In 1994, while assigned to the Orlando Operations Bureau of FDLE as the Technical Agent, I received a telephone call from a citizen; he stated that pedophiles were on the computer service America Online looking to trade child pornography and looking for children to meet for sex. I thought the citizen was over dramatizing the situation. That night, I went home and joined America Online, creating a screen name and online persona of a 14 year old boy. I discovered that the citizen had dramatically understated the problem. Within an hour, I had received numerous child pornographic images and was being solicited by pedophiles for sex. Thus began my trek into the sexual exploitation of children via computers, resulting in the investigation, arrest, and conviction of dozens of online predators.

Since 1994, I have specialized in the investigation of child exploitation. I am a founding member of the FBI's Operation Innocent Images Task Force. This Task Force specializes in the identification and investigation, nationwide, of individuals exploiting children via computers. I founded and coordinate the Central Florida Child Exploitation Task Force, an eighteen agency Task Force of city, county, state, and federal agencies. I have provided training to hundreds of law enforcement officers throughout the nation and regularly instruct at the FBI Academy. I have spent more than 1000 hours online in an undercover capacity as a child victim and as an adult pedophile. My undercover work has resulted in approximately 100 investigations nationwide. I regularly provide consultation for law enforcement agencies throughout the nation concerning child exploitation investigations and have testified in both State and Federal Courts as an expert witness in the area of child exploitation and the area of computers. I am the president of the 400 member Florida Association of Computer Crime Investigators and a trained computer forensic examiner. I am also cross sworn as a Deputy U.S. Marshal.

Historically, pedophiles have sought children wherever they gather. School yards and playgrounds have been traditional hunting grounds, with the malls coming into

vogue during the nineties. Today, cyberspace is the child hangout. This provides the pedophile with virtually limitless possibility for victims and the ability to prowl anonymously from home with virtual safety from authorities.

One common trait of pedophiles is their collection of child pornography. They will amass large collections, but rarely, if ever, dispose of the child pornography. Until very recently, child pornography was extremely difficult to obtain with the primary source being European magazines and 8mm films that were published during the 1970's and 1980's. There was a limited number of these magazines in circulation and pedophiles, while wanting more child pornography, would not want to give up what they already had for new material. This made it virtually impossible for the trading of child pornography.

An even more basic problem for the pedophiles was a means to meet each other to trade child pornography, discuss seduction techniques, and for psychological validation of their behavior. Prior to the computer, this was very difficult and dangerous.

In the late eighties and early nineties, computer technology advanced to the point where the European child pornography could be converted to readily reproducible computer image files. This, coupled with the widespread development of computer bulletin boards (BBS), allowed for the commercial distribution of child pornography via computer. Pedophiles would have to pay fees, typically \$50 or more per month, to be able to download this child pornography.

By 1994, America Online (AOL) had created a very simple user interface that allowed persons with very limited computer skills to get online and navigate with ease. AOL also created "chat rooms" on their system. These electronic gathering places allow up to 23 members of AOL to gather and communicate electronically via keyboard. AOL also provided for the exchange of computer files between users via email attachments. In 1994, AOL only had approximately 500,000 members; today, AOL claims well in excess of nine million.

In 1994, child exploitation was becoming well established on AOL. Pedophiles roamed the various chat rooms in search of child victims and other pedophiles. In terms of its use by pedophiles, AOL became a victim of its own success. In 1994, I coined the term computer pedophiles to describe these online predators. The computer pedophiles from AOL that I have arrested and interviewed all claim that they did not get online for the child exploitation, but rather for the same reasons as legal users. They relate that once online, they came across the child exploitation and joined it. AOL has taken many steps to stop the exploitation of children, however, the computer pedophiles remain committed and find ways around these steps.

Child exploitation is not unique to AOL, the other online services have experienced problems from these online predators as well. In the last several years, the Internet has developed a well deserved reputation as a medium for child exploitation.

The newsgroups are the electronic equivalent of cork boards; there are tens of thousands of newsgroups, covering virtually every topic imaginable. Internet users can post messages which other users can read. Additionally, computer image files can be posted and retrieved for viewing. Newsgroups carry important discussions of topics such as health matters, politics, and technology. Unfortunately, they also carry about a dozen newsgroups dedicated to the sexual exploitation of children. Within these groups, pedophiles regularly post nude images of children, frequently child pornography. They discuss seduction of children and look for victims.

Internet Relay Chat (IRC) provides "channels" that are similar to AOL's chat rooms. Unlike AOL, however, there is no regulation of the names of these channels or of the discussion topics. At any given time, there may be dozens of channels that graphically describe their content as being child exploitation; names such as "preteen sex pics" are commonplace. Through various software applications, computer pedophiles meeting in an IRC channel can exchange computer image files directly between their computers.

All of the above makes child pornography readily available online for anyone seeking it.

The online child exploitation is a double edged sword for law enforcement. For the first time in history, law enforcement has a powerful means for investigating child exploitation proactively. The same online anonymity that attracts the computer pedophiles also provides law enforcement officers with the ability to go undercover as child victims or as pedophiles. The reverse, however, is that computer pedophiles can readily obtain real victims and easily trade child pornography.

Perhaps the worst side effect of the online child exploitation is that it is self-perpetuating. I have arrested several computer pedophiles that would most likely never have engaged in child exploitation had they not gone online. Not all persons with pedophilia are child molesters or engaged in the collection of child pornography.

Many are ordinary law abiding citizens who have a sexual attraction towards children, but control these desires and lead normal lives. When these individuals go online, they encounter computer pedophiles who extol the virtues of sex with children and provide them with child pornography. This psychological validation leads the person to believe that they aren't strange or different after all and that it is society, with its laws criminalizing sex with children and pornography involving children, that is wrong. They then begin the downward spiral into child exploitation, typically beginning by trading child pornography, progressing to sexually explicit online conversations with children, and eventually seeking child victims online for sex.

The most troubling aspect about the sexual victimization of boys is that some percentage will go on to molest children themselves. During post-arrest interviews, many pedophiles admit to having been sexually abused as children. While this abuse may help to explain their behavior, the sexual exploitation of children is a volitional act and is not excused by abuse suffered as a child. This factor, however, makes child exploitation unique among crimes: the victim may grow up to victimize.

Since becoming involved in the computer pedophile problem in 1994, I have spent a significant amount of my time conducting computer pedophile investigations. The vast majority of these investigations have been proactive, however, that has recently begun to change. When I first started working these investigations, many people in the criminal justice community believed that pedophiles were not acquiring victims online and that I was manufacturing crimes by my posing as a child. Unfortunately, since 1994 there has been an ever increasing number of reported victimizations of children that began online.

The typical computer pedophile is virtually always a white male and usually middle or upper socio-economic status. The typical age range is approximately 25 to 45 years old, although computer pedophiles as young as nineteen and as old as mid-fifties have been prosecuted. As the generation that was exposed to computers as children ages, the upper age limit will disappear.

It is just as common for computer pedophiles to be married as not, although it is slightly less likely that they have children. Owing to their socio-economic status, white collar males are over represented. Very few computer pedophiles have a criminal history when they are arrested.

In understanding the behavior of pedophiles, it is important to first realize that it is a sexual orientation. Pedophiles are generally considered to be individuals that have a sexual attraction for children, under the age of 18, that are five or more years younger in age than the pedophile. This attraction is no different than the attraction that a heterosexual adult feels for opposite gender peers.

Pedophiles have very predictable behavior traits. These traits have been recognized by courts at all levels throughout the country through their upholding of search warrants that were based upon a pedophile profile. Of prime importance to law enforcement are studies conducted by various clinical researchers, that have found the average child molester will have more than seventy victims throughout their lifetime. Clinical studies and a wealth of experience by law enforcement officers throughout the country show that pedophiles will collect large amounts of child pornography that they rarely, if ever, dispose of.

Pedophiles are typically sexually obsessed with children. One computer pedophile that I arrested stated that he spends most of his day fantasizing about sex with children. Whenever he sees a child, whether in person, in a magazine, or on television, he begins to fantasize about having sex with that child. It is not uncommon for computer pedophiles to spend dozens of hours per week engaged in online child exploitation.

It is difficult to gain a clear picture of the child victims of the computer pedophiles, although they are generally between twelve and sixteen years of age and from middle socio-economic status homes. In many instances, the victims do not see themselves as such. An adolescent boy that is unsure of his sexual identity may explore homosexuality. These boys, afraid of harassment from their peers, look to the gay online community to discuss these issues. The computer pedophiles are all too aware of this and seek out these confused boys. They will provide them with disinformation and sexually victimize them. This victimization is rarely reported; either the boys believe they are gay and therefore the see they sex as consensual, or the boys are embarrassed by what happened and are afraid of peer harassment.

The victimizations of girls, as with boys, is most often reported by a parent or other concerned adult. The girls typically do not see themselves as victims. They view the pedophile as a prince that will take them away to live a grand life in a castle.

Pedophiles in general, and computer pedophiles in particular, are very good at identifying potential victims. Typically, they look for children that are loners. On a playground, they would look for the child that is apart from the others, the child

that is the last to be picked for a team. These same vulnerable children can be found online in great numbers. The children may spend large amounts of time online, often looking for acceptance and understanding. The computer pedophiles seek out these children and fulfill the children's emotional needs. By fulfilling these needs, the computer pedophile gains the child's trust which allows the pedophile to talk the victim into engaging in sexual acts. After being sexually violated, many victims can not articulate why they engaged in the sexual acts with the pedophile. In retrospect, they realize it was a mistake.

From the time that pornographic magazines were first published, adolescent males have sought out these kinds of materials. Pedophiles have always been aware of this and now have a readily available supply of potential victims online. In the course of my undercover activities as a child, I have received thousands of pornographic computer image files, both adult and child. Often the pedophiles will furnish adult pornography to a potential victim as a means of opening communications about sex. Very often, computer pedophiles will supply potential victims with large amounts of child pornography. By showing the child large numbers of other similar children engaging in sexual acts, the pedophile seeks to show the victim that such behavior is normal and pleasurable.

In the seventies, a child pornography magazine published in Europe called "Lolita" solicited the contributions of readers. In what is perhaps the best illustration of the use of child pornography in the victimization of children, one girl appears in an issue of "Lolita." In a subsequent issue, a second girl is shown looking at the issue containing the first girl. In an even later issue, a third girl is shown looking at the issue containing the second girl.

Computer pedophiles prowl the online services and the Internet seeking victims. They will answer postings by children seeking pen pals. They will go into "teen" chat rooms. In an effort to gain the child's confidence, they will sometimes portray children themselves, later introducing their "father", "uncle", or "friend."

Unfortunately, sex pervades our society. Our children are bombarded with sex on television, the movies, in music, in advertising, and virtually every other facet of their lives. Studies show that children are becoming sexually active at younger ages. While the child's reasoning abilities and decision making processes are not yet fully formed, the child is at least sexually curious. This is a pedophile's delight. Many pedophiles, particularly the boylovers, find their child victims in adult sex chat rooms.

When posing as a potential child victim online, it is routine to be simultaneously contacted by ten or more pedophiles seeking cybersex, or sometimes real sex, with a child. It is very much akin to a shark feeding frenzy.

Through the course of numerous federal prosecutions that I have been involved in, deficiencies in the Federal Statutes have come to light. Below, I have attempted to set forth these deficiencies and to make suggestions for improvements. Unless otherwise noted, all Sections or Chapters refer to Title 18 of the United States Code.

(1) While child pornography violations under Chapter 110 are classified as violent crimes, Sections 2422(b) and 2423, both of which involve the sexual victimization of children are not. They should likewise be classified as violent crimes.

(2) There exists no forfeiture provision for items involved in the violation of Sections 2252A, 2422(b), and 2423, yet there are forfeiture provisions for child pornography violations under Sections 2251, 2251A, and 2252. I have been involved in two Federal investigations of violations of Section 2423 where I was forced to forfeit vehicles and computers through Florida's civil forfeiture laws. Forfeiture should apply uniformly to all child exploitation crimes.

(3) Under the Controlled Substances Act, there is a rebuttable presumption that an individual so charged should be detained. No such provision exists for Chapter 110 and Sections 2422(b) and 2423. Pedophiles who trade child pornography and seek to engage in sexual acts with children are at least as great a threat to our society as drug dealers. An identical presumption should be created for any crime involving child exploitation.

(4) A typical violation of Sections 2422(b) or 2423 carries a sentence of approximately twelve to eighteen months of incarceration. This needs to be significantly increased to reflect the severity of the offense. Likewise, sentences imposed under the guidelines for violations of Chapter 110 need to be increased to reflect their severity.

(5) The Florida child pornography statute contains language that makes the possession of each computer image a separate offense. When this is coupled with Florida's sentencing guidelines, it results in a sliding scale of punishment that directly reflects the severity of the offense. Section 2252 (a)(4)(B) merely

specifies the possession of three or more child pornographic computer images. There should be a provision concerning the possession of fifty or more images and its corresponding sentence should be greatly enhanced. Individuals who have amassed that amount of child pornography have significantly contributed to the sexual exploitation of children.

(6) There is no clear, controlling court ruling on whether a thumbnail page, the electronic equivalent of photographic contact sheet that may contain dozens of separate images of child pornography, should be treated as one image for the purposes of possession, or whether each individual image should be treated as a separate offense. This same question applies to other media such as videotapes. It is not uncommon to find a videotape that contains two or more child pornographic images. Should this be treated as one possession or multiple? This question becomes even more important when charging the transmission of child pornography. Often, multiple image files are placed in an electronic envelope called a zip file. This compressed file is then distributed and "unzipped" by the recipient. Traditionally, the "package" has been treated as a single violation.

Each image represents a different victimization of a child and therefore they should be treated as separate offenses for their possession and/or distribution. Sections 2252 and 2252A should be written to clearly make each image a separate offense.

(7) Child erotica can be defined as those items which serve a sexual purpose to a pedophile. This may include nude photographs of children, children's clothing, and writings about inter-generational sex. Although various items of child erotica may have been lawfully seized pursuant to an "expert search warrant", a search warrant that identifies the traits of pedophiles and establishes that the target is one, there is no provision for forfeiture of these items. The government could be forced to return these items to a convicted pedophile who would continue to use the material for sexual fantasies about children. The forfeiture provisions need to be modified to allow for forfeiture of child erotica.

(8) Provisions should be made for long probation terms following incarceration for child exploitation offenses. Recidivism is high among pedophiles. By allowing for extended probation terms, the offender would be under scrutiny for a much longer period and probation violations could serve to quickly re-confine an offender. In Florida, it is not uncommon for persons convicted of child pornography violations to receive five or more years of probation following their incarceration.

(9) Create a new crime for the use of child pornography by a pedophile in the seduction and victimization of a child. Prima facie evidence of a violation should be the sending of such material to a child or someone believed to be a child. Likewise, the sending of pornography to a minor or someone believed to be a minor should be criminalized.

(10) Specifically mandate the reporting by any government employee or contractor who, in the course of their employment, becomes aware of any violation of Chapter 110 and Sections 2422(b) and 2423; failure to do so should be a criminal act. I have heard numerous stories from federal employees of child pornography, found on government computers or admitted to during polygraph examinations, not being reported to law enforcement.

(11) Section 2422(b) needs to be expanded to include the use of a Federally Regulated or Federally Licensed Facility. In a case that I am presently working, the defendant utilized AOL, an interstate facility, to meet a 14 year old boy for sex; this conduct violates Section 2422(b). The defendant also utilized a cellular telephone, a federally licensed facility, to arrange a meeting, however, this conduct does not violate Section 2422(b) as it is presently written. Additionally, although I am not aware of such a challenge yet, Section 2422(b) does not specifically include the Internet. Future legal challenges could be easily prevented by merely defining the Internet as an Interstate Facility.

(12) Although it is the position of the Department of Justice that a Federal Magistrate or Federal Judge may issue a search warrant for the obtaining of stored electronic communications that reside anywhere in the country, I have encountered difficulty in the past. The United States Code uses different definitions in different applicable sections concerning stored electronic communications. Search Warrants for stored electronic communications are more akin to subpoenas than to actual search warrants. Typically, they are served on the service provider who then provides the information to law enforcement. The Code needs to be clarified to reflect the Department of Justice's position.

(13) In several investigations, I have personally encountered computer pedophiles utilizing encryption to conceal their crimes. In one instance, al-

though sufficient evidence existed to convict the pedophile, we were never successful in breaking the encryption used to conceal the majority of his child pornography. The use of encryption in the commission of any offense should be criminalized. As an alternative, a significant sentencing enhancement to the underlying offense could be created.

(14) Provide for the long term confinement of sex offenders who meet specific criteria. This would be modeled on the Kansas law that was recently upheld by the United States Supreme Court. Offenders who have committed sufficiently heinous offenses or evidenced a pattern of offenses should be removed from society for its protection.

(15) Provide for the forfeiture of a pilot's license when it is utilized in the commission of a child exploitation offense. In an investigation I conducted last year, a pedophile with a pilot's license rented a plane and flew to Orlando with the intention of engaging in sexual acts with 14 year old boys, while airborne. After contacting the FAA, I learned that a pilot's license can be revoked for offenses involving drugs, but not child exploitation. Some states, including Florida, provide for the forfeiture of any professional or business license upon a felony conviction, even one in which the license played no role.

(16) While there are minimum mandatory sentences of five years for a person convicted of child pornography offenses that has a prior child exploitation conviction, no such provision exists for Sections 2422(b) and 2423. The minimum five year sentence should be increased to ten years. Anyone who is twice convicted of child exploitation is a clear and present threat to our society.

(17) While Section 2259 provides restitution for victims of Chapter 110, there is no such restitution provision for Sections 2422(b) and 2423. The provisions should apply uniformly.

(18) With the striking down of the Communications Decency Act, law enforcement has been left with no tool for dealing with pornographic spam. Spam refers to advertising email that is sent to tens or hundreds of thousands of recipients that did not request it; it is the electronic version of junk mail. It is becoming common for young children to have email addresses to communicate with their friends and relatives. I have received complaints from parents of these children who have found spam containing advertisement for web sites containing sexual explicit content. Many of these advertisements have embed links in the email that, when clicked on with the mouse, take the recipient to the sexual web site. I personally receive large amounts of this type of spam at email addresses that I utilize undercover portraying children. Our society would not accept the mailing of similar advertisements en masse to any name that could be found anywhere, some of whom will certainly be children, neither should we allow advertisements for porn sites to be sent to email addresses where the recipient's age is unknown, as the recipient may be a child.

(19) There should be a difference in the sentencing guidelines between the possession or distribution of a child pornographic image and the possession or distribution of a child pornographic videotape, film, or video computer file. Currently, both classes of materials are treated identically. Clearly, the exploitation of a child via videotape is more damaging than a single image.

Child exploitation must be fought by a combined force of federal, state, and local law enforcement officers. No one level of government can be successful on its own. It has been my experience that some cases should be prosecuted in state court while others should be federal. The decision where to prosecute an individual is based upon numerous factors that change as the facts of each case change. These factors may include the attitude of prosecutors at the various levels of government, if the defendant's crime is multi-state, the least intrusive venue for the victim, peculiarities of state or federal statutes, and where the greatest sentence can be obtained.

The online services and the Internet span jurisdictional lines. A pedophile in California may send child pornography to an undercover agent in Florida. A pedophile in Kansas may travel to Florida with the intent to engage in sex with the child being portrayed by an undercover agent. A real child may be lured via the computer to travel across the country to be with a pedophile. All of these have occurred and have required the cooperation of various law enforcement agencies at all levels.

During the past three years, child exploitation task forces have started up around the country. Additionally, numerous federal, state, and local investigations are underway. At present, there is no national clearinghouse for these investigations. As more law enforcement agencies begin to conduct their own isolated investigations, the incidence of one agency investigating another's undercover operation will become common. This is an obvious waste of a very finite resource.

The FBI has required that all online child exploitation investigations conducted by the FBI be coordinated by Innocent Images; this is a visionary step. While an investigation may begin in one location, it may branch off throughout the country and may link to other ongoing investigations.

Last year, I began an investigation into an individual in Jacksonville, Florida who was trading child pornographic video files of preteen children. I gained the individuals confidence through undercover operations as an adult pedophile. Unknown to me, a Customs Service investigation elsewhere in the nation had focused on the same individual. Had it not been for my placing intelligence information concerning the individual into our local task force's newsletter and the Customs case agent in Jacksonville happening to read it, a significantly weaker case against the individual would have resulted. I was able to coordinate my investigation with the Customs' investigation and create an air tight case for prosecution.

At the Federal level, the FBI, Customs Service, and Postal Service are all engaged in online undercover investigations. While there is presently some interchange of information, there needs to be a single nationwide clearinghouse for child exploitation investigations. The Federal agencies must be mandated to supply all intelligence information to the clearinghouse so that it can be analyzed and viable targets throughout the country developed. This intelligence must include all evidence obtained through undercover operations, as well as from search warrants. At present, each of the three agencies could be holding evidence of several different transmissions of child pornography by the same individual; when viewed in totality, the individual clearly needs to be targeted. Currently, this information would not be shared and the individual would most likely not be targeted.

Likewise, the numerous task forces and individual agencies throughout the nation must provide the fruits of their investigations to a national clearinghouse. While it is somewhat easier for the Federal Government to mandate that federal agencies must participate than it is to mandate state and local agencies must participate, the state and local agencies can be induced to participate. Participation should also include the adoption of investigative guidelines and standards. The receipt of federal funds by any task force or individual agency for child exploitation investigations should be conditioned upon that agency participating in the national clearinghouse.

The clearinghouse would collect and analyze all of the intelligence information. Targeted individuals would then be referred out to participating agencies/task forces for investigation. The clearinghouse would also serve as a central coordination point for undercover operations, including sting operations.

Innocent Images has amassed a substantial intelligence database. The capabilities of this database will be significantly enhanced by funding slated for this fiscal year. Innocent Images should be evolved into the national clearinghouse.

A recent investigation illustrates what can be accomplished when law enforcement agencies cooperate. The FBI office in New York City received information from a citizen that an individual in Florida was engaging in sexual acts with girls under the age of ten, videotaping the acts, making child pornographic computer images from the video tapes, and trading the images on the Internet. This information was immediately provided to the FBI's Innocent Images. I was contacted by Innocent Images and provided with the information. Within 36 hours of the information becoming known, the individual and one of the victims had been positively identified, a strike force of FBI Agents, FDLE Agents, and Sheriff's Office Detectives was assembled, a search warrant for the defendant's residence obtained and executed, the defendant arrested, and a videotaped confession obtained. Subsequent examination of the seized evidence resulted in the defendant being charged in State Court with forty-two counts of Capitol Sexual Battery for crimes against two girls, as well as the manufacture of child pornography involving those two girls and one other. While the third victim had not yet been sexually battered, the defendant was in the course of building up to it and would most likely have progressed to this stage within a week or two.

This case also illustrates the need for a specialized team of investigators that can respond to an area within hours to conduct similar investigations. It was fortuitous that this case happened in the Orlando area where a wide variety of resources can be assembled in a brief period. The case required a computer examiner, an expert in the interview of child victims, an expert in the interview of pedophiles, as well as an investigator with a thorough understanding of child exploitation via computer. Had the defendant been located elsewhere, it might have been impossible to assemble such a team in a reasonable amount of time. With modern air travel and communications, a rapid response team could be assembled anywhere in the country in a timely manner. The members of the team would not have to work out of the same location day to day. Rather, they would form into a team upon assembling for an investigation.

It should be noted that while it took less than 36 hours to arrest the defendant in that case, it took hundreds of man-hours of investigation afterwards to examine all of the evidence, interview all of the victims, and prepare the case for prosecution. This is common in computer pedophile investigations. The undercover work leading up to an arrest can take as little as a couple of hours, whereas, the follow-up investigation may take weeks.

These child exploitation investigations require varied investigative skills. In order to be successful, the investigator must first understand the medium via which the crime is committed. Crimes in cyberspace require an entire subset of investigative skills to be able to prove beyond a reasonable doubt that the defendant was the one behind the keyboard. In addition to being able to conduct computer crime investigations, the investigator must be thoroughly familiar with child exploitation, including both pedophile and victim behaviors.

While there are a relatively large number of trained sex crimes investigators throughout the country, few have the luxury of specializing in child exploitation and the resources to excel in this area. Most have enormous case loads that require them to shuffle investigations as quickly as possible. By contrast, excluding the military, there are very few computer crime investigators nationwide.

The number of investigators nationwide that are assigned to conduct computer pedophile investigations on a full-time basis numbers around two or three dozen. There are other investigators engaged in the part-time investigation of computer pedophiles, but their numbers are not significant. Generally, they are sex crimes detectives who may work a few proactive computer pedophile investigations as their caseloads permit.

Although I work these cases on a full-time basis, I still am burdened with responsibilities for electronic surveillance, radio communications, and computer evidence recovery.

One recurring problem that I have observed in federal law enforcement is a lack of recognition of the skills necessary to conduct child exploitation cases in general and computer pedophile cases specifically. There is a view that any agent is capable of investigating any crime. This may be true to a point, however, state and local law enforcement recognized long ago that certain crimes require specialists in order to successfully conclude those investigations. Child exploitation is unquestionably one of those crimes. In the several years that I have been conducting child exploitation investigations, I have continually seen federal agents develop expertise in these cases, only to be transferred to another area of investigation. It is critical that the existing number of law enforcement officers with expertise in child exploitation be maintained and expanded.

A significant federal initiative is needed to provide child exploitation investigation training to all levels of law enforcement. I regularly instruct in a child abuse and exploitation class run by the FBI Academy. Unfortunately, the class is only run once or twice per year with approximately twenty-five students per class. Owing to the broad nature of the class, the students only receive approximately five hours of training specifically relating to computer pedophiles. There needs to be a five to ten day training course created that focuses exclusively on child exploitation and concentrates on teaching those skills necessary to investigate computer pedophiles. The existing FBI class and instructors could easily form the framework of this new training initiative. The class should be designed to train dozens of investigators annually and should be completely federally funded.

Likewise, prosecutors at both the state and federal level need to receive training in the prosecution of these cases. The Child Exploitation and Obscenity Section of the Department of Justice is preparing a training class for federal prosecutors that will be held during the second quarter of 1998. A similar class needs to be developed for state prosecutors. That training must include an understanding of the online environment and how it is used by pedophiles. Where ever possible, one prosecutor in each venue should be designated and trained for the prosecution of these cases.

There is a great need to hold a national conference of law enforcement officers and prosecutors who are actively investigating and prosecuting computer pedophiles. This conference would be the foundation for the creation of a national clearinghouse, as well as allowing for the exchange of techniques, intelligence, and ideas. A further benefit would be the networking of investigators nationwide. All costs of the conference, including the travel and per diem of the participants, should be underwritten by the Federal Government.

Evidence gathering presents a unique problem in these investigations. Just as drug evidence must be examined by a trained forensic technologist, so must computers. Failure to utilize trained forensic examiners may at best result in failure to find evidence and at the worst, result in contamination of the evidence, making it inadmissible in court. The problem, however, is that there are very few trained examin-

ers throughout the country at any level of law enforcement. This is complicated by the fact that even a simple examination may take several days. Complex examinations may take weeks.

Even local agencies that are fortunate enough to have a trained examiner frequently do not have the financial resources to adequately equip them. The startup costs for computer hardware and software necessary to properly equip an examiner can exceed \$35,000; maintaining current hardware and software can cost thousands of dollars annually. Computer evidence recovery is a crucial part of any computer pedophile case.

Large amounts of money need to be invested into the training of law enforcement officers at all levels. This includes training investigators to conduct these investigations, as well as training computer examiners. Money is needed for equipping the investigators and examiners also. The complete funding, including reimbursement for officers' salaries, of child exploitation task forces in areas that have been determined to have high levels of child exploitation could make great inroads into the prevalence of child exploitation. Child exploitation can never be eliminated, however, it should never be allowed to figure as prominently into our society as it now does.

I have been working with the Florida Attorney General's Office of Statewide Prosecution to formulate a strategy for minimizing the availability of child pornography in the Internet newsgroups. The child pornography is principally confined to a few known newsgroups. In an overly simplified manner, the way in which the newsgroups work is that the Internet Service Provider (ISP) subscribes to thousands of newsgroups. When someone makes a posting to a specific newsgroup, it is sent across the Internet. Any ISP that subscribes to that newsgroup will receive that posting and maintain it on their system for a set number of days or weeks. Thus when a child pornographic image file is posted to a newsgroup that a particular ISP subscribes to, the child pornography is physically stored on the ISP's computer system.

Both Federal and Florida Statutes require that an individual have knowledge that the image is child pornography. Our plan is to notify all of the ISPs within Florida that certain newsgroups, which will be specifically identified, have been found to regularly contain child pornography. The letter will place the ISPs on notice that should they provide those newsgroups without removing the child pornography, they will be in criminal violation of Florida Statutes.

Certainly there are First Amendment Rights to free speech that are associated with the newsgroups devoted to child exploitation, however, the ISPs should not be given carte blanche to store and disseminate child pornography on their newsgroup servers via identified newsgroups. If the ISPs do not desire to check every image posted to one of the delineated newsgroups to ensure it is not child pornography, they could discontinue carrying those exploitative groups or they could utilize software that would strip images from postings, but allow text postings in those newsgroups. One ISP I spoke to was under the incorrect impression that they were required by the First Amendment to carry such newsgroups. If this plan was undertaken on a nationwide basis, the prevalence of child pornography contained in the newsgroups could be radically reduced.

While in the past, I have taken cases to both state and federal prosecutors, I have formed a strong working relationship with the office of the United States Attorney in the Middle District of Florida. Charles Wilson, the U.S. Attorney for this District, has made a commitment to prosecuting any child exploitation case that falls within the Federal Statutes. Mr. Wilson has also made a commitment to elevating the Central Florida Child Exploitation Task Force into a true task force where members are assigned on a full-time basis. Presently, it is more of an intelligence unit that provides its members with known resources from other member agencies when needed.

Assistant U.S. Attorney Ana Escobar has been assigned primary responsibility within the Orlando U.S. Attorney's Office for the prosecution of child exploitation. This designation of a single prosecutor makes my job as a case agent much easier. Just as the investigator must understand what is being investigated, so must the prosecutor understand what they are prosecuting. In the past, I have spent considerable time educating a different prosecutor for every case in State or Federal Court. Ms. Escobar has also been given the responsibility for formulating the conversion of the existing task force into a full-time task force, including locating funding sources.

The Middle District of Florida has a very unique child exploitation problem that has been brought to light during numerous undercover operations. As the number one destination in the United States, there are large numbers of pedophiles who travel to Orlando on business or vacation. Investigations have shown that it is common for traveling pedophiles to seek out potential child victims in Orlando well in

advance of their trips. They will work on the potential victims in hopes of engaging in sexual acts when they meet in Orlando. Pedophiles often feel safer molesting a child hundreds or thousands of miles from their home.

Another disturbing aspect of child exploitation in the Orlando area is pedophiles from out of the area that bring child victims with them on vacation. There have been instances of this involving parents, friends of the family, and sponsors of exchange students, among others.

The Orlando and Tampa areas are in the process of being designated as High Intensity Drug Trafficking Areas. This designation will bring more than one million dollars annually to law enforcement in Central Florida for the establishment and operation of a multi-agency task force to combat drugs. A funding bill for the current fiscal year will provide \$2.4 million for the establishment of child exploitation task forces. This money, however, is for the entire nation. Countless millions of dollars are spent annually in anti-drug efforts, only a tiny fraction of that is spent on eliminating child exploitation, yet the damage caused to our society by child exploitation is immeasurable. The countless victims must carry their scars throughout their lifetimes.

It is ironic that in 1994, some of the first computer child pornography that I seized during my undercover work in Orlando was actually created in Orlando some two decades earlier. After the photographs were made in Orlando, the pedophile took the film to Europe where he had it developed and sold it for publication in various child pornography magazines. In a further irony, the Special Agent in Charge of the Orlando FDLE office at the time that I seized it was the case agent in the investigation into its manufacture two decades earlier.

The child exploitation problem is well beyond the resources of state and local law enforcement. A major influx of federal dollars is needed to combat these heinous crimes. In cyberspace, pedophiles routinely cross jurisdictional lines. In the real world, owing to our highly mobile society, pedophiles regularly cross jurisdictional lines. Federally funded task forces must be established throughout the country. The funding must completely underwrite the costs, including officers' salaries. Likewise, additional federally funded and highly trained prosecutors are needed at both the federal and state level to prosecute the avalanche of child exploitation cases.

Unlike drug trafficking, there is no one looking to take the place of an arrested pedophile. A concentrated effort at all levels, aimed at pedophiles engaged in child exploitation, could have significant impact on the problem.

Never before in history has there been a better time to be a pedophile than today; both child pornography and child victims are readily available via computer. Never before in history has law enforcement had an opportunity to impact child exploitation as can be done now via computer. For many years, we have been waging a war against illegal drugs. The time has come for a declaration of war against child exploitation.

Mr. McCOLLUM. Thank you, Mr. Rehman. Ms. Cleaver, you are recognized.

STATEMENT OF CATHY CLEAVER, DIRECTOR OF LEGAL POLICY, FAMILY RESEARCH COUNCIL

Ms. CLEAVER. Okay. Good morning, Mr. Chairman and members of the subcommittee. Dave Barry describes the Internet as a 'world-wide network of university, government, business, and private computer systems run by a 13-year-old named Jason.' This draws a smile precisely because we acknowledge the high proficiency of our children on computers; a proficiency that far surpasses that of their parents. In fact, many parents know only that which their children have taught them about the Internet, making the Internet as accessible to many children as it is inaccessible to many adults.

Now, each week at Family Research Council, we receive telephone calls and letters from people horrified by what their children are encountering online. Now, I'm not here to indict the Internet or to say that pedophiles and pornographers dominate this new medium, but rather to highlight the fact that the Internet provides new and greater opportunities for harm to children. This morning, I'll briefly address the issue of children's easy access to pornog-

raphy and predators' access to children, and I refer members to my written testimony for further information.

I'd also like to recommend an excellent new Little Book, written by Zachary Britton, and published by Harvest House for a February release, called *Safety Net: Guiding and Guarding Your Children on the Internet*, for more information.

The Washington Post has called the Internet the largest pornography store in the history of mankind. There are an estimated 72,000 pornographic sites on the World Wide Web alone, with approximately 39 new explicit sites everyday; everyday. There's always discussion about whether or not you can accidentally come across pornography online. Well, it's absolutely clear that you can. A career-minded child can innocently select a link to a page called "Working Men," and be confronted with men working together with no clothes on.

Further, as Zachary Britton reports in his new book, not all accidental pornography is accidental. When Pathfinder landed on Mars last July, millions of people took to the Internet to look at the beautiful photographs the robot was sending back. An Internet video stripper company foresaw the interest that would be created by the NASA website and created another website with the same name but a different extension, NASA.COM instead of NASA.GOV. So, over a million people a day were subjected to the video stripper content when they typed NASA in their browser's address bar.

In addition, it's not uncommon to receive unsolicited email messages that contain strong sexual conduct and hyperlinks to pornographic websites. With a commonly used email software, it literally takes just one click of a mouse to be viewing a pornographic website.

Here are just a couple of excerpts from the many, many letters we receive. A man from Minnesota wrote us saying, "I am a 23-year-old male currently on probation for sexually assaulting children. Before my conviction and my serving of two—"only 2 years—"in the juvenile facility, I became addicted to pornography. I had not, however, seen any type of child pornography until I went to school—"this is not college—"where there was an Internet connection."

A father from Washington, DC. wrote, "My son called me and said, 'You're not going to believe this. Our teacher wanted us to get familiar with the Internet and told us to log on and surf the net. I logged on to Yahoo and chose movies as my search. One more click and suddenly I was face-to-face with triple X-rated pictures on my screen.'"

And, finally, a mother from Alaska contacted us and told us, "My 13-year-old son chose the unfortunate screen name of Studmuffin. One day, he was sent an email with an unidentified attachment. When he opened it up, it was a close-up photograph of two people engaged in a sex act."

Now, note, that each of these examples are situations where children viewed pornography at school where the diligence of their parents could do nothing to protect them.

Now, turning to predators. An adult who signs on to an AOL chat room as a 13-year-old girl is hit on 30 times within the first

half an hour. Here are just a few of the less highly publicized stories we've become aware of.

Two Long Island men were recently indicted of sexually abusing, raping, and sodomizing a 13-year-old girl they met on the Internet.

Another man traveled to Texas intending to molest a 15-year-old girl he met in an Internet teen chat room where he had told the girl he was 18. After a number of sexually oriented telephone conversations, he bought the girl a plane ticket to San Jose, but when she didn't use it he came to her house.

And, finally, two Houston men were arrested for sexually assaulting two 15-year-old boys. The men operated a gay oriented bulletin board called "Lifestyles" that they used to meet dozens of boys in the Internet—in the Houston area.

And now, just a brief word about laws. Federal laws which completely prohibit the distribution of child pornography and obscenity do apply online. So, with the great respect I have for the members of law enforcement that are testifying here today and who obviously take this issue seriously, there's not enough enforcement of these laws that are currently in place, and the subcommittee may want to examine whether laws are being adequately enforced. But, adults are currently free to send pornography that is neither obscene nor child pornography directly to children without legal recourse. This creates the following irony: publishers and distributors of pornographic magazines and videos are legally forbidden from selling, renting, or displaying these videos in magazines to children in a bookstore or a video store. Yet, the same publishers and distributors are free to sell, display, and provide these same magazines and these same videos to children online. This was the what the CDA was attempting to address.

As for stalking and seduction, last year, the Communications Decency Act prohibited, for the first time, the use of a means of interstate commerce, such as the Internet, for the purpose of enticing or attempting to entice a minor to engage in a criminal sex act. The question, therefore, again, turns to enforcement of a currently existing law.

The subcommittee might also want to address the question of whether penalties for these crimes are sufficient. It's not at all surprising that the parents of this—of a target of the convicted Rockville pedophile we've heard about who contacted 100 young girls online, and had sex with one of them, these parents were outraged when he received only 2 years in prison; the maximum under Federal sentencing guidelines. So often, when the penalties seen tough, sentencing guidelines prohibit them from being tough in practice. This may be an issue that the subcommittee might want to address.

And a final quick word about filtering software. Every effort should be made to protect children online including the use of software designed to block pornography and guard children's personal information. But at a rate of 40 new sites a day, it's impossible for software to be completely effective, and the most sophisticated software can only be effective where it's installed; makes sense. Yet, children are beginning to have access to many computers that don't have filtering software, such as computers in schools; down the street at the neighbors house, and even in the public libraries. The

American Library Association refuses to install blocking software on library computers even for illegal material and even when children only are using these computers. So, it is terribly short-sighted for anyone to believe that software alone can protect children from the dangers online.

I commend the subcommittee for investigating the dangers posed to the children on the Internet, and thank you so much for the opportunity to address this issue.

[The prepared statement of Ms. Cleaver follows:]

PREPARED STATEMENT OF CATHY CLEAVER, DIRECTOR OF LEGAL POLICY, FAMILY RESEARCH COUNCIL

Mr. Chairman and Members of the Subcommittee:

I want to express my sincere appreciation for the opportunity to address this distinguished Subcommittee on the important issue of the dangers posed to children on the Internet.

Dave Barry describes the Internet as a "worldwide network of university, government, business, and private computer systems, run by a 13-year old named Jason." And this description draws a smile precisely because we acknowledge the advanced computer literacy of our children. Most children demonstrate a computer proficiency that far surpasses that of their parents, and many parents know only what their children have taught them about the Internet. In fact, one could go so far as to say that the Internet is as accessible to many children as it is inaccessible to many adults.

Each week we receive telephone calls and letters from parents and other concerned citizens horrified by what children are encountering online. There is a growing sense of frustration that this wonderful new technology, with all of its promise for education, commerce, and communication—especially for the next generation—is being misappropriated by those who would exploit the Internet's capabilities.

Now I want to be clear that I'm not here to indict the Internet, or to say that pedophiles and pornographers dominate this new medium. Rather, the question is: does the Internet provide new and greater opportunities for harm to children. And I think the answer is: yes.

I would like to briefly cover two areas: (1) children's easy access to pornography and (2) pedophiles' easy access to children, in addition to addressing the laws which currently exist related to these matters.

I would like to recommend to the Subcommittee an excellent new book written by Zachary Britton and published by Harvest House to be released next February called *SafetyNet: Guiding and Guarding Your Children on the Internet* for descriptions of the problems and explanations of the technology.

1. CHILDREN'S ACCESS TO PORNOGRAPHY.

There are an estimated 72,000 pornographic sites on the Worldwide Web alone, with approximately 39 new explicit sex sites appearing every day. The Washington Post has called the Internet the largest pornography store in the history of mankind.

There is always discussion about whether or not you can accidentally come across pornography on-line. Well, it is absolutely clear that you can: a career-minded child can innocently select a link to a page called "Working Men" and be confronted with men "working" together without any clothes.

Further, as Britton reports in his new book, not all accidental pornography is "accidental." When Pathfinder landed on Mars last July, millions of people took to the Internet to look at the beautiful photographs the robot was sending back. An Internet video stripper company foresaw the interest that would be created by the NASA Web site and created another Web site with the same name but different extensions—"nasa.com" instead of "nasa.gov." So, over a million people a day were subjected to the video stripper content when they typed "nasa" in their browser's address bar.

In addition, it is not uncommon to receive unsolicited e-mail messages that contain strong sexual content and hyperlinks to pornographic Web sites. With a commonly-used e-mail software (e-mail client software that can display HTML documents), it literally takes just a single mouse click to be viewing a pornographic Web site.

Here are just a few of the many examples of stories reported to us from around the country on the issue of children's access to Internet pornography:

1. A man from Indiana wrote to us, saying:

"My job requires frequent use of the Internet. I bristle when I hear people say there is not much pornography on the Internet, or that it is not easily available. . . . [T]he thing that really stunned me is the presence of child pornography on the Internet. I was grieved when I stumbled on to some homepages of child molesters complete with pictures and boasting about their perversion. . . . Typically, there is nothing to keep a 'net surfer' from viewing whatever he desires."

2. A man from St. Bonifacius, MN wrote to us, saying:

3. "I am a 23 year old male, currently on probation for sexually assaulting children. Before my conviction and my serving of two years in a juvenile facility, I became addicted to pornography. I had not, however, seen any type of child pornography until I went to school, where there was an Internet connection. In a moment of spiritual weakness, I searched for it . . . and came across a link that had quite a few different categories. . . . I do not want any more victims because of this."

4. A father from Washington, D.C. wrote:

"My son called me and said: You are not going to believe this. Our teacher wanted us to get familiar with the Internet and told us to log on and surf the net. I logged on to Yahoo and chose 'movies' as my search. [One more click] and suddenly I was face to face with triple X-rated pictures on my screen."

5. A mother from Alaska contacted us, and told us:

"My 13-year old son chose the unfortunate screen name of 'Studmuffin.' One day he was sent an email with an unidentified attachment. When he opened it up, it was a close-up photograph of two people engaged in a sex act."

6. A mother from Franklin, KY wrote:

"My son's local high school uses SurfWatch. It is a program intended to screen out pornographic or other vulgar web sites, but it fails drastically. He has run into plenty of other students who know how to get around SurfWatch, and view anything and everything they please (all within the library walls)."

II. PEDOPHILES' ACCESS TO CHILDREN.

Pedophiles use the Internet to trade child pornography and to contact children. An adult who signs onto an AOL chat room as a 13-year old girl is hit on 30 times within the first half an hour.

Here are a just a few of the less highly publicized stories we've become aware of:

1. Two Long Island men were recently indicted of sexually abusing, raping, and sodomizing a 13 year old girl they met on the Internet. They also photographed and videotaped their acts with the girl. (New York Post, Wednesday, March 26, 1997.)

2. Another man traveled to Texas intending to molest a 15 year old girl he met in an Internet a teen chat room, where he had told the girl he was 18. After a number of sexually oriented telephone conversations, he bought the girl a plane ticket to San Jose. When she didn't use it, he came to her house and tried to persuade her to go immediately with him to the airport, but he fled when a neighbor intervened. (Chronicle Peninsula Bureau, May 17, 1996.)

3. Two Houston men were arrested for sexually assaulting two 15 year old boys. The men operated a gay-oriented bulletin board called "Lifestyles" that they used to meet dozens of boys in the Houston area. They used the chat rooms to make contact with boys and then invited them to their store, where they would molest them. (Houston Chronicle, Dec. 4, 1995.)

4. An Orlando man met a 15 year old Western Maryland girl in a Prodigy chatroom and encouraged her to run away from home and meet him in Orlando, where he raped her in a hotel room. (The Washington Times, August 30, 1995.)

III. RELEVANT LAWS.

As you know, federal laws prohibiting the distribution of child pornography and obscenity do apply to and cover computer transmission of such material. These laws prohibit the distribution of such material to adults and children alike. Since these laws are in place to deal with the worst of the material on-line, this Subcommittee should consider looking at the issue of whether they are being adequately enforced.

With all due respect to the members of law enforcement who are testifying here today and who obviously take this issue very seriously, the laws in general are not being adequately enforced, and that issue may be worth closer study.

But as to pornography that is neither obscene and nor depicting children, the situation is somewhat different. The portion of the Communications Decency Act that was recently struck down was an effort to address the distribution of *non-obscene* pornography to *children*. Unfortunately, adults are currently free to send non-obscene pornography to children without legal recourse. This creates the following irony: publishers and distributors of pornographic magazines or videos are legally forbidden from selling, renting, or displaying them to children in a bookstore or video store; but the same publishers and distributors are free to sell or display those same magazines and videos to children on-line. I understand that the purpose of this hearing is to explore problems and not solutions—but I simply point out the disparity in application of child-protective laws on-line and off-line as one potential source, or exacerbation, of the problem.

Federal laws addressing child exploitation have been slow to come about. For instance, it was not until December of 1995 that it was even a crime to cross state lines for the purpose of engaging in sex with a minor; before then, only interstate travel for prostitution was illegal. And last year, the Communications Decency Act prohibited for the first time the use of a means of interstate commerce, such as the Internet, for the purpose of enticing or attempting to entice a minor to engage in a criminal sex act. So, as with obscenity and child porn activity, some good laws are there, but the question of adequate enforce should be addressed.

In addition, federal sentencing guidelines limit punishment for first offenses of these type of crimes to two years in prison. So, it is not surprising that the parents of a target of a convicted Rockville pedophile who had contacted 100 young girls on-line and had sex with one 14-year-old were outraged when he received only 2 years in prison. Sentencing guidelines for these crimes must also be addressed.

A quick word about filtering software. Every effort should be made to protect children on-line, including the use of software designed to block pornography and guard children's personal information. But at a rate of 39 new sites a day, it is impossible for software to be completely effective. And the most sophisticated software can only be effective where it's installed; children are beginning to have access to many computers that don't have filtering software, such as computers in schools, down the street at the neighbor's house, and even in public libraries. The American Library Association refuses to allow libraries to use blocking software on library computers, even for illegal material, and even when children are using the computers. So it is terribly short-sighted for anyone to believe that software *alone* can protect children from the dangers on-line.

CONCLUSION

No one can doubt that the Internet is a technological revolution of enormous proportion, with outstanding possibilities for human advancement. Yet we must face the fact that, through the Internet, children are accessing pornography and predators are accessing children. We have got to start considering what kind of society we'll have when the next generation learns about human sexuality from the Internet. What does Internet pornography teach children about intimate relationships? What do chat rooms teach little girls about themselves and their worth?

I commend this Subcommittee for investigating the dangers posed to children on the Internet and appreciate the opportunity to present these comments.

Mr. McCOLLUM. Thank you, Ms. Cleaver. Mr. Reid.

STATEMENT OF PAUL J. REID, DETECTIVE, ARLINGTON COUNTY POLICE DEPARTMENT

Mr. REID. Good morning, Mr. Chairman, members of the subcommittee. For the past 2 years I have worked with the FBI on the Innocent Images Task Force. During those years, I have focused my efforts in two areas in reference to child exploitation on the Internet.

First, I started working on individuals who trade in the child pornography online. I have found both adult pornography and child pornography easily attainable online. Secondly, and what I feel to be the most serious of the offenders, I began to work what the task

force refers to as "traveler cases." These are individuals who are no longer just satisfied with trading kiddy porn but take the next step to actually meet minor children for the purpose of gratifying themselves through sexually illicit conduct.

When I first started investigating pedophilia it was mostly through complaints from parents concerned about an adult at a local park talking to their children; a teacher observing an individual constantly around the school, recreation centers, or things of that nature.

Today, the Internet has become a dream come true for the pedophile. It takes the playground from the street and puts it right into their home where they can cultivate potential victims in secrecy and in seclusion. These child molesters enter chat areas where children frequent usually profiling themselves as minors. Many of the service providers enable them to view a list of online customers by checking profiles of screen names of people online. Once a target in a preferred age range is located that child is then contacted.

While online posing as a young female myself, I have been contacted by numerous individuals in these preteens chat rooms and rooms created specifically for young people or through instant messages. Some take no time in establishing what they are about and talk in sexually explicit text, while others are more cautious in taking their time and careful in evaluating a potential victim.

Pornography is readily available; legal for the pedophiles to obtain, and is often sent to a potential victim in an attempt to lower their inhibitions. Text conversation will often lead to cybersex and/or convincing the child to give them their phone number to have phone sex. They will ask for screen names of their friends who are online, and have them send pictures of them and their friends either via computer or U.S. mail.

I have had them talk me through the process by which one can have their picture, a pic, loaded onto a disk by a commercial vendor and installed onto their own computer so that they can send it to whomever. Conversations will increase and be sexually graphic. The pedophile will tell them, gradually over time, that they're a little older; wait for a reaction, and then further manipulate the child into convincing them that sex with an adult is normal. I have read numerous text conversations recovered by search warrants, done by the task force, we have served on pedophiles subsequent to their arrest. In many cases, although the child has become aware of the age difference, ultimately, they do agree to meet with their molesters.

Child pornography is often sent to a child to further demonstrate that this is a normal activity. The ultimate objective of the pedophile is to meet that child. I have investigated cases where they have traveled great distances to engage in their illicit sexual relations with a minor. They treat their child friend with gifts, money, and enhance the relationship explaining that this is their secret. Many of them will bring cameras with them to photograph their victims.

A case that was recently investigated by the Innocent Images Task Force in which I was the lead investigator was recently adju-

dicated. This case, I feel, illustrates how a pedophile used the computer to benefit his illicit sexual desires.

The parents of 12-year-old female reported that a man known only to them by the screen name of "DeLiteEd" had been communicating with their daughter on America Online. They had allowed her to meet this individual at a local library thinking that he was a male similar in age to that of their daughter. The parents drove their daughter to the library and were to attend a meeting, themselves, in another location at the building. A suspicious mother left her meeting to check on her daughter and meet who she thought was going to be a young man that her daughter had been corresponding with on America Online. She was shocked to see her daughter conversing with an older man. Subsequent investigation, revealed that this man, who I will call Ed, was 64-years of age. The 12-year-old stated that she was about to leave the library with Ed to go to his car where she believed they would engage in sexual activity as "DeLiteEd" had planned.

Subsequently, I assumed the AOL screen name and online identity of the complainant's daughter. A fictitious 13-year-old female, screen name "xqcsxqcs" who I gave a true name of Cris, was introduced to Ed by this screen name, and "xqcsxqcs" began to correspond with Ed via AOL. In January and February 1997, Cris communicated extensively with Ed. Ed sent numerous sexually explicit messages over America Online. On February 10 and 11, Ed transmitted two image files containing photographs of children engaged in sexual activity via AOL to Cris. On February 18th, 1997, Ed communicated via AOL with Cris and planned to meet in person on February 19th in Arlington, Virginia for the purpose of having sex. On February 19th, Ed did travel to Arlington, Virginia and approached Cris who was actually an undercover FBI Agent. Ed was arrested for interstate travel with the intent to have sexual intercourse with a juvenile.

A search warrant was executed at Ed's residence located in Rockville, Maryland. Seized from the location was the defendant's computer equipment along with several letters resulting in the discovery of other victims. A 13-year-old female victim was identified in Atlanta, Georgia who stated that Ed had traveled during November 1996 from Maryland to Georgia and had engaged in sex with her. The task force also determined that Ed had traveled to Pennsylvania and on two occasions to New Jersey for the purpose of engaging in sex with a minor.

Further investigation revealed that Ed had communicated with over 200 females online. These conversations were extensive and sexually explicit in nature. On July 11, 1997, Ed plead guilty to interstate travel for the purpose of engaging in sex with a minor.

The profile of Ed is similar to many other pedophiles that I have investigated and interviewed. Ed is a wealthy, well-educated man. He is married to a woman who held a high a governmental office and himself was a successful computer consultant. He maintained a list of target victims; retained volumes of his conversations with the numerous children he had communicated with, and in many cases, had cybersex with.

I have found that these individuals, once arrested, they are arrogant; they have little or no remorse about their actions; they blame

their demise on the child indicating that the child wanted it, and the child enticed them. Most of these individuals we have encountered from the task force cases have the resources to hire high quality counsel to represent them and will explore every avenue to gain their freedom. Seldom do they cooperate with law enforcement.

I strongly feel that the multi-jurisdictional task force approach provided by the FBI Innocent Images Task Force needs the support of local and Federal law enforcement agencies. The tracking and apprehension of these types of crimes is far reaching, requiring multi-jurisdictional cooperation.

Mr. Chairman, I believe you have before you some literature that I've given you. This is in reference to the case that I had just mentioned. If I could just explain the letter that you have there. The young lady that was online, Cris, had just moved into the area, and she was going to school to see a guidance counselor. The letter that was sent by Lytle (Ed) which is sexually graphic is about this girl going to see a guidance counselor and what happens to her there. The following text is the actual text that lead up to the actual meeting in which this girl did go to meet this individual. And that concludes my statement.

[The prepared statement of Mr. Reid follows:]

PREPARED STATEMENT OF PAUL J. REID, DETECTIVE, ARLINGTON COUNTY POLICE DEPARTMENT

For the past two years I have worked with the FBI on the "Innocent Images Task Force." I have focused my efforts on two areas in reference to child exploitation on the Internet. I worked on individuals who trade in child pornography on-line. I have found both adult pornography and child pornography easily attainable. Secondly, and what I feel to be the most serious of offenders, I began to work with what the task force refers to as "Traveler Cases." These are individuals who are no longer just satisfied with trading kiddie porn but take that next step to actually meet minor children for the purpose of gratifying themselves through sexually illicit conduct.

When I first started investigating pedophiles it was mostly through complaints from parents concerned about an adult at the local park talking to children, a teacher observing an individual constantly around the school or recreation centers, etc.

The Internet has been a dream come true for a pedophile. It has taken the play ground from the street and put it into their home where they can cultivate potential victims in secrecy, and in seclusion.

These child molesters enter chat areas where children frequent, usually profiling themselves as minors. Many of the service providers enable them to view a list of on-line customers by checking profiles of screen names on-line. Once a target in their preferred age range is located, the children are contacted. While on-line posing as a young female, I have been contacted by numerous individuals in these pre-teen chat rooms and rooms created for young people, or through instant messages. Some take no time in establishing what they are about and talk in sexually explicit text, while others are more cautious in taking their time to carefully evaluate a potential victim.

Pornography is readily available, legal for them to obtain, and is often sent to a potential victim in an attempt to lower their inhibitions. Text conversations often will lead to "Cyber Sex," and/or in convincing the child to giving them their phone number to have phone sex. They will ask for screen names of their friends who are on-line and have them send pictures of them and their friends either via computer or U.S. Mail. I have had them talk me through the process by which one can have their picture (PIC) loaded onto a disk by a commercial vendor and installed to their computer so they can send it to them. Once the pedophile is comfortable that they have a potential victim, the manipulation begins. Conversations will increase in sexually graphic text. The pedophile will tell them gradually over time that they are a little older, wait for a reaction, then further manipulate the child convincing them that sex with an adult is normal. I have read numerous text conversations recovered by search warrants we have served on pedophiles subsequent to their arrest. In

many cases, although the child has become aware of the age difference, they ultimately did agree to meet with their molesters.

Child pornography is often sent to the child to further demonstrate that this is a normal activity. The ultimate objective of the pedophile is to meet the child. I have investigated cases where they have traveled great distances to engage in their illicit sexual relations with a minor. They treat their child friend with gifts, money and enhance the relationship explaining that this is their secret. Many of them will bring with them cameras to photograph their victims.

A case that was investigated by the "Innocent Images Task Force" in which I was the lead investigator was recently adjudicated. This case I feel illustrates how a pedophile used the computer to benefit his illicit sexual desires.

The parents of a 12 year old female reported that a man known to them only by the screen name "DeLiteEd" had been communicating with their daughter on America On-line (AOL). They had allowed her to meet with this individual at a local library, thinking that he was a male similar in age to their daughter. The parents drove their daughter to the library and were to attend a meeting themselves at another location of the building. A suspicious mother left her meeting to check on her daughter and to meet this young man with whom her daughter had been corresponding with on AOL. She was shocked to see her daughter conversing with an older man.

Subsequent investigation revealed that this man was Don Lytle, 64 years of age. The 12 year old stated that she was about to leave the library with Lytle to go to his car where she believed they would engage in sexual activity as "DeliteEd" had planned.

Subsequently, I assumed the AOL screen name and the on-line identity of the complainant's daughter. A fictitious 13-year-old female screen name "xqcsxqcs", true name Cris, was introduced to Lytle by this screen name and "xqcsxqcs" began to correspond with Lytle via AOL.

In January and February 1997, Cris communicated extensively with Lytle. Lytle sent numerous sexually explicit messages over AOL. On February 10 and 11, 1997, Lytle transmitted two image files containing photographs of children engaged in sexual activity via AOL to Cris.

On February 18, 1997, Lytle communicated via AOL with Cris and planned to meet in person on February 19, 1997, in Arlington, Virginia, for the purpose of having sex. On February 19, 1997, Lytle traveled to Arlington, Virginia, and approached Cris, who was actually an undercover FBI Agent. Lytle was arrested for interstate travel with the intent to have sex with a juvenile.

A search warrant was executed at Lytle's residence, located in Rockville, Maryland. Seized from that location was the defendant's computer equipment, along with several letters resulting in the discovery of other victims. A 13-year-old female victim was identified in Atlanta, Georgia, who stated that Lytle had traveled during November 1996, from Maryland to Georgia and had engaged in sex with her. The task force also determined that Lytle traveled to Pennsylvania and on two occasions to New Jersey, for the purposes of engaging in sex with a minor.

Further investigation revealed Lytle had communicated with over 200 females. These conversations were extensive and sexually explicit in nature.

On July 11, 1997, Lytle pled guilty to Interstate Travel for the Purpose of Engaging in a Sexual Act With a Minor, Title 18, U.S.C., Section 2423 (b).

The profile of Don Lytle is similar to many other pedophiles that I have investigated and interviewed. Don Lytle is a wealthy, very well educated man. He is married to a woman who held a high governmental office and himself was a successful computer consultant. He maintained a list of target victims, retained volumes of his text conversations with the numerous children he had communicated with and in many cases having "Cyber Sex" with them.

I have found that these individuals, once arrested, are arrogant and have little or no remorse about their actions. They blame their demise on the child, indicating that the child wanted it, the child enticed them. Most of these individuals we have encountered from the task force cases have the resources to hire high quality counsel to represent them and will explore every avenue to gain their freedom. Seldom do they cooperate with Law Enforcement.

I strongly feel that the multi-jurisdictional task force approach, as provided by the FBI Innocent Images Task Force, needs the support of local and federal law enforcement agencies. The tracking and apprehension of these types of crimes is far reaching, requiring multi-jurisdictional cooperation.

Mr. McCOLLUM. Thank you very much, Mr. Reid. In the information that you've given us and in your testimony it appears that the Lytle case involved a sentence of only 2 years, and—

Mr. REID. That's correct.

Mr. MCCOLLUM [continuing]. And that for contacting over a hundred young girls online and having sex with at least one 14-year-old. Is that correct?

Mr. REID. That is correct, sir.

Mr. MCCOLLUM. At this juncture, the prosecutor actually sought even a larger sentence, did he not?

Mr. REID. He did seek an upward departure; yes, sir.

Mr. MCCOLLUM. But he didn't get much of one.

Mr. REID. No, he didn't.

Mr. MCCOLLUM. Now, we have Federal laws that would have allowed either 10 years or 15 years for the actual assault—probably more than that—but the judge in that case was obviously reluctant to do so. Mr. Wiley, do you find that to be true generally that judges are reluctant to depart from the guidelines in these kinds of cases or do you have enough experience to know?

Mr. WILEY. Mr. Chairman, I don't have enough experience to know on the exact sentences, but, generally, from the information I've seen, two to 3 years is a fairly high sentence.

Mr. MCCOLLUM. Mr. Rehman, what about you? Do you think the judges are reluctant to depart from the guidelines, which you've indicated in your testimony are too low?

Mr. REHMAN. Yes, sir. In my experience, I have had a few Federal judges who have upwardly departed, however, the upward departures, typically, only added an additional 6 to 12 months to the sentence. I would agree with Mr. Wiley that it's probably, on average, for child pornography cases, pretty much regardless of the severity of the offense, 30 months is almost a given sentence pretty much throughout the country.

Mr. MCCOLLUM. Now, Xderalte, who plead guilty to and has convicted of traveling interstate for the purpose of having sex with a minor, was sentenced to 1 month in jail, 5 months home detention, 2 years probation, and a \$6,000 fine. Mr. Wiley, is that an adequate sentence someone like this? What should we think of it?

Mr. WILEY. Well, it's hard for me to say exactly. I think it speaks for itself whether it's adequate or not, Mr. Chairman. For an individual to travel interstate to meet with a 14-year-old and is sentenced to 1 month in jail, I don't know if there were extenuating circumstances and what was taken into consideration. As I previously stated, the sentences generally range from two to 3 years—

Mr. MCCOLLUM. But would two to 3 years—

Mr. WILEY [continuing]. And many of them are less than that, sir.

Mr. MCCOLLUM. In the case of the Lytle matter, which Mr. Reid testified to, you actually had an assault, contact with over 100 young girls online, and so forth. However, let's assume Xderalte only had contacted one girl—that you had proof of—and he had no previous convictions. Do you think that a 1 month sentence, a small fine, and probation would be the common sentence? Is that the norm?

Mr. WILEY. Mr. Chairman, I think people who are willing to travel to meet with minors to have sex is probably the most egregious problem in crimes against children. Much more so than indi-

viduals that are trafficking in child pornography, and I think people that are willing to travel should get the most harsh sentences.

Mr. MCCOLLUM. I am deeply disturbed by the apparent sentencing that's going on in this area—whether it's the guidelines or our laws or prosecutions. I'm also disturbed, Mr. Wiley, by what I'm sure you're very familiar with: this Weekly Standard piece in April 1997 discusses the FBI's database as having 4,000 names in it at that time. Of those suspects, I think we now have 152 convictions that you've related to us. They are very critical in the article of the failure to prosecute more, the failure to do more in the investigations, and so on. Can you respond to that?

Mr. WILEY. Mr. Chairman, I think the FBI and those that are involved with the FBI in conducting the Innocent Images type investigations have been very aggressive. We've increased the number of people that are staffing Innocent Images. In addition, just recently, we have franchised the Innocent Images undercover operation to our Los Angeles office, and there is a interagency task force in Los Angeles called the Southern California Sex Assault and Exploitation Felony Enforcement Team, SAFE, and they are going to be going online very shortly as soon as they have the staff—excuse me, the space and doing very similar things that Innocent Images in Baltimore is doing. In fact—

Mr. MCCOLLUM. I just want to clarify something and then you can go ahead and complete your response. It says in here that the FBI has three agents working full-time to handle these 4,000 cases. Was that true in April 1997 when the article appeared?

Mr. WILEY. I don't believe that is true.

Mr. MCCOLLUM. How many agents are working full-time presently on the 4,000 cases?

Mr. WILEY. That's a good point, Mr. Chairman. I—what we have are agents and task force officers working at Innocent Images that are doing the undercover work, and then we have individual agents and support staff that are in all of our 56 field offices that are conducting investigations. So, we have hundreds of people conducting these investigations throughout the country on a regular basis. What goes on in Innocent Images is just the beginning of the investigative process. Once that information is sent to the field, then we have many, many agents in each of the field divisions that are conducting the investigations.

Mr. MCCOLLUM. What you're saying is that an individual FBI Agent, can handle all kinds of cases—bank robberies or whatever—while also handling these cases? So, the number of full-time agents is not as important as how much investigation is actually going into these cases? Is that what you're saying?

Mr. WILEY. Mr. Chairman, actually, we do have full-time people in the field. This year, the Director mandated that we have two individuals, two agents in every field office designated as Crimes Against Children Coordinators. We brought those individuals back, maybe in September and October for training. We'll continue that training throughout this fiscal year, so we have a cadre of people that are very familiar with what's going on at Innocent Images and to develop their own types of task forces with State and local law enforcement.

Mr. MCCOLLUM. Whatever the case may be, one of the things this Committee wants to look into as we move into the next session is what Mr. Rehman discussed, as several of you have, and that is whether or not we have a need for more resources going into this type of investigation. That may require Congress to enact authorization, appropriations, et cetera targeted specifically to this task. I know from sitting on this Committee that with all the other things the FBI has to deal with, it's very hard to suggest that you should move resources from here to there to accomplish this task. However, I think the American public really is ill-served if we don't put enough resources toward this type of investigation.

Mr. HUTCHINSON, you're recognized for 5 minutes.

Mr. HUTCHINSON. Thank you, Mr. Chairman, and let me just continue along the same line with Mr. Wiley. With regard to the task forces, having been a United States attorney I understand every office has a lot of different task forces, and you might have one agent or one assistant U.S. attorney that's assigned to a number of different task forces or things that they're working on. On the Innocent Images Task Force you have 4,000 individuals identified who have engaged at one level or another in child exploitation on the Internet. Now, it's my understanding, I think, it's like 87 of those cases have been prosecuted. Are those categorized and prioritized so that—are the 4,000 being worked or did they not raise to the level of a prosecutable case?

Mr. WILEY. What we tried to do, Congressman, is to make a prosecutable case, and our investigative case file has names that we look at and as soon as we can make a prosecutable case we do that. Often, it's immediate, and on other occasions we wait for another transmission. It depends on the circumstances, but every case gets attention. Every allegation gets attention, and we try to make every single one of them prosecutable.

Mr. HUTCHINSON. Well, on the Innocent Images, did you set up a criteria where there would have to be 10 solicitations or 10 contacts with minors before it would be prosecutable as a matter of priority? I mean, it might just be impossible for three agents to go through 4,000 of them. Was there that type of priority set on these?

Mr. WILEY. There was not a priority on the numbers, because we have to prioritize, because we only have so many agents working. That is not the case. We make sure that we can take a case to prosecution; that's the whole point of the investigation. So, we will, as I said, Congressman, investigate every case and try to make it prosecutable. It isn't a resource issue in terms of the FBI, in terms of whether we investigate it or not. We're going to do that.

Mr. HUTCHINSON. I want to address this question to you, Mr. Rehman and Mr. Reid. Are the cases you investigate prosecuted federally or do any of them go State?

Mr. WILEY. Some of them go State. It depends on once they get investigated as to what the prosecutors think. Some of those can go locally, and some of them go federally.

Mr. REHMAN. That would be my experience also, sir. We—at the point we begin an investigation, make a determination of whether all the factors would be better in—the case would be better served in Federal court or State court, and some of those factors would be what the final sentence would be. We have very strong State child

pornography laws in Florida. The possession of each piece of child pornography is a separate offense by itself, and so when you have a pedophile that has anywhere from 500 to 1,000 pieces of child pornography, that individual's committed in excess of 500 third degree felonies in our State.

Mr. HUTCHINSON. Mr. Reid.

Mr. REID. I would agree that we have done the same and that is that we look for the best possible charge, be it at the State level or at the Federal level, but one thing I have found, if I may, is that if we do choose to go Federal, and there may be another charge that we can do locally, we don't do so. There seems to be some type of an unwritten rule here that if the locals take the case, that the Federal avenues won't and vice versa, and I have found that to be a problem where we could be prosecuting on both avenues and we are not.

Mr. HUTCHINSON. This appears to be a somewhat sophisticated area of investigation and prosecution that requires a significant amount of training—I think Mr. Rehman touched upon this in his written testimony. Being from a rural area, I'm concerned that our rural law enforcement might not be up to speed on this type of crime and the ability to investigate and prosecute. Is that your impression? Do you believe we need more training, particularly in the rural areas? Mr. Wiley?

Mr. WILEY. Congressman, I think we do need more training, and one of the things the National Center for Missing and Exploited Children intends to do is to conduct that kind of training, and the FBI wants to be a partner in that, and with additional resources we can certainly, as we already are going to have an agent assigned over there, have additional agents to do training at the National Center.

Mr. HUTCHINSON. For example, in my district in Arkansas, we have some very, very good FBI, but they are stretched thin. I don't know of any other agency, and I don't think our County Sheriffs are up to speed on this, and I know people are online, and so I really think that there'd be a lot of areas where there could be a gap in investigation and, perhaps, even prosecution. Are there any—well, my time's up, and I just want to compliment Ms. Ellison and Ms. Cleaver. I didn't ask you any questions, but you gave outstanding and very compelling testimony. As a parent, I appreciate your efforts in this and your concern and your testimony. Thank you, Mr. Chairman.

Mr. MCCOLLUM. Thank you very much, Mr. Hutchinson. Unfortunately, we have a vote on, but because your testimony is very important to us I just want to wrap up a little bit here with you. Ms. Ellison, what personal information does somebody have to secure to get an account with an online service provider?

Ms. ELLISON. For the most part, very little. When you sign on, you usually provide your name and a credit card number. Billing, then, is done through the credit card group. You have the option of filling out a personal profile. This is certainly true on America Online and is true on a number of the smaller services as well. Lots of people create profiles. There's no way of knowing that the information in them is accurate or correct. Often it is, but sometimes it's an exaggeration. I think I saw Steve Case, CEO of AOL,

once quoted as saying that there were an awful lot of 24-year-old starlits online.

Mr. MCCOLLUM. All that information's available to somebody else?

Ms. ELLISON. It is available. The spam mail lists that I mentioned take the names from the member directories of these services and from any public bulletin boards where members have posted messages that would identify their email address. There are even utilities that e-mail database operations can run to record the names of people who are moving in and out of chat rooms.

Mr. MCCOLLUM. What's a buddy list?

Ms. ELLISON. A buddy list is what it's called on America Online; you find similar features elsewhere. Let me explain how it works.

Mr. MCCOLLUM. Okay.

Ms. ELLISON. As a user, I would fill out a form that lists the screen names, the user names or email names—you can call them any one of those things—of people who I know and people who I would like to know are online when I'm online. The list is stored in your computer, and when you are on your particular service, the buddy list will pop up and alert you to the presence of the individuals mentioned in the buddy list.

Mr. MCCOLLUM. How would a pedophile take advantage of that?

Ms. ELLISON. They could search through a member directory or gather names from a chat room and enter the names of individuals they suspect to be minors. They could enter, really, anyone's name. It needn't be a friend or family member. It can be anyone you've identified online. Once the buddy is identified as being online, the buddy list usually pops up within a window and gives you the option of sending that person a private message. It will also tell you where, precisely, they are. If they're in a chat room, you then can go to that chat room to talk with them.

Mr. MCCOLLUM. That kind of brings us, Ms. Cleaver, to one of the big problems in all of this: how can, or can, individuals who advertise sexually explicit materials and services on the Internet distinguish between an adult or a child recipient?

Ms. CLEAVER. Well, it depends on where they're advertising, but the issue of, say, a website which is pornographic, being able to determine the age or whether the person coming to the site is a minor or an adult, the industry claims now that it is impossible to do that. I find that hard to believe given that with the Internet capability, it's virtually impossible to find anything that's impossible to accomplish if you have the will to do it. I believe that there's a lack of will in a lot of the industry, but, on the other hand, you can do some—take some cumbersome steps to find out the—whether the person coming to your site is a minor or an adult. There are identification services that cost as little as \$6 or \$7 a year that you can sign up with an adult to prove you're an adult, and if you don't have one of those adult I.D.s then the website could decide to decline to let you come in. There are digital signatures now, becoming a more frequently used option to identify the true identity of someone coming to your site. So, there are questions that can be asked. It will delay the ability of the person seeking the site to get in right away, and that—some people don't like that, but the question is, is there an instantaneous way for a website to be able to determine

that? The industry says now, that it's impossible, and I'm skeptical about that.

Mr. MCCOLLUM. To your knowledge, is any online service provider doing anything today either to do something like you've described or to distinguish the child from the adult?

Ms. CLEAVER. Well, some commercial pornographic sites who want to make money, obviously, charge credit card entry access, and the law generally distinguishes that only adults own credit cards even though we know that's not exactly the case. However—and that would be a good way for commercial providers to distinguish between adults and minors except for the fact that these commercial pornographers often provide many pages of free teaser images to try to get people interested and hooked on their stuff, and they provide those free images to adults and children alike. So, one thing they could be made to do is not provide free images, and if they're going to sell pornography, then go ahead and sell it requiring a credit card. So, some services do do that. When the whole Communications Decency Act was going through the courts, many more did that, and when it failed, we saw that many free images popped right back up there for everyone to see, so there's much more ease for commercial providers to address this adult/child issue, and the Supreme Court acknowledged that.

Mr. MCCOLLUM. Mr. Wiley, listening to all of this talk about America Online today, is America Online or are other service providers doing anything to police illegal activities that you're aware of?

Mr. WILEY. Yes, sir. I think, Mr. Chairman, that America Online is doing some of that policing as I'm told and perhaps the two detectives here could address that better than I that it is a little more difficult now to transmit child pornography on America Online because of what they're doing, and I—

Mr. MCCOLLUM. Mr. Rehman or Mr. Reid, are you familiar with what America Online's doing in particular? Or anyone else in the service provider area?

Mr. REHMAN. America Online, in particular, has begun to police their rooms much more than in the past. Previously, there was a category of rooms known as private rooms where America Online had taken a hands-off approach, saying that those were entirely private. Within the last 6 months after realizing that there was significant amounts of child exploitation occurring in those private rooms, because there were regular rooms set up for the exploitation of children, rooms with names like "Preteen" where pedophiles knew to go, they've changed their software so those rooms are no longer allowed, and when rooms pop up that appear to be like that, they will monitor those rooms to determine whether they are.

Mr. MCCOLLUM. I want to thank all of you for being here today. I wish I could continue this hearing. We've had a lack of some members attending, which I think is due entirely to the nature of this particular day at the end of the session. However, you provided a lot of very valuable information, which just gets us into the subject. I assure you we're going to be doing a lot more with it in the next Congress.

Thank you very much for coming. This hearing is adjourned.
[Whereupon, at 11:42 a.m., the subcommittee adjourned.]

A P P E N D I X

MATERIAL SUBMITTED FOR THE HEARING

PREPARED STATEMENT OF SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, I want to thank you for bringing us together in this forum this morning to examine this critical issue. I am pleased to see that so many of my colleagues share my commitment to making the Internet safer for our children. I hope this hearing today will bring to light the specific ways our children are being subjected to pornography and pedophilia on the Internet. I would like to welcome our distinguished witnesses and look forward to hearing from them about what additional enforcement measures Congress can provide to help eradicate this danger to our nation's young people.

As those of us who are parents know, most children today have computer knowledge and familiarity that far exceeds our own. In excess of 10 million children have access to the Internet today, and that number is expected to more than double within the next five years. This presents us with the challenge of encouraging our children to pursue all avenues to expand their education and horizons, while we simultaneously seeking to protect them from those who may seek to corrupt or abuse them.

By now many of us are familiar with the horrible stories of children lured into online sexual relationships or, even worse, sexually assaulted by predators they met on the Internet. The ubiquitous nature of the Internet means that pedophiles and other strangers with online access and the Internet can invade the sanctity of the home or school and contact children without the knowledge of their parents or teachers. There are currently over 75,000 sex-related web sites on the Internet, and countless chat rooms, newsgroups, and e-mail senders which provide inappropriate material to our children.

I am convinced, however, that there is a way to create a safe Internet environment in which our children can safely explore the Internet and that will let them learn and enjoy access to the ever increasing numbers of useful websites which come on line each day. We, in Congress, must work in conjunction with the men and women of law enforcement, as well as those in the Internet industry who are grappling with this terrible problem, to find a way to make the Internet safe for our young people.

I commend law enforcement for its commitment to protecting our children as they travel the Internet. The Federal Bureau of Investigation, for example, is conducting an on-going nation-wide investigation into the use of computer online services and the Internet to lure minors into illicit sexual relationships and to distribute child pornography. This investigation, called "Innocent Images," has resulted in dozens of arrests and many convictions, but it is just a beginning. Much more remains to be done.

I ask the law enforcement personnel here today: What can we do to help you protect our children from the proliferation of pornography and violence on the Internet? Is it a matter of providing you additional resources to enforce the laws already in place? Is it a question of creating new regulations which will supplement those currently in effect? Or do you need access to better technological capabilities and resources?

In an effort to answer the last of the needs that I just mentioned, I successfully offered an amendment to the Commerce-Justice-State Appropriations bill which was before the House a few weeks ago. This amendment directs the Department of Justice to enter into a contract with the National Research Council of the National Academy of Sciences to conduct a study of computer-based technologies and other approaches that could help to restrict the availability to children of pornographic images through electronic media, including the Internet and on-line services.

My amendment will address the problem of digitized pornographic images which have criminal intent through the identification of software or hardware innovations which currently may be available. We know that most pornographic material on the Internet in the form of words can be blocked by conventional web block software, but the bulk of pornographic material is in the form of images which current technology may or may not be able to detect with a high enough degree of accuracy to aid in the development of enhanced web block software. My amendment would provide for the identification of illegal pornographic images with the goal of criminally prosecuting the purveyors of such pornographic images to children.

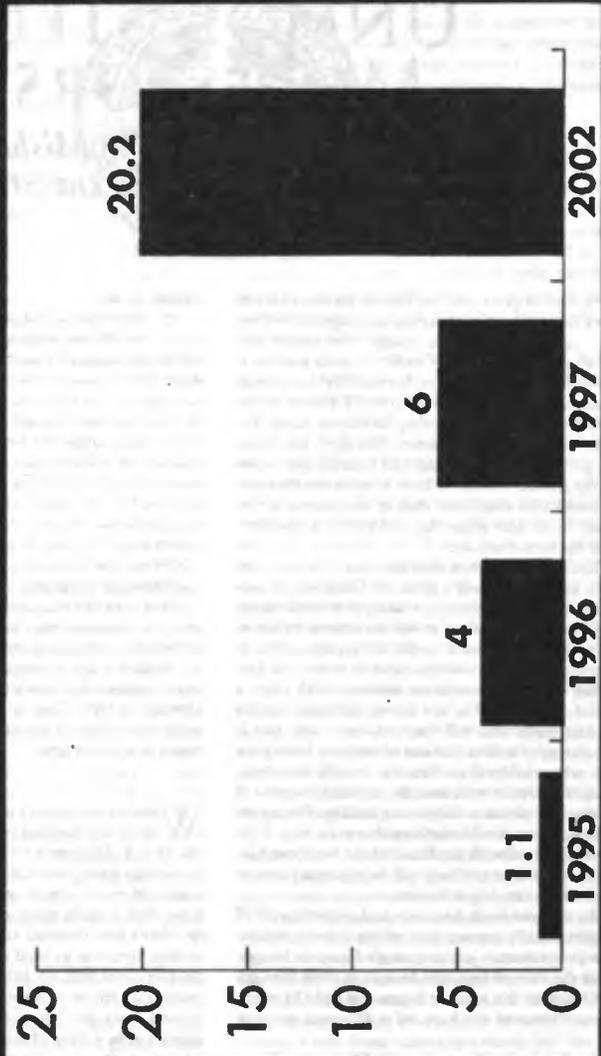
I, like many of my colleagues on this Subcommittee, strongly support the Internet and the introduction of telecomputing technologies into education and commercial settings, but, like my colleagues, I am concerned about the misuse or abuse of this technology.

I am interested in hearing from our esteemed witnesses suggestions for how best to protect our children on the Internet without limiting the fantastic range of information and experience that so characterizes this medium and without impinging on the First Amendment rights of its users. This is most certainly a delicate balance and one that we must navigate with great caution.

Mr. Chairman, I want to thank you again for bringing us here today to engage in a dialogue on this subject of such importance to the security and well-being of our young people. I commend you for your leadership on this issue and look forward to working with you to find an answer to the questions we will hear raised this morning.

Thank you.

Is Your Child One of the Millions Who Have Access to the Internet?



Source: Jupiter Communications
<http://www.jup.com>

Numbers in millions

UNAPPROPRIATELY MISLEADING

How the FBI's Ignoring and Mishandling a Major Child Pornography Investigation

By Todd Lindberg

For three years now, the Federal Bureau of Investigation has been running an undercover operation called "Innocent Images" that targets people who use computers in traffic in child pornography—and the results have been oddly reassuring. Innocent Images has nabbed over 70 people so far, from time to time generating headlines about the arrest of a truly vile perpetrator. But given the explosive growth in online services and Internet use—some put the number of users at 20 to 30 million—the number seems very small. And that, in turn, seems to vindicate those who argue that the problem of online smut has been overstated.

Kiddie porn is more than just smut. Its very existence has been deemed a crime by Congress; its possession and dissemination are both point-blank illegal. It is a crime to distribute it—an act defined by law as the exchange of even a single image, regardless of whether money is involved—and to own it. A first offense can draw a maximum sentence of 15 years; a second offense, 30. The law allows the justice system to come down with full force on those who find it stimulating to look at pictures of children having sex with other children, performing sex acts on adults, engaged in sex acts with animals, depicted in scenes of bondage and sadomasochism, and the like. The material in question is so disturbing that even such First Amendment stalwarts as officials of the American Civil Liberties Union routinely call for vigorous prosecution of traffickers in kiddie porn.

At congressional hearings and elsewhere, FBI officials proudly recount their efforts to bring kiddie-porn perpetrators to justice through Innocent Images. From the start of Innocent Images in 1994 through mid-March of this year, the bureau has had 183 search warrants executed that have led to 88 arrests and over

70 convictions.

But that's not the real story of Innocent Images. In truth, the FBI has nothing to brag about. Rather, it should be hanging its head in shame, because its conduct in the Innocent Images investigation has been nothing short of a scandal, a gross dereliction of duty deserving of congressional hearings and mass firings. For it turns out the FBI has caught a lot more than 70 kiddie-porn traffickers in its net, and is allowing them to slip through. According to congressional and other sources, FBI personnel have acknowledged that, in fact, the bureau has so far compiled a database of 4,000 cases from Innocent Images. In every one of these 4,000 cases, the bureau has solid evidence of distribution of child pornography online.

Data from the U.S. Customs Service offer a telling contrast. Customs, too, runs undercover kiddie-porn investigations involving online services and the Internet because it has authority to investigate the use of any foreign-made products for illegal purposes. Since October 1, 1996, Customs has managed 55 convictions—more than 75 percent of the FBI's total in less than a third of the time.

What are the nation's top law enforcers—the FBI itself, the Justice Department in Washington, the 94 U.S. Attorney's offices throughout the country—doing about these 4,000 people, each of whom, if convicted, would almost certainly face serious prison time? Well, nothing much—and on purpose.

→ Here's how Innocent Images works, according to sources present at a closed-door briefing the FBI gave congressional staff on February 13. An agent goes online via a service provider (America Online especially) and seeks out "chat rooms" where kiddie porn appears to be a topic of discussion. The agent makes known an interest in the subject and asks for others

Todd Lindberg is editorial-page editor of the Washington Times.

with similar interests to send electronic files of images to an e-mail address the agent is using as a drop box. Then it's just a matter of checking the e-mail to see what comes in and from whom. (FBI personnel did exactly this at the February briefing, showing congressional staff a couple of new kiddie-porn pictures that had just been received as part of Innocent Images at the FBI's electronic mailbox.) Upon receipt of an image, which comes with the "username" of the person sending it, the FBI presents a subpoena to America Online seeking the real name and address of the sender. "AOL keeps records of credit card numbers, names and addresses," according to the written notes of a source who attended the briefing. "The FBI then only has to issue subpoenas for records." Thus, a database is born. To take the matter further, as in the case of those actually prosecuted, investigators can use the information they have gathered thus far to seek a search warrant. When they get it, they can search the suspect's home and seize the computer to conduct a forensic examination of its contents.

The FBI is careful to stay away from entrapment—and to avoid falling into the distribution of child pornography itself. In some instances, for example, persons with whom the FBI makes contact will respond to a request for kiddie porn images by saying, in effect, show me yours and then I'll show you mine. The FBI won't do it, and thus won't pursue that individual further. The implication, therefore, is that the FBI's 4,000-name database constitutes only the least subtle and most eager segment of the kiddie porn universe: those willing to hand over an image to a total stranger, apparently in the mistaken belief that the online world actually offers genuine anonymity.

How many more people are sufficiently cautious to avoid the FBI by waiting to receive an image from another user before they send one? And how many more still have realized that AOL and the other online service providers are particularly porous to law-enforcement authorities with subpoenas? As the FBI briefers explained, "There are many more Internet providers [but with them,] identifying the predator and serving a search warrant becomes much more difficult. For example, [Company X], an Internet server, gives a user a new identification number for every sign-on. It is therefore impossible to track the system for distributors."

The federal prosecutions stemming from Innocent Images to date "have been of white men around the age of 40," according to the notes. "Many of the people convicted under the investigation are first time offenders. . . . 98% of those individuals pled guilty. There have been two suicides. These people have been

lawyers, police officers, principals. Generally, they are well educated and employed."

In addition, those selected for prosecution would seem to be only the most egregious and conspicuous of kiddie-porn offenders. The bureau's investigation "targets forwarders and redistributors of child pornography."

This, of course, begs the question: What about the rest? The real starting point in trying to figure out how many kiddie-porn aficionados are out there and doing something about them ought to be the 4,000-name database—and even that is only a beginning. Unfortunately, the FBI, for whatever reasons, seems to have decided to take the 4,000 names and cull for the most blatant cases (the ones easiest to make, perhaps?) instead of using the 4,000 names as a point of departure for an investigation that could potentially net many more offenders.

This is no accident. Sources describe the FBI protocols governing Innocent Images cases as designed apparently with very different goals in mind. The initial protocols called for evidence of 10 separate instances of distribution by a particular individual before the FBI would seek to prosecute. Sources say the number is now three—though, by law, one is enough. It may be that investigators are looking for "jury appeal"—evidence that will hit jurors over the head like a two-by-four. But, as it happens, most of these cases end in plea bargains, anyway. Another problem area is that some U.S. Attorneys are more receptive toward cases of this kind than others; some are overly cautious, whether as a result of the disagreeableness of the evidence in these cases, unfamiliarity with the law, or for other reasons.

The most startling fact of all may be this: To handle these 4,000 potential cases, the FBI has . . . three agents working full-time. Until recently, there was only one. The bureau has 81 people working in congressional relations and public affairs.

The agents themselves deserve praise, obviously, for generating enough material to build 4,000 separate cases against perpetrators most of whom were hitherto unknown to law enforcement. But the FBI and the Justice Department and the Clinton administration seem utterly uninterested in doing anything about it.

What they mainly seem interested in doing now, however, is denying the massive scope of the evidence they have amassed and are sitting on—in an effort to avoid embarrassment over the inaction. Charles Grassley, Iowa Republican and chairman of a Senate Judiciary subcommittee, sent a letter March 27 to FBI director Louis Freeh asking specifically for "the precise number of osmes in this database; how those

names came to be included in the database; why the names included in the database are not being further investigated; [and] any 'threshold' requirements to launch an investigation for sending computerized child pornography." Grassley was asking Freeh to provide, in writing, what FBI briefers had already told congressional staff. One can only imagine the scramble within the FBI and the office of the deputy attorney general, to whom the FBI director reports, as Grassley's April 3 deadline for reply came and went. Freeh finally replied late the next day. His letter, replete with FBI procedural boilerplate, pointedly answered none of Grassley's questions.

It's time to get back to basics. Trafficking in kiddie porn is a serious crime. Nor is this a matter for some neat distinction between "mere" images and the act of child molestation. What we are talking about is photographs of *real* acts of molestation. They have been recorded on film for use by those whose demand for this material can only lead to more instances of molestation in the effort to meet that demand. And law-enforcement authorities know of at least 4,000 people willing to distribute these images for the asking.

Notwithstanding certain fringe views on the subject, most Americans react to child pornography with visceral repulsion. And with fear—for their own children and grandchildren, for the children of their friends and loved ones, and even on behalf of the anonymous children on whom unspeakable horrors are being inflicted for the purpose of feeding the appetite out there for material of this, the worst, sort.

Four thousand names. Is the real problem with this database, then, its very success? Is it just *too many* people? Too many to assimilate, internalize, deal with, process, let alone act upon? Are people running smack into this mountain of data and saying, "Oh, so many, we had better concentrate on the really bad ones," when, in fact, they are *all* really bad ones? Are we now going to define deviancy down, in Sen. Daniel Patrick Moynihan's famous phrase, to allow trafficking in child pornography so long as it is not done to excess?

Or is somebody going to do something about the 4,000? It's hard to imagine how the reaction from ordinary Americans to such an initiative would be anything other than a resounding cheer. Indeed, given what we know about offenders of this kind, it's hard to



WASHINGTON WEEK IN REVIEW

After us, it's all old news. Every Friday night on PBS, Washington Week in Review leads the weekend news programs. Join commentator Ken Belie and Washington's most savvy reporters for up-to-the minute insights on the most vital issues of our day. Seven days in 30 minutes.

A Production of
1997
WETA
Funded by
Ford Motor Company

Imagine you wouldn't have more than 3,000 guilty pleas within 24 hours of the 4,000 arrests. And the cooperation that would ensue from the plea bargainers would probably yield a list of some thousands of hitherto unknown others with similar appetites. This is not symbolic; on the contrary, it would be devastating to the trade in child pornography.

To be sure, resources are tight. But that's an excuse. Mainly what we have is a lack of resolve at the highest levels of law enforcement. People who, when they open the gate to the devil's playground and see that his name is Legion—that he has 4,000 demons, not a more manageable 400 or 40 or 4—close the gate quickly and walk away before someone sees them. ♦

OSLO IS DEAD

The Peace Process Is Over—Time to Save the Peace

By Charles Krauthammer

Young Palestinians throwing stones at Israeli soldiers. Israelis responding with tear gas and rubber bullets. Firebombs thrown at Israeli vehicles. Terrorist bombs going off in Tel Aviv.

As these scenes of murder and mayhem are endlessly replayed, we are told in solemn voiceover that the Middle East is back to the days of the intifada. Not quite. There is one large difference, hardly noticed and hardly mentioned. These Palestinians throwing stones and hurling firebombs are not living under occupation. The single most misunderstood fact about the Middle East today is that of the 2,300,000 Palestinians living in Gaza and the West Bank, 2,250,000 live under the rule of Yasser Arafat and the Palestinian Authority. Of the Palestinians who were formerly under Israeli rule, 98 percent now live under Palestinian rule.

Ten years ago, the world experienced an outpouring of sympathy and support for these stone-throwing youths because they were living under occupation. Well, they no longer are. They have long ago had their wild ceremonies celebrating their liberation from Israeli occupation. Nonetheless, the Western sympathy they enjoyed seems not to have abated.

Why exactly are these young men throwing stones and firebombs? Answer: Because they are unhappy with what is happening *outside* their liberated zones. Specifically, they are protesting Israel's building Jewish housing in East Jerusalem. They are also protesting Israel's latest territorial concession. The Jewish

state gave them only 9 percent of the relatively empty land remaining in the West Bank rather than the 30 percent Yasser Arafat says he is entitled to.

Thus the violence you see on your TV screen is not the work of an unjustly occupied people wanting to be free. It is the work of an already freed people trying to storm demarcation lines solemnly established by their own leadership to separate their territory from Israel's. Their aim is to attack Israeli soldiers and civilians on the Israeli side of the line as a way of protesting Israeli policies elsewhere. Were the Israeli soldiers not to fire back with tear gas and rubber bullets, these mobs would overrun the Israeli areas—in Hebron, for example—and no doubt kill and expel their Jewish inhabitants.

These are not Gandhi's Indians rising up against the Raj. The better analogy is Mexicans storming the border crossings at Tijuana, attacking American police and civilians with stones and firebombs to protest U.S. government actions in, say, Los Angeles.

It is important to understand that Palestinian violence is coming from a self-governing people. Otherwise, one cannot understand what the current turmoil is all about. Ten years ago, there was a great debate among Israelis whether or not to hold on, have the intifada, and rule the Palestinians. There was a great debate whether or not to annex the land the Palestinians lived on and create a Greater Israel. There was a great debate whether or not to grant the Palestinians the essentials of sovereignty over the places they inhabit.

Those debates are over. The Left won. Greater

Contributing editor Charles Krauthammer has won the Pulitzer Prize for his weekly newspaper column.

Raw porn skulks just a click away

75,000 sex sites put out e-mail feelers

By Tom Heinon
MEMPHIS JOURNAL SENTINEL

Timothy Muth and his children weren't on one of the information superhighway's sleazy side streets when the electronic equivalent of a trench-coated pornographer reached into their Delafield, Wis., home.

Three unsolicited e-mail messages offering such entitlements as "live sex" or "the hottest girls on the Internet" showed up on the family computer account in a recent two-day period.

What's more, the messages contained direct links to sex-oriented sites. Click on one of the highlighted words with a mouse and a child or an adult could be transported to a home page or other page with eye-popping images.

"It bothered me because my kids use that account to send e-mail back and forth to their friends," said Mr. Muth, who deleted the messages before his three children, all under the age of 13, were exposed to them. "My kids could have very easily clicked on this, and suddenly they're at a Web site for live Internet sex."

Mr. Muth, a Milwaukee lawyer whose practice includes Internet law, has contended that the U.S. government should encourage technology that allows parental control over sexually explicit material on the Internet without trying to regulate it directly across international borders.

But this was the first time he had encountered sex-oriented junk e-mail.

What a child could see by clicking on an e-mail message is difficult to say with certainty, partly because there are an estimated 72,000 pornographic World Wide Web sites on the Internet. Often a sample is offered before commercial sites require downloading of software and/or payment with a credit card number.

"Some of the stuff you click on depicts oral sex up close, and once you've seen it, the damage is done," said Michael Bradshaw, chief executive officer of Log-On Data Corp., whose X-Stop screening software blocks access to sex-oriented sites and can refer suspect e-mail messages for parental review.

Shyle Welch, a spokeswoman for Enough Is Enough, an anti-pornography group based in Fairfax, Va., agrees. "These people are not doing any screening as to whether this is an appropriate cus-

tomor or not. They are simply going to as many people as they can, hoping to draw in customers."

Some messages are specialized or ambiguous enough that a child might not know what to expect from the site, Miss Welch said. And even though many sites precede their content with a warning that it's intended only for people over 18, "a 14-year-old with raging hormones is going to click," she added.

Click on one e-mail message and there is an introduction that shouts, "FREE SEX SHOW LIVE FROM MOSCOW! NO CREDIT CARD NEEDED!!!!" There are color ads with small photos of bare-breasted women and a grainy, three-second video of a naked woman.

For more, viewers must dial a number in the former Soviet republic of Georgia and download photo files or software that enables them to see and send requests to live male and female "performers."

Another site uses identical graphics and includes a list of sexual poses and acts in its library of "way over 300,000 nasty hard-core erotic computer images."

Rep. Tom Barrett, Wisconsin Democrat, was contacted earlier this year by the family of a 14-year-old Wauwatosa, Wis., boy who racked up an \$1,800 long-distance telephone bill from AT&T by downloading software from an overseas sex site.

Mr. Barrett is co-sponsoring a bill introduced by Rep. Zoe Lofgren, California Democrat, that would require Internet service providers who don't already do so to offer parents optional software for blocking sexually explicit sites.

Regulating overseas Web sites is likely to be difficult. A major question for now is whether parents who are concerned about their children's potential exposure to sexually explicit material can rely on screening and blocking software. Many programs that filter for key words also can block offensive sites that deal with topics such as health and medicine. New sex sites are added daily, so programs that block specific sites need to be updated frequently. And even established sites often send e-mail messages through third-party distributors that cloak their origins.

"There isn't a software I know of that is 100 percent effective," Miss Welch said. "We're telling parents you need to keep the computer in a public area of the house, and you need to monitor it."

Internet User Gets 2 Years For Having Sex With Girl

Parents of Another Alleged Target Decry Term

By Brooke A. Masters
Washington Post Staff Writer

In what prosecutors called one of the most serious cases brought by an FBI task force targeting pedophiles who use the Internet, a Rockville computer consultant who contacted more than 100 young girls online and had sex with a 14-year-old was sentenced yesterday to two years in prison.

The parents of one of Donald M. Lytle's alleged targets—a 12-year-old Fairfax girl whom Lytle had arranged to meet at a library—said they were outraged that Lytle didn't get more prison time. But U.S. District Judge Claude M. Hilton said it was the maximum he could legally impose under federal sentencing guidelines. Lytle, 64, had no prior record before he pleaded guilty in July to two counts of crossing state lines to engage in sex with a minor.

Assistant U.S. Attorney Robert A.

Spencer had asked Hilton to make a rare upward departure from the guidelines because Lytle, unlike most people caught by the Innocent Images task force, actually had sex with a minor, and he admitted that he made sexual advances to his stepdaughter and a teenage babysitter nearly 20 years ago.

Lytle's attorney, Jonathan Shapiro, urged Hilton to go easy on the self-employed consultant because he is receiving psychiatric treatment and did not have sexual contact with minors for nearly 20 years between the incident with his stepdaughter and his online activity.

Hilton rejected defense pleas for leniency and ruled he didn't have the legal grounds to give Lytle more than 24 months in prison, although he also imposed three years of probation and a \$4,000 fine.

"They did not give him enough of
See SENTENCE, B5, Col. 4

Internet User Gets 2 Years for Having Sex With Girl

SENTENCE, From B1

a sentence," said the father of the 12-year-old Fairfax girl whom prosecutors said Lytle arranged to meet for sex in the Burke public library. The girl's mother, who was in the library for another meeting, prevented the liaison when she saw her daughter with a much older man, according to court documents filed in Alexandria.

"I don't know if these treatments really work. After 20 years of not doing it, he started again," the mother said. "It's too bad he's going to be out fairly soon."

After the Fairfax parents notified

authorities about their daughter's contact with Lytle, the multi-jurisdictional task force launched an online sting. The work of the task force, an outgrowth of the investigation of the 1993 disappearance of George "Junior" Barynski, a 10-year-old Prince George's County boy, has led to the conviction of 153 people, but in most cases the contact with children occurred entirely online.

Arlington Detective Paul Reid and FBI Special Agent John Meisica ran the investigation of Lytle, in which investigators pretended to be a 13-year-old and arranged to meet Lytle in an Arlington park in February, according to court documents.

Lytle was arrested, and further investigation determined that he had contacted more than 100 girls through computer chat rooms, traveled to New Jersey and Atlanta to meet youngsters, and had sex with a 14-year-old Georgia girl, court documents said.

"We're getting more and more of these traveler cases where the guys want to meet the girl," Reid said. "We need to change the statute. People getting charged with possessing child pornography are getting more [prison] time than these people."

Under Lytle's plea bargain, he still could be prosecuted for statutory rape in Georgia, prosecutors said.

1ST STORY of Level 1 printed in FULL format.

Copyright 1997 The New York Times Company
The New York Times

October 12, 1997, Sunday, Late Edition - Final

SECTION: Section 14LI; Page 1; Column 4; Long Island Weekly Desk

LENGTH: 1472 words

HEADLINE: A Look at Perils The Internet Poses to Children

BYLINE: By JOHN RATHER

BODY:

WHEN Carol Ellison, a senior editor at Home PC Magazines in Manhasset, entered a computer chat room and posed as a 14-year-old, she received what she called "a fair number of interesting overtures."

"It was a bit of an eye opener," Ms. Ellison said. "Peopls were asking my measurements and that sort of thing. And I was only on for four hours."

What occurs among strangers in chat rooms and what children can find on what some people have said are 10,000 pornographic sites on the World Wide Web are concerns on Long Island. The region's high family incomes and education levels, coupled with an emphasis in schools on computer literacy, assures the presence of tens of thousands of powerful home computers.

In many cases, experts say, children in those homes are more adept and frequent computer users than their parents.

Long Island authorities and computer experts said there was an urgent need for parents to catch up and regain control. They have recommended frank discussions, guidelines, filtering programs and training to show parents how to trace children's steps in cyberspace.

Last month a convicted pedophile, Stephen P. Simmons of Holbrook, was arrested after having been accused of luring a 14-year-old from New Jersey into sexual encounters after exchanges with the boy in a chat room on America Online that focused on homosexuals.

The case was publicized when the boy, now 15, was arrested in the case of an 11-year-old neighbor who was sexually assaulted and strangled to death as he was selling candy door to door for a P.T.A. fund-raising drive in Jackson.

District Attorney James M. Catterton Jr. of Suffolk County then announced plans for a panel to increase parental awareness of children's use of computers and the Internet. Mr. Catterton said the Internet was "a wonderful repository of information," but that it was also "a city with no cops, and no traffic signals or controls."

Advocates of free speech and other civil libertarians have vigorously opposed government actions to regulate the Internet. In June the United States Supreme

Court declared unconstitutional a 1996 Federal law that made it a crime to post indecent material on line that could reach children.

"A task force is a great idea, particularly if it goes toward more public education of parents," said Ann Beeson, a lawyer for the American Civil Liberties Union in New York City. "But what is not needed is new laws. There are laws on the books in all 50 states and Federal law that makes it a criminal offense to lure an adolescent. It is just not accurate to say there are no cops on the Internet. Law enforcement is very busy patrolling. They are present in a lot of chat rooms."

Last month State Attorney General Dennis C. Vacco announced that his office had identified more than 1,500 traffickers in illegal pornography on computers worldwide. His 18-month Federal-state investigation resulted in 34 arrests in New York, as well as additional scores in other states and countries, Mr. Vacco's office said.

The 15-year-old suspect in New Jersey, Sam Manzie, had been assisting the police in Suffolk and Monmouth Counties in investigating Mr. Simmons, but three days before the attack Mr. Manzie smashed tracking equipment that the authorities had installed on his home computer.

Because Mr. Simmons' previous arrests for sexual misconduct involving children predated the New York version of the so-called Megan's law, neighbors in the neighborhood where he had lived for years with another gay man were unaware of his past. Some neighbors said Mr. Simmons had done nothing to raise suspicions in a neighborhood with young children.

Some neighbors said they were not aware that Mr. Simmons took the boy home in August 1996 for sex.

Authorities said pedophiles relied on chat rooms and newsgroups to stalk children, sometimes initially posing as children themselves. "They go into the public chat rooms to select a target, and when they find a likely prospect they will invite him into a private chat room," said Detective Sgt. Robert J. Haack, who heads computer crime investigations for the police in Suffolk.

In private chat rooms, where outsiders are excluded, a pedophile strikes up a sympathetic relationship, often eliciting personal information and lending a sympathetic ear. "It is a process of seduction," said Kenneth Wooden of Child Lursa Ltd. of Shelburne, Vt.

Mr. Wooden, an expert on preventing the sexual assault and abduction of children, said pedophiles used the same techniques on-line that they would to lure a child from a playground.

"Predators have told me when they go to a playground they can spot their prey 200 yards away," he added. "They look for a loner. On the Internet they look for a child alone."

Mr. Wooden said predators often revealed themselves by inquiring how children were getting along with their parents or how their parents were getting along with each other.

"This is the crowbar question," Mr. Wooden said. "Pedophiles know that

The New York Times, October 12, 1997

teen-agers and parents have normal conflict and difficulties and that the kid is pulling away. That is why it is crucial for children to understand they should never talk about how the family is getting along to a stranger on the Internet."

"Parents have to become more sophisticated," Detective Sergeant Haack said. "Any time there is an opportunity for a predator to target an individual you need to take some precautions. People who go on the Internet need to keep their guard up. The people they are conversing with may not be the people they portray themselves to be."

The president of the Long Island chapter of Webgrrls, Alison Berks of Great Neck, said she advised staying away from chat rooms. "I tell people, 'Please don't go to the chat rooms,'" Ms. Berks said. "You get the most unbelievable messages in there. People approach you all the time as if they know you, and they are complete strangers."

Webgrrle, an international group that helps teach women to use the Internet, is among several groups and businesses that say they have training and software to enable parents to protect their children, and even themselves, from the worst of the Internet.

The group, which uses a double "r" because a computer search using an "i" accessed a pornographic site, offers low-cost classes.

Ms. Berks said one easily learned method let parents view sites that their children had visited. Browsers, the programs that access and read Web pages, kept the records of sites accessed, she said.

"We will teach you, even if you don't know a thing about the Internet," said Dolly Nielsen of Valley Stream, a member of Webgrrls and the owner of a public relations company.

Ms. Nielsen said that Internet users could learn how to access so-called remailers, a technique used to hide the source of messages and that could help them prevent being inundated by junk e-mail. Such spam mail involves mass postings to offer products, and, in some cases, pornography.

Ms. Ellison of Home PC, published by CMP Media, said her spam mail regularly had offers of pornographic material. "I find it terribly offensive," she said. "There will be '800' numbers for hot talk and offers to visit such and such a site for nude photos. The people who send this out have no idea who I am or how old I am. I'm just an e-mail address."

Ms. Ellison, who posed as a 14-year-old in connection with an appearance on "Oprah," said she had heard alarming accounts from children in a testing laboratory that her magazine had organized, recalling: "All of the kids said they had some experiences on line that were questionable. In the vast majority of cases it was that they received e-mail with links to pornographic sites."

Software manufacturers on Long Island say they are paying increasing attention to such problems. Two weeks ago Eshare Technologies of Commack held a seminar, "Stomping Out Cyber-Smut," on "safety, security and wholesomeness on the Internet."

The New York Times, October 12, 1997

Page 6

Bascom Global Internet Services of Farmingdale offers schools a list of Internet sites that educators have approved. The list deletes pornographic and similar sites, but lets officials override the exclusions.

The company president, Peter Cirasola, said Bascom was developing services to make it easier to block material without installing filters. Such programs, Mr. Cirasola added, could be eventually offered by Internet service providers.

Software that blocks objectionable material is already available. Some service providers, including America Online, offer limited blocking services.

Some experts say many parents have neither the time nor the skills to install filters. Even when such programs are installed, they said, skilled children may find a way to disable it. Mr. Cirasola said, "You have to give the parents the tools, but you don't make the decisions for them."

LANGUAGE: ENGLISH

LOAD-DATE: October 12, 1997

○

