

**SEXUAL EXPLOITATION OF CHILDREN  
OVER THE INTERNET: WHAT PARENTS,  
KIDS AND CONGRESS NEED TO KNOW  
ABOUT CHILD PREDATORS**

---

---

**HEARINGS**

BEFORE THE

**SUBCOMMITTEE ON OVERSIGHT AND  
INVESTIGATIONS**

OF THE

**COMMITTEE ON ENERGY AND  
COMMERCE**

**HOUSE OF REPRESENTATIVES**

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

---

APRIL 4, APRIL 6, AND MAY 3, 2006

---

**Serial No. 109-126**

---

Printed for the use of the Committee on Energy and Commerce



Available via the World Wide Web: <http://www.access.gpo.gov/congress/house>

---

U.S. GOVERNMENT PRINTING OFFICE

30-793PDF

WASHINGTON : 2006

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas	JOHN D. DINGELL, Michigan
MICHAEL BILIRAKIS, Florida	<i>Ranking Member</i>
<i>Vice Chairman</i>	HENRY A. WAXMAN, California
FRED UPTON, Michigan	EDWARD J. MARKEY, Massachusetts
CLIFF STEARNS, Florida	RICK BOUCHER, Virginia
PAUL E. GILLMOR, Ohio	EDOLPHUS TOWNS, New York
NATHAN DEAL, Georgia	FRANK PALLONE, JR., New Jersey
ED WHITFIELD, Kentucky	SHERROD BROWN, Ohio
CHARLIE NORWOOD, Georgia	BART GORDON, Tennessee
BARBARA CUBIN, Wyoming	BOBBY L. RUSH, Illinois
JOHN SHIMKUS, Illinois	ANNA G. ESHOO, California
HEATHER WILSON, New Mexico	BART STUPAK, Michigan
JOHN B. SHADEGG, Arizona	ELIOT L. ENGEL, New York
CHARLES W. "CHIP" PICKERING, Mississippi	ALBERT R. WYNN, Maryland
<i>Vice Chairman</i>	GENE GREEN, Texas
VITO FOSSELLA, New York	TED STRICKLAND, Ohio
ROY BLUNT, Missouri	DIANA DEGETTE, Colorado
STEVE BUYER, Indiana	LOIS CAPPS, California
GEORGE RADANOVICH, California	MIKE DOYLE, Pennsylvania
CHARLES F. BASS, New Hampshire	TOM ALLEN, Maine
JOSEPH R. PITTS, Pennsylvania	JIM DAVIS, Florida
MARY BONO, California	JAN SCHAKOWSKY, Illinois
GREG WALDEN, Oregon	HILDA L. SOLIS, California
LEE TERRY, Nebraska	CHARLES A. GONZALEZ, Texas
MIKE FERGUSON, New Jersey	JAY INSLEE, Washington
MIKE ROGERS, Michigan	TAMMY BALDWIN, Wisconsin
C.L. "BUTCH" OTTER, Idaho	MIKE ROSS, Arkansas
SUE MYRICK, North Carolina	
JOHN SULLIVAN, Oklahoma	
TIM MURPHY, Pennsylvania	
MICHAEL C. BURGESS, Texas	
MARSHA BLACKBURN, Tennessee	

BUD ALBRIGHT, *Staff Director*

DAVID CAVICKE, *General Counsel*

REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

ED WHITFIELD, Kentucky, *Chairman*

CLIFF STEARNS, Florida	BART STUPAK, Michigan
CHARLES W. "CHIP" PICKERING, Mississippi	<i>Ranking Member</i>
CHARLES F. BASS, New Hampshire	DIANA DEGETTE, Colorado
GREG WALDEN, Oregon	JAN SCHAKOWSKY, Illinois
MIKE FERGUSON, New Jersey	JAY INSLEE, Washington
MICHAEL C. BURGESS, Texas	TAMMY BALDWIN, Wisconsin
MARSHA BLACKBURN, Tennessee	HENRY A. WAXMAN, California
JOE BARTON, Texas	JOHN D. DINGELL, Michigan
<i>(EX OFFICIO)</i>	<i>(EX OFFICIO)</i>

# CONTENTS

	Page
Hearings held:	
April 4, 2006.....	1
April 6, 2006.....	238
May 3, 2006.....	423
Testimony of:	
Cooper, Sharon W., Developmental and Forensic Pediatrics, PA, Department of Pediatrics, University of North Carolina Chapel Hill.....	17
Berry, Justin.....	75
Eichenwald, Kurt, Reporter, The New York Times.....	85
Allen, Ernie, President and Chief Executive Officer, National Center for Missing and Exploited Children.....	126
Aftab, Parry, Executive Director, WiredSafety.....	144
Schroeder, Teri L., President/Program Director, i-SAFE America.....	187
Sullivan, Shannon, Teen Angel, WiredSafety.....	201
Mercer, William W., United States Attorney for the District of Montana; Principal Associate Deputy Attorney General, United States Department of Justice.....	256
Swecker, Chris, Acting Assistant Executive Director, Federal Bureau of Investigation, United States Department of Justice.....	268
Kardasz, Dr. Frank, Sergeant, Phoenix Police Department; Project Director, Arizona Internet Crimes Against Children Task Force, United States Department of Justice...	275
Waters, Flint, Lead Special Agent, Wyoming Division of Criminal Investigation, Internet Crimes Against Children Task Force Technology Center, United States Department of Justice.....	285
Clark, John P., Deputy Assistant Secretary, United States Immigration and Customs Enforcement, United States Department of Homeland Security.....	290
Kezer, William E., Deputy Chief Inspector, United States Postal Inspection Service.....	295
Weeks, Grier, Executive Director, National Association to Protect Children.....	347
Allen, Masha.....	444
Grace, Nancy, CNN Nancy Grace.....	449
Fisher, Hon. Alice S., Assistant Attorney General, Criminal Division, United States Department of Justice.....	470
Roldan, Raul, Section Chief, Cyber Crime Section, Cyber Division, Federal Bureau of Investigation, United States Department of Justice.....	487
Additional material submitted for the record:	
Kezer, William E., Deputy Chief Inspector, United States Postal Inspection Service, response for the record.....	409
Waters, Flint, Lead Special Agent, Wyoming Division of Criminal Investigation, Internet Crimes Against Children Task Force Technology Center, United States Department of Justice, response for the record.....	411
Swecker, Chris, Acting Assistant Executive Director, Federal Bureau of Investigation, United States Department of Justice, response for the record.....	412
Kardasz, Dr. Frank, Sergeant, Phoenix Police Department; Project Director, Arizona Internet Crimes Against Children Task Force, United States Department of Justice, response for the record.....	417
Plitt, James, Director, Cyber Crimes Center, Office of Investigations, United States Immigration and Customs Enforcement, United States Department of Homeland Security, response for the record.....	421
Weeks, Grier, Executive Director, National Association to Protect Children, response for the record.....	422
Fisher, Hon. Alice S., Assistant Attorney General, Criminal Division, United States Department of Justice, response for the record.....	582
Marsh, James R., Esq., response for the record.....	585
Allen, Faith, response for the record.....	616
Roldan, Raul, Section Chief, Cyber Crime Section, Cyber Division, Federal Bureau of Investigation, United States Department of Justice, response for the record.....	618



# **SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET: WHAT PARENTS, KIDS AND CONGRESS NEED TO KNOW ABOUT CHILD PREDATORS**

**TUESDAY, APRIL 4, 2006**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ENERGY AND COMMERCE,  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,  
*Washington, DC.*

The committee met, pursuant to notice, at 10:06 a.m., in Room 2123 of the Rayburn House Office Building, Hon. Ed Whitfield (Chairman) presiding.

Members present: Representatives Walden, Ferguson, Burgess, Blackburn, Barton (ex officio), Whitfield, and Stupak.

Staff present: Mark Paoletta, Chief Counsel for Oversight and Investigations; Alan Slobodin, Deputy Chief Counsel for Oversight and Investigations; Kelli Andrews, Counsel; Karen Christian, Counsel; Michael Abraham, Legislative Clerk; Edith Holleman, Minority Counsel; and David Nelson, Minority Investigator/Economist.

MR. WHITFIELD. I would like to call this hearing to order. Today's subject of our hearing is "Sexual Exploitation of Children Over the Internet: What Parents, Kids and Congress Need to Know About Child Predators."

Today, we are going to have five panels of witnesses on this very important subject matter. The first panel which we will introduce a little bit later, will be Sharon Cooper who is with the Developmental and Forensic Pediatrics for the Department of Pediatrics at the University of North Carolina Chapel Hill.

I welcome all of you here today and this will be the first of several hearings on issues relating to the sexual exploitation of children over the Internet. Today's hearing aims to protect our children's--if you will excuse me one minute. May I have a glass of water? Today's hearing aims to protect our Nation's children by putting a spotlight on how parents and children can better educate themselves on the dangers of child predators on the Internet.

In the early 1990s, before the advent of the Internet, it seemed in the United States that commercial child pornography was on the decline. This was due to several factors, especially several U.S. Supreme Court

decisions that removed any first amendment protection for the possession or distribution of child pornography. These decisions were coupled with aggressive law enforcement efforts primarily targeting the U.S. mail system, which was the means of transporting these images. Unfortunately, the Internet reversed this trend.

With the growing use of the Internet, the number of child predators who seek to make, distribute, and view images of children being sexually abused continues to skyrocket. This is due to the anonymity, accessibility, and ease with which child predators can operate on the Internet. The extent of the problem is staggering. Some examples of statistics that our witnesses today at the hearing will discuss more fully include: one in five children report being sexually solicited over the Internet and only 25 percent of those children that are sexually solicited online tell their parents; 3.5 million images of child sexual exploitation over the Internet have been identified in the United States alone. The commercial enterprise of online child pornography is estimated in 2005 to be approximately \$20 billion, and it is an industry on the rise. The National Center for Missing and Exploited Children receives approximately 1,500 tips a week on its cyber tip line about suspected online child pornography. Child predators that are found in possession of child pornography typically have thousands of images of sexual abuse of children on their computers.

In my own State of Kentucky, a man was arrested last month and, according to a press release, agents from the immigration and customs enforcement reportedly discovered over 400,000 images of child pornography on his computers. Thinking about the number of children that were abused in order to create all of those images is sickening and intolerable. We must do everything possible to stop it.

I want to particularly thank all of our witnesses today for appearing before the subcommittee. We appreciate your taking the time to speak to us about an important issue concerning our most vulnerable citizens, and that is our children. You will hear today from a young man named Justin Berry and he will tell a story about his experience in this horrible world of online child exploitation. He will also talk to us about how he received a free webcam and was preyed upon and exploited by child predators. I believe Mr. Berry is brave to come forward and speak publicly to this subcommittee about matters that are very personal to him and painful for him to even talk about. Justin, we appreciate your willingness to share your experiences with us, as well as, with parents and children around the country who may learn some valuable lessons from your story.

We will also hear from Mr. Kurt Eichenwald, who as a New York Times reporter exposed this world that captures children like Justin. Mr.

Eichenwald feels so strongly about the dangers he has uncovered that he has taken the extraordinary step to come to testify about how readily available this material is over the Internet. He will provide a firsthand account of how predators lure and manipulate children over the Internet.

In addition, I would like to thank Dr. Sharon Cooper who as I said, is on the first panel. She altered her travel plans for a trip to Germany in order to be here and testify today. I believe your testimony will be invaluable in helping us understand what happens to children like Justin who fall victim to these predators and what the modus operandi of these predators are so parents and children can keep a watchful eye. We appreciate you making a special effort to be here.

Today we will also here testimony from Mr. Ernie Allen from the National Center for Missing and Exploited Children. Mr. Allen and his staff at the center have done a phenomenal job of working to keep children safe. We look forward to hearing about the Center's role as a clearinghouse for tips regarding child pornography over the Internet by way of their cyber tip line, as well as future plans they have to help stem the tide of child sexual exploitation over the Internet. I believe the one valuable lesson that can come out of this hearing is that parents, children, and of course Members of Congress become well versed in what the cyber tip line is and how and when to use it.

On our last panel, I am very happy to say, we have representatives from WiredSafety and i-SAFE America to tell us more about how they promote safety over the Internet for children. We are also interested in hearing first hand from your teenage witness, who is a Teen Angel from WiredSafety and an I Mentor for i-SAFE America, on how they communicate Internet safety to their peers.

I must note that we also have today a witness who was subpoenaed by the full committee to appear to testify. His name is Ken Gourlay from Michigan. We will hear more about why Mr. Gourlay is here through Justin's testimony. I have been advised that Mr. Gourlay intends to invoke his Fifth Amendment privilege against self-incrimination and will decline to answer the subcommittee's questions, but we are hopeful maybe he will decide to speak, because it is critical that we confront his explanation for his actions.

At Thursday's hearing, we are going to be focusing on the U.S. law enforcement's efforts devoted to eradicating the sexual exploitation of children over the Internet and learn more about the challenges facing law enforcement in this area.

[The prepared statement of Hon. Ed Whitfield follows:]

PREPARED STATEMENT OF THE HON. ED WHITFIELD, CHAIRMAN, SUBCOMMITTEE ON  
OVERSIGHT AND INVESTIGATIONS

GOOD MORNING.

TODAY THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS HOLDS THE FIRST OF SEVERAL HEARINGS ON ISSUES RELATING TO THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET. TODAY'S HEARING AIMS TO PROTECT OUR NATION'S CHILDREN BY PUTTING A SPOTLIGHT ON HOW PARENTS AND CHILDREN CAN BETTER EDUCATE THEMSELVES ABOUT THE DANGERS OF CHILD PREDATORS ON THE INTERNET.

IN SO DOING, WE WILL HEAR THE STORY ABOUT ONE CHILD'S EXPERIENCE IN THIS HORRIBLE WORLD OF ON-LINE CHILD EXPLOITATION. AND, WE WILL LEARN HOW THE INTERNET HAS FUELED THE HIGHLY LUCRATIVE BUSINESS OF SELLING SEXUALLY ABUSIVE IMAGES OF CHILDREN AROUND THE WORLD.

IN THE EARLY 1990'S, BEFORE THE ADVENT OF THE INTERNET, IT SEEMED IN THE UNITED STATES, COMMERCIAL CHILD PORNOGRAPHY WAS ON THE DECLINE. THIS WAS DUE TO SEVERAL FACTORS—ESPECIALLY SEVERAL U.S. SUPREME COURT DECISIONS THAT REMOVED ANY FIRST AMENDMENT PROTECTION FOR THE POSSESSION OR DISTRIBUTION OF CHILD PORNOGRAPHY. THESE DECISIONS WERE COUPLED WITH AGGRESSIVE LAW ENFORCEMENT EFFORTS PRIMARILY TARGETING THE U.S. MAIL SYSTEM, WHICH WAS THE MEANS OF TRANSPORTING THESE IMAGES. UNFORTUNATELY, THE INTERNET REVERSED THIS TREND.

WITH THE GROWING USE OF THE INTERNET, THE NUMBER OF CHILD PREDATORS WHO SEEK TO MAKE, DISTRIBUTE AND VIEW IMAGES OF CHILDREN BEING SEXUALLY ABUSED CONTINUES TO SKYROCKET. THIS IS PRIMARILY DUE TO THE ANONYMITY, ACCESSIBILITY AND EASE WITH WHICH THESE CHILD PREDATORS CAN OPERATE ON THE INTERNET.

THE EXTENT OF THE PROBLEM IS STAGGERING. HERE ARE SOME EXAMPLES OF STATISTICS THAT OUR WITNESSES AT THE HEARING WILL DISCUSS MORE FULLY:

- 1 IN 5 CHILDREN REPORT BEING SEXUALLY SOLICITED OVER THE INTERNET. AND ONLY 25% OF THOSE CHILDREN THAT ARE SEXUALLY SOLICITED ON-LINE TELL THEIR PARENTS.
- 3.5 MILLION IMAGES OF CHILD SEXUAL EXPLOITATION OVER THE INTERNET HAVE BEEN IDENTIFIED—IN THE UNITED STATES ALONE.
- THE COMMERCIAL ENTERPRISE OF ON-LINE CHILD PORNOGRAPHY IS ESTIMATED, IN 2005, TO BE APPROXIMATELY \$20 BILLION U.S. DOLLARS. IT IS AN INDUSTRY ON THE RISE.
- THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN GETS APPROXIMATELY 1,500 TIPS A WEEK ON ITS CYBERTIPLINE ABOUT SUSPECTED ON-LINE CHILD PORNOGRAPHY.
- CHILD PREDATORS THAT ARE FOUND IN POSSESSION OF CHILD PORNOGRAPHY TYPICALLY HAVE THOUSANDS OF IMAGES OF SEXUAL ABUSE OF CHILDREN ON THEIR COMPUTERS.
- IN MY HOME STATE OF KENTUCKY, A MAN WAS ARRESTED LAST MONTH AND, ACCORDING TO A PRESS RELEASE, AGENTS FROM THE IMMIGRATION AND CUSTOMS ENFORCEMENT REPORTEDLY



DISCOVERED OVER 400 THOUSAND IMAGES OF CHILD PORNOGRAPHY IN HIS COMPUTERS.

THINKING ABOUT THE NUMBER OF CHILDREN THAT WERE ABUSED IN ORDER TO CREATE ALL OF THOSE IMAGES IS SICKENING AND INTOLERABLE.

THIS MUST BE STOPPED.

TODAY WE WILL HEAR FROM SEVERAL PANELS OF WITNESSES WHO WILL HELP US CONFRONT THESE UNSETTLING FACTS AND PROVIDE INFORMATION ABOUT WHAT WE CAN DO ABOUT IT. I WANT TO THANK ALL OF THE WITNESSES APPEARING BEFORE THE SUBCOMMITTEE TODAY. WE APPRECIATE YOUR TAKING THE TIME TO SPEAK TO US ABOUT SUCH AN IMPORTANT ISSUE CONCERNING OUR MOST VULNERABLE CITIZENS—OUR CHILDREN.

WE WILL HEAR TODAY FROM MR. JUSTIN BERRY. MR. BERRY WILL TELL US HIS ALARMING STORY ABOUT HOW A 13 YEAR OLD GETS A FREE WEBCAM AND IS PREYED UPON AND EXPLOITED BY CHILD PREDATORS. I BELIEVE MR. BERRY IS EXTREMELY BRAVE TO COME FORWARD AND SPEAK PUBLICLY TO THIS SUBCOMMITTEE ABOUT MATTERS THAT ARE VERY PERSONAL TO HIM AND PAINFUL FOR HIM TO TALK ABOUT.

WE APPRECIATE YOUR WILLINGNESS, JUSTIN, TO SHARE YOUR EXPERIENCE WITH US—AS WELL AS WITH PARENTS AND KIDS AROUND THE COUNTRY WHO MAY LEARN SOME LESSONS FROM YOUR STORY.

WE WILL ALSO HEAR FROM MR. KURT EICHENWALD, WHO, AS A NEW YORK TIMES REPORTER, EXPOSED THIS WORLD THAT CAPTURES CHILDREN LIKE JUSTIN. MR. EICHENWALD FEELS SO STRONGLY ABOUT THE DANGERS HE HAS UNCOVERED THAT HE HAS TAKEN THE EXTRAORDINARY STEP TO COME TO TESTIFY ABOUT HOW READILY AVAILABLE THIS DISGUSTING MATERIAL IS OVER THE INTERNET. HE WILL PROVIDE A FIRST HAND ACCOUNT OF HOW THESE PREDATORS LURE AND MANIPULATE CHILDREN OVER THE INTERNET.

IN ADDITION, I WOULD LIKE TO THANK DR. SHARON COOPER, WHO WILL APPEAR ON THE FIRST PANEL, FOR ALTERING HER TRAVEL PLANS TO GERMANY IN ORDER TO BE ABLE TO TESTIFY TODAY. I BELIEVE YOUR TESTIMONY WILL BE INVALUABLE IN HELPING US UNDERSTAND WHAT HAPPENS TO CHILDREN LIKE JUSTIN WHO FALL VICTIM TO THESE PREDATORS AND WHAT THE MODUS OPERANDI OF THESE PREDATORS ARE—SO PARENTS AND KIDS CAN KEEP A WATCHFUL EYE.

TODAY WE WILL ALSO HEAR TESTIMONY FROM MR. ERNIE ALLEN, FROM THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN. MR. ALLEN AND HIS STAFF AT THE CENTER HAVE DONE A PHENOMENAL JOB WORKING TO KEEP OUR CHILDREN SAFE. THE CENTER HAS BEEN ENORMOUSLY HELPFUL TO COMMITTEE STAFF ON MANY ISSUES RELATED TO THIS INVESTIGATION AND WE CAN'T THANK THEM ENOUGH. I LOOK FORWARD TO HEARING ABOUT THE CENTER'S ROLE AS A CLEARINGHOUSE FOR TIPS REGARDING CHILD PORNOGRAPHY OVER THE INTERNET VIA THEIR CYBERTIPLINE -- AS WELL AS FUTURE PLANS THEY HAVE TO HELP STEM THE TIDE OF CHILD SEXUAL EXPLOITATION OVER THE INTERNET.

I BELIEVE ONE VALUABLE LESSON THAT CAN COME OUT OF THIS HEARING IS THAT PARENTS, KIDS AND OF COURSE MEMBERS OF CONGRESS BECOME WELL VERSED IN WHAT THE CYBERTIPLINE IS --AND HOW AND WHEN TO USE IT.

ON OUR LAST PANEL, I AM VERY GLAD TO HAVE REPRESENTATIVES FROM WIRED SAFETY AND I SAFE AMERICA TO TELL US MORE ABOUT HOW THEY PROMOTE SAFETY OVER THE INTERNET FOR CHILDREN. WE ARE ALSO INTERESTED IN HEARING FIRST HAND FROM YOUR TEENAGE WITNESSES—A TEEN ANGEL FROM WIRED SAFETY AND AN I-MENTOR FROM I SAFE AMERICA—ON HOW THEY COMMUNICATE INTERNET SAFETY TO THEIR PEERS.

I MUST NOTE THAT WE ALSO HAVE TODAY A WITNESS WHO WAS SUBPOENED BY THE FULL COMMITTEE TO APPEAR TO TESTIFY. HIS NAME IS KEN GOURLAY FROM MICHIGAN. WE WILL HEAR MORE ABOUT WHY MR. GOURLAY IS HERE THROUGH JUSTIN'S TESTIMONY. I HAVE BEEN ADVISED THAT MR. GOURLAY INTENDS TO INVOKE HIS FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION AND WILL DECLINE TO ANSWER THE SUBCOMMITTEE'S QUESTIONS. YET I AM HOPEFUL HE WILL DECIDE TO SPEAK, BECAUSE IT IS CRITICAL THAT WE CONFRONT HIS EXPLANATION FOR HIS ACTIONS.

WE HAVE A LOT OF GROUND TO COVER. LET ME KNOTE THAT, AT THURSDAY'S HEARING, WE WILL FOCUS ON THE U.S. LAW ENFORCEMENT EFFORTS DEVOTED TO ERADICATING THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET AND LEARN MORE ABOUT THE CHALLENGES FACING OUR LAW ENFORCEMENT EFFORT IN THIS AREA.

I NOW TURN TO THE RANKING MEMBER, MR. STUPAK FOR HIS OPENING STATEMENT.

MR. WHITFIELD. I now turn to the Ranking Member of the subcommittee, Mr. Stupak of Michigan, for his opening statement.

MR. STUPAK. Thank you, Mr. Chairman and thank you for holding this hearing.

This investigation is certainly among the most important conducted by the Oversight and Investigations Subcommittee. I feel most Americans have no idea of the dimension of the problem. Because of the anonymity provided by the Internet and because of the marketing potential of the Internet, children that are being exploited, manipulated, and violated and whose lives and images of the predatory practice are digitized, displayed, and transmitted instantly around the world in astonishing numbers.

The statistics as you said, Mr. Chairman, are shocking. One in five children report receiving a sexual solicitation over the Internet. Today there are over 3.5 pornographic images of American children in circulation on the Internet. The sale of these images over the Internet brought in \$20 billion to traffickers in 2004. To compare, music sales over the same period were just \$3 billion. This \$20 billion was spent to view photographs and videos of children being raped and tortured. Since 2004, the child exploitation industry has only grown. The images have become more graphic as video capabilities have expanded and the content of those videos have become more heinous.

Who are these children that are solicited and abused? It is the little children who make up the vast majority of the victims of child

pornography. Over 90 percent of arrested children pornographers possess images of children under age 12. Forty percent have pictures or videos of children under the age of six, and almost 20 percent possess images of children less than three years of age. A couple of weeks ago, the Attorney General announced a Customs bust that involved among other crimes the portrayal of a rape of an 18 month old girl.

Who produced this most sickening material? The National Center for Missing and Exploited Children will tell us that 80 percent of all child pornography is produced by parents, other relatives, or family members. Every American parent should know what we will hear today. Parents need to learn and teach their children tools to protect themselves against these predators. Hopefully, today's hearing will reduce the unmonitored use of web cameras, picture phones, and other equipment that enable these people to prey on and abuse our children.

Today we will also hear the tragic story of Justin Berry. It is a story of the seduction and sexual abuse of a 13-year-old boy who was led on a pornographic exploitation, multiple molestations, and drug use, all of which were a constant reality in his life for 5 years. We will learn how adults, as well as Justin himself made money from Justin's online performances. One of the accused molesters is under subpoena to appear before us today and he will I understand he will evoke his Fifth Amendment right not to testify. Justin Berry could have a very different life had there been no Internet connection in his room. The chat rooms which are a magnet where these twisted minds can congregate and exploit our children. Unfortunately, just as the Internet has changed just about every aspect of our lives, it has also virtually eliminated the barriers that once discouraged child pornography.

The National Center for Missing and Exploited Children and similar crime operations at the International Customs Enforcement and the FBI do wonderful work with a handful of agents and tech specialists. We will hear about their efforts at a hearing we have scheduled for Thursday. Still our law enforcement can do better. Justin believes that there has been an ineffective response by the Justice Department to prosecute the persons who paid to watch his websites. Questions have been raised about the low number of prosecutions in the United States. For example, in one of the larger busts involving effective work for law enforcement in the U.S., Australia, and other countries, there is confirmed information that 21,000 Americans had paid to subscribe to websites that saved images of the sexual exploitation of children. Nine hundred Australians were similarly identified. As of the end of this past year, some 338 convictions have been obtained in the U.S. while some 500 arrests or convictions or expected convictions have been made in Australia, a country with a legal system as protective of individual rights as ours. I

want to know why we conduct less than 2 percent of these voyeurs of child sexual violence while the Australian authorities can put away 55 percent. What I do know is that the lack of prosecution threatens all of our children to have over 20,000 of these criminals walking free amongst us with the knowledge that even when police identify them they are unlikely to be prosecuted only encourages further actions of exploitation.

I also know that as we reorganize our telecom industry which transmits images and messages so efficiently over the Internet, we should also hold those that make billions of dollars from the data of image transmission accountable to eliminate those images of sexually violated children; take the profit and communications away and the problem will shrink proportionately.

The bottom line is that the darkest side of the Internet can invade any American home. Given the shortage of resources for law enforcement to adequately protect our children and the lack of will by Internet providers to police themselves, parents and children must be vigilant.

With that, Mr. Chairman, I would yield back the balance of my time.

MR. WHITFIELD. Thank you, Mr. Stupak.

At this time, I recognize the Chairman of the Full Committee, Mr. Barton of Texas, for his opening statement.

CHAIRMAN BARTON. Thank you, Chairman Whitfield, for holding this hearing.

I have three grown children, two teenage stepchildren, three grandchildren, and an infant son who is seven months old. Of all the hearings that we have done in all the years that I have been on this committee and this subcommittee, which is over 20 years, I have never been more revolted in preparing for a hearing than in reading the materials I have had to read for this one. My mind simply cannot conceive of a parent exploiting their own children for profit for sexual purposes and I cannot conceive of anyone in this universe wanting to perform, or watch performed, sexual acts on an infant. I simply cannot comprehend that. Yet that is what we are here today to investigate.

Child pornography is apparently a multi-billion--my staff analysis says \$20 billion a year business. In spite of all the rhetoric, I will not say we are doing nothing, as that is not fair to our law enforcement agencies and all the groups here that are trying to help, but we are doing very little to counteract it and everyone agrees that it is a growing problem. What kind of society do we have if we cannot protect infants from sexual exploitation? One of the agency's material shows that almost half of the incidents of sexual exploitation of children are by family members. What kind of family is that? I just cannot understand it.

So, I believe this is one that you can expect the subcommittee and the full committee, if we need to, to do everything possible, and I mean

everything. Not just hold hearings, but if we need legislation, if we need to go to our Federal law enforcement agencies that have tended to not treat this as seriously as they should; whatever we need to do on a bipartisan basis, we are going to do. I think I am a tolerant person and I am appalled, I mean absolutely appalled at what is happening on the Internet with regards to sexual exploitation of the children of the United States, and the children of the world.

So I am very appreciative of the staff's work on both sides of the aisle, and very appreciative of Mr. Stupak and Mr. Whitfield's personal involvement. I am very, very supportive of doing whatever we can to really turn the tide on this.

And with that, Mr. Chairman, I ask that my formal statement be considered in the record and I yield back.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY  
AND COMMERCE

Thank you, Chairman Whitfield for holding this hearing on the sexual exploitation of children over the Internet. As Justice Brandeis wrote, "sunlight is said to be the best disinfectant." If there was ever a case for sunlight and disinfecting, it is the toxic world of online child pornography.

Child porn is a \$20 billion a year business, and it is growing daily on the Internet. The more you know about it, the more revolted you become.

There are accounts of children — some as young as eighteen months old— being raped on camera for profit. Less than a month ago, based on an investigation by agents from United States Immigration and Custom Enforcement and international law enforcement, 27 people in the United States and abroad were charged with trafficking in pornography. Among their alleged crimes were the production of live, pay-per-view molestations of children which were carried over the Internet by streaming video.

These are actions so repugnant that they are difficult for the mind to even acknowledge, much less grasp and consider.

With the ability to post and trade images anonymously over the Internet, current estimates indicate that there are three million images of child pornography on the Internet today. While law enforcement is working to tackle this epidemic of abuse, their resources are taxed as an endless supply of child pornography is pumped into the Internet by individuals around the globe.

No one wants to believe that predator's abuse and torture children and sell or swap the pictures of that abuse. We do not like to think that even though our children have been warned by about strangers, children are still logging onto the Internet and meeting strangers child predators and pedophiles. But according to one estimate, one in five children report that they have received a sexual solicitation over the Internet.

It is because this problem is so horrific that we need to know more about it. Our nation's parents, children, and educators need to know exactly what dangers are lurking on the Internet. They need to appreciate how serious this problem is so that they can prepare their children for what — or who — is waiting for them online.

One of our witnesses today, Justin Berry, will speak personally to the horrors of child sexual exploitation on the Internet and its impact on its victims. Justin's life is a terrible lesson to every parent and child in America. It began when Justin went online to meet and communicate with other children his age. Instead, he was greeted almost

immediately by child predators who, by pretending to be his friends, convinced him to engage in sexual acts. First it was through a webcam, and then it was in person. Again, at the encouragement of these predators, Justin turned these performances into an online pornography business. Justin, I want to thank you for appearing here today to tell your story. I know it must be painful to talk about your involvement in the pornography industry and the abuse you suffered. I hope that your story might prevent others from following your path or convince a victim to seek help.

With Justin today is New York Times Reporter Kurt Eichenwald, who, when researching an story on cyber fraud, found Justin's websites and eventually persuaded Justin to seek help. Justin credits Mr. Eichenwald as being the person who rescued him from the world of child pornography.

Today's testimony will shine a bright light on a business that has flourished in the dark corners of the Internet. I hope that what the public learns today will help children to recognize a child predator if they meet one online. Finally, by speaking frankly about the impact of child pornography on its victims, this hearing will make plain that parents, educators, law enforcement, and lawmakers must make every effort to protect our children and put an end to an industry that profits from the abuse and degradation of children.

I look forward to hearing from the witnesses and yield back the balance of my time.

MR. WHITFIELD. Thank you very much, Mr. Chairman. We appreciate your being here and the leadership you continue to provide on this issue and all of the opening statements will be a part of the record without objection.

At this time, I would recognize Dr. Burgess for his opening statement.

MR. BURGESS. Thank you, Mr. Chairman. I too will thank you and Chairman Barton for having this hearing. I will submit my formal remarks for the record.

I do not know that I have much to add to what has already been spoken, but a newspaper, not from my district but from a county just west of my district, Wise County, the Wise County Messenger, has in its March 26 edition a story about yet another case, a brother and sister linked in a child porn case and apparently the data is in the process of being collected by the Forth Worth Branch that investigates this type of crime. It just underscores how it is pervasive in every community. This is a very rural area that is being described here in this newspaper article and it is as Chairman Barton points out just absolutely unconscionable that this activity is taking place literally right within our own communities.

And I also want to thank Mr. Chairman for bringing to light some of the tools that are available for parents who do want to be proactive and protect their children and I think that is an invaluable part of the hearing and this service that we provide today.

So with that, I will yield back. Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you, Dr. Burgess.

At this time, I recognize Mr. Walden for his opening statement.

MR. WALDEN. Thank you very much, Mr. Chairman.

I concur with the comments of my colleagues about how disturbing this information is and about what is going on the Internet. As a father of a 15-year-old, soon to be 16, I think I share the concern that most parents across America indeed the world probably have about how awful this is. And I appreciate, Justin, your being here today and coming forward not only before this committee but also for your diligence in trying to work with the Department of Justice and all the frustration that you expressed in your testimony in that process. And I think for me as a member of this committee, how important it is to get this information on our record. I want to know what is going on at the Child Exploitation and Obscenity Section. And why they conducted themselves the way they did as certainly it has been alleged in your testimony and that of others.

I was just reading some remarks that Mr. Eichenwald gave at Marquette University just a few days ago and his detailed description about COS handled this case is extraordinarily disturbing. And for me as a member of this oversight committee, as Vice Chairman, I am going to be asking some tough questions later in the week when we have the Justice Department here. It strikes me as absolutely perverse in the justice system that in effect the victim who comes forward to not only identify a problem but help round up those who are perpetrating this disgusting and terrible crime against humanity that somehow the victim is treated as the perpetrator and the fact that there are lots of other kids out there you are trying to save from this problem on the Internet. They seem to be lost in time. And for me COS has a lot of explaining to do and our Department of Justice has a lot of explaining to do.

And I again, appreciate your courage in coming forward along with the others and Dr. Cooper, thank you for rearranging your schedule to be here, we are really looking forward to your comments.

Thank you, Mr. Chairman.

MR. WHITFIELD. Mr. Walden, I am delighted that you focused your opening statement on that point because all of us are a little bit puzzled by what is going on over at the Child Exploitive and Obscenity Section of the Justice Department. That is something that we hope to get into today and certainly on Thursday as well.

At this time, I recognize the gentlelady from Tennessee, Mrs. Blackburn, for her opening statement.

MRS. BLACKBURN. Thank you, Mr. Chairman.

I also want to join my colleagues in thanking you for holding the hearing today. I want to thank our witnesses also for making the effort to be here. And I also want to thank our staffs and the committee staff for their diligence and their work on this issue. This is not an easy issue and

it is a very unpleasant issue digging through, reading the material, and we thank you all for your cooperation in submitting that.

Online child pornography is something that is increasingly used as an avenue by those that are child predators and that seek to do our children harm and exploit innocent, precious, precious children. Just the fact that there are millions of images that are transmitted daily, videos that are transmitted daily, on these acts that are being done to these children and transmitted over the Internet. And as our Chairman said, the fee for that is a \$20 billion a year industry. That is sickening to my soul, absolutely sickening. And parents and children do need to be aware of the dangers that exist on the Internet and they do need to be aware of the mechanisms that they can use to report these instances where adults may be trying to seduce children and to move these precious vulnerable children into dangerous situations.

And I do hope, Mr. Chairman, that we are able to correct some of the problems and look at some of the avenues of getting information to parents. Law enforcement also has got to be diligent and they have got to be prepared to shut down this despicable industry because there is no justifiable reason for this repulsive action of child pornography. It is horrible. It is a detestable mark on our society. And it is with sadness that we have to admit there are such sick and revolting people that walk on the face of this earth that they would want to watch, to copy, and to sell this type information to others.

I am looking forward to what we are going to hear today. Again, I thank you all for taking your time to be here and to work with us and work with families to be certain that law enforcement and us, each of us that we are doing what we need to do to address the issue.

Thank you, Mr. Chairman. I yield back.

MR. WHITFIELD. Thank you, Mrs. Blackburn.

At this time, I recognize the gentleman from New Jersey, Mr. Ferguson.

MR. FERGUSON. Thank you, Mr. Chairman.

I want to echo your comments and that of Mr. Stupak and our other colleagues up here. I particularly want to echo the comments of Chairman Barton in his expressions just of being mystified and revolted in our preparation for this hearing.

The questions that many of us ask and all of us probably ask of ourselves is what does it say about those who have been involved in this--as we are hearing this morning--industry? What does it say about those who would exploit children, young kids for these purposes? And I have, my wife and I are blessed to have four little ones in our house. But I think that an important question would be to ask ourselves this morning is what does it say about us in this Congress if we do not act, if we do not



conduct these hearings, if we do not take our responsibility seriously to ensure that these types of exploitations and problems and challenges do not happen again? It is our responsibility, certainly part of our responsibility to act.

I also want to thank our witnesses for being here today. Justin, in particular, I appreciate you being here today. I applaud the courage of those who are coming forth to educate members of this subcommittee about this topic. It is not an easy topic to deal with, it is graphic and it is gruesome, and more often than not it is hard to hear about, but it is a topic that cannot be ignored. Last year in New Jersey, in my home State, police arrested 39 people across the State in connection with a child Internet pornography ring that in one of the more horrifying videos depicted the rape of a 5-year-old girl.

Today's technology holds tremendous potential to enhance our lives; however, this advancement of technology is opening the door to a whole new generation of criminals, the child predator who takes advantage of children in the worst way by using this technology to prey upon children in the safety and the confines of their own home. There is no question in anybody's mind that we must pay serious attention to this horrific industry and take steps to stop it. We must let the children and the parents of this country know that we will not allow this practice to continue. We will not allow them to be exploited or harmed or taken advantage of. People who are engaging in this type of activity must face serious consequences and it is our responsibility, as I said earlier, to let our children know that we will protect them at all costs. And I think of our formative ones in our house and am well aware of the dangers facing them and all of our children in the world today. It is the responsibility of parents to stop at nothing to protect our children from those who prey upon their innocence by taking advantage of them in ways that frankly many of us thought was simply unimaginable.

Luckily, this industry is beginning to be brought into the limelight. There are now groups and law enforcement organizations that have made finding and punishing these criminals a priority, but they cannot do it alone. We must give them the tools to find these predators and bring them to justice and we must let our children know that they are not alone. Organizations like i-SAFE have made it their mission to educate children about how to use the Internet safely and what warning signs to look out for. This group has educated over 43,000 students on Internet safety and implemented 20 parent education organizations in New Jersey alone. I commend them for their programs and I sincerely hope that they and others continue this type of activity in the future.

I hope that this hearing serves to draw further attention to this terrible industry and I would like to thank you, Mr. Chairman and Mr.

Stupak, for holding this hearing and I look forward to hearing from our witnesses both today and later in this week.

I yield back.

MR. WHITFIELD. Thank you very much, Mr. Ferguson.

I guess that concludes the opening statements.

MR. STUPAK. Mr. Chairman, if I may?

MR. WHITFIELD. Yes, sir.

MR. STUPAK. Mr. Chairman, I would like to submit the statement of the Honorable John Dingell, the Ranking Member of the Energy and Commerce Committee, his opening statement for the record, please.

MR. WHITFIELD. Without objection, so ordered.

[The prepared statement of Hon. John D. Dingell follows:]

PREPARED STATEMENT OF THE HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS  
FROM THE STATE OF MICHIGAN

Mr. Chairman, thank you for opening this important investigation and convening the first hearing today. This hearing will examine one of the most disturbing topics affecting the safety and health of our youngest citizenry. Those who have found the Internet a most expedient venue for peddling the worse kind of smut, not only profit from some of the most heinous crimes imaginable, but also encourage its creation around the world.

Let us be clear about this. This is not about pornographic images of adults. What we are investigating today is the purveyance of live and videotaped broadcasts, as well as photographs, of sexual and other physical assaults on children -- many prepubescent but some as young as toddlers and infants -- for the purpose of producing images for sale or trade over the Internet. The Internet has regrettably provided the medium for the exponential growth in these deplorable crimes.

The uses of the Internet by tech-savvy pedophiles are many. Among their most common uses are pay-to-view Web sites and peer-to-peer chat rooms. Some of these chat rooms provide opportunity to trade images. Unfortunately, the price of admission is often new material; hence, the ease of contact via the Internet has contributed to the incentives and growth of the horrendous abuse endured by these young victims, usually within their own home.

Other chat rooms contain the candid thoughts of millions of adolescent and even preteen subscribers. Molesters, often initially posing as an adolescent themselves, use these chat rooms to seduce unsuspecting children into meetings for their heinous pleasure and/or profit.

I suspect we will learn more about the ways and means of the Internet perverts today and at future hearings. What is certain is that this global problem has deep and dirty tentacles right here in the United States.

Taking away the profit and anonymity from these criminals may not put an end to these crimes. Reducing the convenience and incentives for the depraved individuals who use the Internet for such activities, however, will be an important start. As this Committee works on increasing broadband competition and Internet use across the country, we must also work toward eliminating the scourge of child pornography from the Internet.

MR. STUPAK. Thank you.

MR. WHITFIELD. Thank you.

At this time, we will call our first witness, Dr. Sharon Cooper. And as I had mentioned in my opening statement, Dr. Cooper was scheduled to be in Germany today and postponed that trip, so we generally appreciate that, Dr. Cooper, and if you would come forward and sit here in the center would be great. Now, Dr. Cooper is not only a physician, but she is involved in forensic pediatrics. As I said, she is the head of the Development and Forensic Pediatrics, I guess within the Department of Pediatrics at the University of North Carolina at Chapel Hill. We welcome you today and we look forward to your testimony. As you may understand, this is a hearing of the Oversight and Investigations Subcommittee and we generally take testimony under oath. I would ask you; do you have any objection to testifying under oath today?

DR. COOPER. No, I do not.

MR. WHITFIELD. The rules of the House and rules of the committee, you are entitled to be advised by counsel about your constitutional rights. Do you desire to be advised by legal counsel today?

DR. COOPER. No, I do not.

[Witness sworn]

MR. WHITFIELD. Thank you, Dr. Cooper, you are now sworn in and you will be recognized for five minutes for your opening statement.

**TESTIMONY OF SHARON W. COOPER, M.D., FAAP,  
DEVELOPMENTAL AND FORENSIC PEDIATRICS, PA,  
DEPARTMENT OF PEDIATRICS, UNIVERSITY OF NORTH  
CAROLINA CHAPEL HILL**

DR. COOPER. Thank you, sir.

My name is Sharon Cooper and I am an Adjunct Professor of Pediatrics at the University of North Carolina at Chapel Hill. I have worked as a pediatrician for 30 years and in the area of forensic pediatrics since 1980. As a doctor who works with maltreated children, a forensic pediatrician has advanced understanding of the nexus of medicine and the law and focuses on assuring that children will have the correct diagnosis if they are victims of child maltreatment.

Serving as a multidisciplinary child abuse team member for 27 years, I have examined thousands of children who have been the victims of child sexual abuse, as well as other forms of child maltreatment. I have lectured throughout the United States and internationally providing more than 200 trainings in the areas of child sexual exploitation, physical abuse, child neglect, and child homicide. I spent 21 years as an active duty Army officer providing general pediatric developmental and behavioral pediatric, and forensic pediatric care for members of the armed services. I continue as an instructor for the Department of the

Army Medical Education Center and School at Fort Sam Houston, Texas, which provides the multidisciplinary training to family advocacy program members in branches of the services.

Since my retirement from the Army, with the rank of colonel 9 years ago, I focused my area of expertise on child sexual exploitation, child and youth development, behavior, and all aspects of child maltreatment. I have been an instructor for the National Center for Missing and Exploited Children in Alexandria, Virginia for nearly 6 years and have been provided training on victim impact on children depicted in child sexual abuse images and exploited through prostitution. In addition, I teach prosecutors, law enforcement officers, judges, and healthcare providers on how to medically analyze these pornography images and facilitate the evaluations of such images with the children's agents. I have worked with the Child Victim Identification Program and the National Center. I have taught at the International Center for Missing and Exploited Children and the Microsoft Corporation providing similar training to law enforcement officers in the U.S., Canada, Europe, Russia, Southeast Asia, and the Middle East.

As a forensic pediatrician, I have also provided medical care directly to children who have been sexually abused and pornographically photographed or videotaped. These clinical evaluations have included family and investigator interviews, review of the pornographic images, victim medical interviews, full medical examination, and case conferences. I have also evaluated children who have been exploited through prostitution both from within their families, as well as by acquaintances and intimate partners.

In addition to having to evaluate children and youth victimized in this manner, I have also analyzed thousands of images of child pornography. These images were stored as computer files, videotapes, DVDs, Polaroid's, and other images.

Child sexual exploitation is the most underreported form of child abuse. Child pornography on the Internet, in particular, has untold impact upon victims. The possession and distribution of these images which are in fact digital crime scenes, promote the need for more and more plentiful and more graphic images. The two most commonly cited reasons that individuals collect these images are for sexual gratification through masturbation and as a plan for action. Many criminology studies have been done to show the motivation of individuals who would collect these images and this research has revealed that there is a one and three chance to as high as three out of four chances that an individual with such images has already sexually abused a child.

Child pornography constitutes insult to injury to a victim. The injury is child sexual abuse. The insult is the memorialization of that child

sexual abuse from time untold. It is very important for us to recognize that child pornography is a phenomenon which we must pay close attention to and seek to eradicate.

I am very pleased to be here before the committee today and look forward to answering any questions that you may have.

[The prepared statement of Sharon W. Cooper, M.D., follows:]

PREPARED STATEMENT OF SHARON W. COOPER, M.D., FAAP, DEVELOPMENTAL AND FORENSIC PEDIATRICS, PA, DEPARTMENT OF PEDIATRICS, UNIVERSITY OF NORTH CAROLINA CHAPEL HILL

#### SUMMARY

Child sexual exploitation is the most underreported form of child abuse today. Boosted by the Internet, these sexual abuse images constitute a digital crime scene, and a significant percent of such images online are of children less than 5 years of age. Driven by a offender pool which has anywhere from a one in three chance to a three out of four chance of having already sexually abused a minor, the supply and demand for this multibillion dollar industry continues to grow. Initially, the National Center and Missing and Exploited Children® monitored a database of 100,000 images. Today, this number of images has ballooned to more than 3 million. Children are often sexually abused and pornographically photographed by family members and familiar acquaintances.

The presence of extremely graphic sadistic images of very young toddlers reinforces the skill of offenders who choose the most vulnerable of victims who are not only often preverbal, but who are also most likely to have trouble qualifying as a competent witness at a criminal trial.

The link of pornography to the other four types of sexual exploitation: prostitution of children and youths, cyber-enticement, child sex tourism and human trafficking is well described. Professionals in the child abuse multidisciplinary teams must work ardently to become educated regarding this form of abuse. Recognizing the impact of child sexual abuse images on the Internet and predator dynamics is essential to reversing this exploding and extremely dangerous crime in America today.

I. My name is Sharon Cooper and I am an adjunct professor of Pediatrics at the University of North Carolina at Chapel Hill, School of Medicine. I have worked as a Pediatrician for 30 years and in the area of Forensic Pediatrics since 1980. As a doctor who works with maltreated children, a Forensic Pediatrician has an advanced understanding of the nexus of medicine and the law, and focuses on assuring that children will be correctly diagnosed as victims of child maltreatment when that diagnosis is considered. Serving as a multidisciplinary child abuse team member for 27 years, I have examined thousands of children who have been the victims of child sexual abuse as well as other forms of child maltreatment. I have lectured throughout the United States and internationally, providing more than 200 trainings in the areas of child sexual exploitation, child sexual abuse, physical abuse, neglect and child homicide. I spent 21 years as an active duty Army officer providing general Pediatric, Developmental and Behavioral Pediatric and Forensic Pediatric care for children of members of all branches of the armed forces. I continue as an instructor for the Army Medical Education Department Center and School at Fort Sam Houston, Texas which provides multidisciplinary team training to Family Advocacy Program members in all branches of the services. Since my retirement with the rank of colonel from the United States Army 9 years ago, I

have focused my areas of expertise on child sexual exploitation, child and youth development and behavior, and all aspects of child maltreatment. I have been an instructor at the National Center for Missing and Exploited Children in Alexandria, Virginia for nearly six years, and have provided training on the victim impact on children depicted in child sexual abuse images and exploited through prostitution. In addition, I teach prosecutors, law enforcement officers, judges and health care providers how to medically analyze child pornography images. I have provided even more in depth training regarding the determination of probable victim ages to the analysts of the Child Victim Identification Program of the National Center for Missing and Exploited Children as well as similar professionals of the Canadian Cybertipline. Working with the International Center for Missing and Exploited Children and the Microsoft Corporation, I have provided similar training to law enforcement officers in the US, Canada, Europe, Russia, Southeast Asia and the Middle East.

- II. As a Forensic Pediatrician I have provided direct patient care to several children who have been sexually abused and pornographically photographed or videotaped. These clinical evaluations have included family and investigator interviews, review of the pornographic images, victim medical interviews, behavioral analyses, and full medical examinations as well as case conferences after the medical assessment. I have also evaluated children who have been exploited through prostitution both from within their families as well as by acquaintances and intimate partners. In addition to having evaluated children and youths victimized in this manner, I have also analyzed thousands of images of child pornography. These images were stored as computer files, videotapes, DVDs, Polaroid pictures, and published images in trade magazines. The overwhelming majority of this contraband was computer stored images and videotapes, confiscated during investigations by Internet Crimes against Children (ICAC) teams and almost all federal criminal investigative agencies. I have published in this area to include an article with Attorney Damon King of the Child Sexual Exploitation and Obscenity Section. of the Department of Justice. I have served as an expert witness in family court and criminal prosecutions involving child pornography in state, federal and court martial proceedings.
- III. I have recently completed a textbook on the subject of child sexual exploitation in 2005 which has been endorsed by the National District Attorney's Association. The text, entitled *Medical, Legal, and Social Science Aspects of Child Sexual Exploitation: A Comprehensive Review of Pornography, Prostitution, and Internet Crimes* has four other co-authors: Richard Estes, DSW, ACSW, Angelo P. Giardino, MD, PhD, FAAP, Nancy D. Kellogg, MD, and Victor I. Vieth, JD. This compendium of nearly 60 contributors from 8 different countries provides a thorough background of the five types of child sexual exploitation: child pornography, prostitution of children and youths, cyber-enticement, child sex tourism, and the human trafficking of children and youths, both domestically and internationally. The text has a supplemental CD-ROM which includes further information in this area with case reports, training modules, selected readings and in particular an emphasis on the medical care of victims of these forms of child abuse.
- IV. Child sexual exploitation is cited to be the most underreported form of child abuse. Child pornography on the Internet in particular has as yet untold impact

upon victims. The possession and distribution of these images, which are in fact, digital crime scenes, promotes a need for newer, more plentiful and more graphic images. The two most commonly cited reasons that individuals collect these images are for sexual gratification through masturbation and as a plan for action. Criminology studies to date from the US Postal Inspection Service, the Toronto Child Sexual Exploitation Unit and the Federal Bureau of Prisons here in the US reveal that those who possess these images have a 1 in 3 chance to as high as 3 out of 4 chance of having already sexually abused a child. Further research from the National Juvenile Online Victimization (N-JOV) Study (Wolak, Mitchell & Finkelhor, 2003) has revealed that from 2000-2001, offenders primarily collected child pornography of children between the ages of 6 and 12 years. It is important to know, though those offenders are often diverse in the content of their child pornography collections and during that same period, nearly 50% of collected images were of children less than 5 years old. Such young victims are prime targets for sex offenders because of their preverbal nature and the fact that they often unable to be made competent on a witness stand in criminal proceedings.

- V. Child pornography constitutes insult to injury for a victim: the injury is child sexual abuse in all of its methods of victimization. The insult is the memorialization of that exploitation for an untold amount of time. Many of the images which I see on a regular basis show severe vaginal and anal assault against toddlers, bondage of these children with gags in their mouths, ligatures around their necks, and on occasion, physical beatings in conjunction with video clips of brutal oral, vaginal and anal penetration. In addition, recent research has shown that 88% of girls who have been sexually abused do not make a disclosure during childhood (Hansen, 1999). Numerous case examples of victims of child sexual abuse and pornography production, denial of the existence of photos or videotapes etc. is also very common, even though children do acknowledge the sexual abuse. Training for interviewing and treating such children and youths as well as those who have been groomed into compliant victimization is both essential and an immediate priority. Programs such as *Finding Words* and other forensic interviewing curricula must include the evaluation of these types of victims.
- VI. It is very important to understand that child pornography is a common thread in all forms of child sexual exploitation: prostituted children and youths, cyber-enticement, child sex tourism and human trafficking of children. The bottom line is that children have become a commodity for a practice that seeks to normalize sexual harm. Preferential sex offenders who produce these images have been reported to be responding to special requests from like minded online offenders, or strictly as a means of financial gain. Infant and toddler sexual abuse is a frightening and sobering reality particularly in light of the National Institute of Justice report in 1994 which cited that victims of child sexual abuse were twenty-eight times more likely to be arrested in their lives for prostitution, than children who had never been sexually abused. Recent high profile multiple victim and multiple offender sex rings have alerted those of us who work in this area to the fact that immense technology exists in support of these types of heinous crimes against our most important national treasure, our country's future, our children. I urge you to read the attached document, "Unto the Third Generation" written by one of our co-authors, Attorney Victor Vieth, Director of the American Prosecutor's Research Institute's National Child Protection Training Center. I look forward to providing whatever information

that I can to the members of this committee and express my appreciation for the opportunity to answer any of your questions.

MR. WHITFIELD. Dr. Cooper, thank you. Thanks so much for your testimony.

Did you read the December 19, 2005 story in the New York Times about Justin Berry?

DR. COOPER. Yes, I did.

MR. WHITFIELD. Well, could you explain how an online predator is able to actually convince a child to do some of the things that Justin did, like perform sexual acts on a webcam for money? How can they actually do that?

DR. COOPER. I think that the important phenomenon for us to understand is that online predators befriend adolescents. They become closer to them than many times their family members are. They are frequently in touch with them several times a day. In addition to giving them numerous awards and rewards for their discussion online, they become their closest friends. And because of that, and because of the adolescent's mind which is very much in the sexually explorative phase in child development, it is not unusual for sexual exploration to be part of that relationship. So we find that many adolescents who become exhibitionistic on the Internet are doing so partly because of sexual exploration and sexual development, and also because of a normalization of sexual harm that is very prevalent in our society today. Sexualized images are everywhere to be found on the television, in their music, in music videos, in magazines, it is very, very common and so consequently it is easy for me to understand how an adolescent who is reaching out for some type of companionship online could fall prey and become a compliant victim.

MR. WHITFIELD. So these so-called predators, they actually form a close friendship with the child by way of the Internet initially and then maybe start talking to them on the phone or meet them somewhere.

DR. COOPER. That is correct, sir. I have taken care of several adolescent victims who have had their first relationships via an online partnership. And first of all, it is odd that we would think this is hard for teenagers because adults do the same thing. We have lots of online dating today. Lots of Internet chat rooms between adults and kids are very much the same way. I think what is more important is that predators recognize the vulnerability of children and they frequently will be there at all times of the night, frequently contacting the children after their parents have gone to bed, giving them cell phones so that they can have direct contact and the parents will not know. And this secrecy, as well as attention that is provided to teenagers is very, very convincing to young children.



MR. WHITFIELD. Now, we all know what the word predator means, but looking at that term as it relates to sexual exploitation of children on the Internet, how would you actually define the term predator?

DR. COOPER. I would say that a person who is a predator on the Internet is a person who commodifies children. They do not see children as beings, but as a commodity and what purpose and function do they serve for that person's sexual gratification or monetary benefits. So they are a predator from the standpoint of certainly presenting themselves as harmful to a child, but the most important thing is that they will look upon this child as a checkmark if you will among the whole group of children that they are seeking to exploit in this manner.

MR. WHITFIELD. And so it starts out as a friendship that eventually ends up with the predator providing gifts and/or money or some other inducement. Is that correct?

DR. COOPER. That is correct.

MR. WHITFIELD. Now, could you explain from your professional experience how say Justin's experiences, what kind of impact does that have on a child over time?

DR. COOPER. If I were to use an example such as the case of Mr. Berry, I would have to say that this is a life changing event. Child sexual abuse in and of itself is the beginning of this process for him. And much of the research tells us that 86 percent of children who are sexually abused, whether that occurs in early childhood or in adolescent years, will have long-term consequences. Typically the most common problems that we will see are going to be depression, anxiety, and post-traumatic stress disorder. But we also think that kids who are exploited online have an additional phenomenon and that is the paranoia that other people will be able to know what has happened to them and the fact that other people may discover those images at any time in the future. This causes a degree of computer absorption, a paranoia regarding peer groups that children who have been sexually abused and others do not know or may be able to hide better.

MR. WHITFIELD. Now I have read Justin's testimony and I have also read stories about other young people who have been solicited over the Internet. One of the things that is kind of puzzling about this is once they actually meet the predator and they are sexually exploited or molested, there seems to be a tendency to continue to meet with the predator even after that. How does that happen and why does that happen?

DR. COOPER. What frequently occurs is that that initial meeting on the part of the child and the predator is one of explanation. Initially the child sees themselves as an equal to that predator. What they do not recognize and as time goes on, they are not in control of that relationship. They would like to be in control of that relationship, but this other person

continues to, I would say, digitally stalk them, to being in touch with them all the time, to encourage them to continue to meet, that they cannot live without them. This type of attention and inducement is very difficult for anybody, including an adolescent to resist. It causes them to feel better about themselves initially, until they discover that they are being exploited and it is not their choice to continue in those relationships.

MR. WHITFIELD. Now, in your testimony, you described child pornography as a digital crime scene.

DR. COOPER. That is correct.

MR. WHITFIELD. When you said those three words, would you elaborate on that just for a few minutes?

DR. COOPER. Yes, I would be happy to. For a long time, healthcare professionals and others in the field of child abuse had a hard time acknowledging that child pornography was real. They thought perhaps these images were morphed and thought that these were not truly children, they were adults made to look like children. It took a lot for individuals to finally come to recognize that these are actually children. What we are seeing is very similar to a video camera in a convenience store. You are seeing the actual real time sexual abuse of a child. When we see online images or if we see videotapes that have been made of children, by sex tourists who have gone outside the country and made their own videotapes, we are looking at a crime scene. The fact that it is online makes it a digital crime scene. And it is very important for us to recognize that in the United States, we call this child pornography, but in Europe, in many of the other countries outside of this country, these are referred to as child sexual abuse images. So that the public will not be confused if this is a voluntary modeling, it is not voluntary modeling, it is in fact a crime.

MR. WHITFIELD. Now, in your professional capacity have you had the opportunity to interview or study or meet with the so-called predators at all?

DR. COOPER. I have had the opportunity to testify in court cases in fact of individuals who have exploited children through either pornography and many times pornography and prostitution together because that is a very common connection.

MR. WHITFIELD. And that motivates a predator?

DR. COOPER. I would say that there are three common reasons, although the researchers, the best researchers for this have been in Ireland who have gone into the prison system and interviewed collectors of child pornography. The three most common reasons that are cited are, number one for sexual gratification. These individuals will look at images in order to fantasize about their own relationship with that child.

A second reason that they will collect images or seek to make images is because it is a plan for action. That is the most important one that I think we will need to be aware of. When an individual is looking at child pornography online, many of these individuals are planning how they are going to commit a contact offense with another child. They are using what they are seeing online, both to normalize and justify their behaviors. Particularly if they see hundreds and hundreds of images online, they come to the belief that this is common, everyone is doing it, and so, therefore, I am going to do it too. They will use what they see as a plan for action. The third reason is because it allows them to be a collector, in fact and with their likeminded friends, they can speak of the fact that they have numerous images within their collection.

MR. WHITFIELD. Now, would you say that, and I know it is difficult to generalize, but predators who are engaged in this activity, I am assuming most of them have full-time jobs. They may be a professional, they may come from any walk of life. Is that correct?

DR. COOPER. There is a very interesting phenomenon about child pornography, that is correct, that they do come from all walks of life. There may very well be small town individuals who have very minimal resources, who still are downloading child pornography. In one particular case that I am familiar with in my State, an individual was marketing his seven-year-old daughter by sending pictures of her on the Internet and he did not even have his own computer, he was using the county library computer to do this. So you can have individuals who are not wealthy well-to-do individuals, are still very much involved in this practice.

MR. WHITFIELD. It would not be unusual for them to send over the Internet, a webcam of them actually molesting the child on, I mean, televised while they are doing it, right?

DR. COOPER. They would have live webcam situations. You have almost all of those, a receiver of that information so you usually have at least two individuals who are intentionally communicating with images. As you are aware, the most recent and high profile case that occurred two weeks ago is associated with 27 individuals who were live web casting to each other and talking so that they could ask for certain sexual acts to be performed on a given child so that they would have the opportunity to watch this.

MR. WHITFIELD. Well thanks, Dr. Cooper, my time is expired and I recognize Mr. Stupak.

MR. STUPAK. Well thank you.

Thank you, Dr. Cooper, for rearranging your travel schedule to be with us here today on this important issue.

DR. COOPER. Thank you.

MR. STUPAK. You mentioned a small town and actually my staff being well prepared went to the Michigan site for a public sex offender registry and this was just from my small town, I come from a very small town but it is seven pages, there are 39 people there. And I will quite tell you as I just thumbed through it here quickly I was quite surprised. These public sex offender registries we hear a lot about, are they any kind of a deterrent? It seems they catch a lot of attention but is it some kind of deterrent to a kind of sexual abuse we are seeing on the Internet?

DR. COOPER. Sir, I would say that the presence of being a registered sex offender may deter a person from having a contact offense with a child in their neighborhood; however, I believe that it does contribute to individuals going online more, because unless their sex offense results in a parole or a probation, or that they cannot access or use a computer, individuals are more likely to go online to access images of children for the purpose of sexual gratification through masturbation because they are fearful to actually have contact offenses. What we also know is that sex offender registries have a higher association of spawning child sex tourists. Americans are the most common child sex tourists and one of the main reasons they leave the United States to travel to third tier countries in order to have sex with children is because they are registered sex offenders. And so it sort of switches or transitions the victims from American children to foreign national children.

MR. STUPAK. I see. In this and I just read that, I was just looking at again just very quickly. Are you surprised that the number of people registered here who are only 20, 21, 22. Is there any kind of, in your research or studies, is there any kind of profile of the person who is trying to obtain this information over the Internet? I mean, I got all ages on this list and I do not know what the offenses are for but is there any kind of profile that has developed through your work?

DR. COOPER. We know that the majority of individuals who are seeking either to contact children or who are collecting images are male, almost 99 percent are male. They tend to be non-Hispanic white males. We also know that they have the highest incidents of committing this crime between the ages of 26 and 35. That is your most common age, however, we are beginning to see younger and younger offenders if you will, to include youth offenders because of the availability of child pornography on the Internet. I believe that we are in a bit of a quandary to decide what to do about teenagers, for example, who are downloading images because we are not sure if the images titled 13-year-old daughter, for example, and a 15-year-old is accessing that image, we would be a little confused as to whether or not that actually would constitute child abuse or sexual exploration. So you can see that while we have the young offenders, they are breaking a low but we are not positive about

the positive there. On the other hand, we have definitely older people who are clearly accessing images of very young children. There is no doubt that they are doing that with informed consent so to speak.

MR. STUPAK. Let me ask you this in your research and I see you have a couple of your books there. One part was, in your research is about the law but just the public sex offender registry, each State has them, would those convictions for a sexual possession of pornography, children, would that necessarily be on these offenders if the list teaches things a little different as to what offenses make up to find yourself on a public sex offender registry? It is my understanding some States even if you are convicted of the crimes we are talking about today you do not appear on the sexual offender list.

DR. COOPER. That is correct, sir. It really depends upon the State and the judge, how that final sentencing is going to be. Our goal is to educate prosecutors, juries, and judges that if you are going to not have any type of incarceration as the sentence for this kind of crime, the least that should happen is that a person should become a registered sex offender.

MR. STUPAK. So that would be one area where Congress probably would have an opportunity to act on since the Internet is interstate commerce and no doubt about that.

Do you think child pornography is becoming more acceptable in our society? You mentioned that if I am convicted here in the United States, then I will just go elsewhere to get around the limitations that may be placed upon me here in the United States.

DR. COOPER. I believe that child pornography in our society, no, I do not think it is becoming more acceptable, although it is becoming more common. What I do believe is that people who are sexually abusing their children are changing. They are becoming more exhibitionistic with respect to how they sexually abuse their children. Ten years ago, before we had public access to the Internet so readily, parents were sexually abusing their children but they were not taking videotapes and making pictures and putting them on the Internet. Now that is what we are beginning to see, which means that they see their children not only as their victims but as a commodity for money to the public and those who are likeminded and would like to have access to their children in that sense. So I see the commodification of children as a bigger problem in our society and the fact that we fail to see them as individuals who will be highly harmed by knowing that their images are on the Internet.

MR. STUPAK. You indicated in your answer that while it is not more acceptable, it is more common in children in the ways they become more of a commodity, a commercial enterprise.

DR. COOPER. This is correct.

MR. STUPAK. Because of the growing use of the Internet, are consumers then often required not only to purchase images but also to provide their own unique picture, I do not want to say unique but provide something which will not only be it for purchase for the personal satisfaction but also then are they required then to provide pictures or to put the pressure upon them to access?

DR. COOPER. Yeah, absolutely, correct. There are several episodes of discussions on the Internet between individuals who want new images. They may want, for example, the reset of a known series that they have. A series may have 30 or 40 images, and they only have 15 so they want the rest. The key thing though, is that they will usually be required to provide their own images in order to, as a trading in order to do that. There are certain situations where they are asked to provide new images that have never been on the Internet before, and this is what encourages individuals to sexually abuse their own children in order to make those images available. Those have a higher desirability because more people already have many of the hundreds of thousands of images that are already on the Internet.

MR. STUPAK. Let me ask you this. And I do not mean this in any way a reflection upon baseball. What I am going to say is are they trading them--like when I was growing up we traded baseball card and certain things, certain cards you wanted, certain stars. Is it like that on the Internet?

DR. COOPER. Very much it is that way, particularly when you have collectors who want to complete their series, or if you have individuals who have a certain fetish. For example, one case that I worked in, the individual had a child smoking fetish and he wanted pornographic images of children, all of whom were smoking. So they work very hard to find other people who have those kind of images and frequently those are homemade images.

MR. STUPAK. Let me ask this question because I mentioned in my opening and in my research and someone mentioned, our staffs have really done a good job in helping us prepare for this but in our research in everything we have done here, it appears that about 60 percent of these victims are under the age of 12. So did you and you mentioned it earlier, could you explain what you mean by grooming children into compliant victimization?

DR. COOPER. Yes, I will. And if I could make a comment--

MR. STUPAK. Sure.

DR. COOPER. --of the 60 percent who are under 12, the reason that 60 percent are under 12, is because it is easier to charge when children are pre-pubescent appearing. You will have plenty of adolescent victims

whose images are also on the Internet. But because they are adolescents, it is more difficult to tell that they are less than 18, which is the standard of the law. You will have adolescent victims and they would be marketed under gold banners, and others with still underage minors, but it is much easier to charge and successfully prosecute children who do not appear to have any sexual maturation which classically is children under 12. Now in answer to your question regarding complaint victimization, when children see or are shown images of other children who are being sexually abused and this is a common behavior of cyber enticers who will send pornographic images to children in order to help them understand that everybody does this, it is okay. When that happens, children will come to believe that this is something that lots of other kids do so maybe it is not that bad and they become a compliant victim in that situation and can actually recruit other victims.

MR. STUPAK. Now then what happens to the very young victim after they are rescued from their abusers after years of grooming and being used in child pornography images? What kind of a child is left us?

DR. COOPER. A very damaged child. The National Institute of Justice tells us that they are 28 times more likely to be arrested for prostitution in their lives than other children.

MR. STUPAK. It looks like my time has expired. Thank you, Mr. Chairman and thank you again for your testimony and being here today.

DR. COOPER. Thank you.

MR. WHITFIELD. Thank you.

At this time, I will recognize the Chairman for his 10 minutes of questions.

CHAIRMAN BARTON. Thank you, Mr. Chairman. I have been in my office watching the hearing on television.

Dr. Cooper, let us set aside the tragedy of this for a moment; what is the societal poison or wrong that happens as a result of child pornography? What happens to us as a society because of this?

DR. COOPER. Sir, I would say that our society responds as it did to violence on television. We become tolerant to the presence of really significant violence and we fail to recognize after a while that it is indeed violence. The same is true with child pornography. If we do not respond with an absolute zero tolerance type of response, we will begin to accept the form of child abuse. I think the other important point is that because this is a technology driven type of crime, many people fail to recognize that we are talking about child sexual abuse. In fact, I sit on several committees, national committees, that have had a hard time grasping that we are really talking about child sexual abuse with the digital moralization. So we have had a tough time getting our child protection services workers to the table for example because it has been hard for

them to understand that this is not a victimless crime. Five years ago, that was the most common statement, this is a victimless crime.

CHAIRMAN BARTON. Well do the children that are molested, as adults, do they manifest any social behavioral problems, law enforcement run-ins on a higher level of incidents than children that are not exploited as children sexually?

DR. COOPER. Yes, they do, sir. When they have been exploited especially visually, you are much more likely to accept yourself that way. To become a marketer or to be easily marketed by others is the next that follow to this type of exploitation so many that prostitution has a much higher occurrence in individuals who are exploited in this manner. And in fact, Dr. Richard Estes research from the University of Pennsylvania, revealed when he went to codify the cities he went out of State to juvenile detention centers talking to kids who had been arrested for prostitution. There was an overwhelmingly large number of these children who had been already prostituted and pornographically photographed from within their families before they ran away and ultimately were being prostituted on the streets.

CHAIRMAN BARTON. And when you talk about, excuse me, digital molestation what is the minimum standard that would be considered to be sexually exploitive?

DR. COOPER. In the United States, images revealed new lascivious, if you will, visualization of the genitals of a child. The child may be dressed but their clothes, their position, the way that the individual closeness from inside of camera is focusing typically on the genital area. That is the beginning of an exploitive image for the U.S.

CHAIRMAN BARTON. Now is that under current law, is that illegal?

DR. COOPER. That is illegal under the Protect Acts; however, many images of nude children who are then shown in various sexually explicit poses without any evidence of actual sexual assault are considered erotica in the United States, although they are considered pornography in Canada just across the border.

CHAIRMAN BARTON. So if a parent were to take his or her child and pose them without their clothes on and send that over the Internet that would be illegal today?

DR. COOPER. It would depend upon how they are posed. And let me give you an example. One of my patient's in my child abuse clinic stepfather posed her, 11-year-old, posed her at a table with her breasts lying on grass and put little bunny ears above her breasts and took pictures of this. This is not considered to be pornographic because it was not genital. The effect on the child as you can imagine was significant. The Walgreen Department Store that made these pictures out of the film called law enforcement right away because they thought this was child



pornography but it did not meet the letter of the law under that circumstance because it was not genital exposure.

CHAIRMAN BARTON. Is there any indication that because of the Internet, parents that exploit their children is growing as a percent of the population?

DR. COOPER. I think so because I have been seeing child sexual abuse cases since 1980 and I cannot recall seeing as many parents who have taken pictures of their children like they are now and beginning to put them on the Internet, to exchange them with each other. This is very much a concerning trend.

CHAIRMAN BARTON. Now under current law, a parent that does that, if caught and convicted, does the parent lose custody of the child?

DR. COOPER. Almost always that would be the case, yes.

CHAIRMAN BARTON. What about the amounts of money? We were briefed that in one of the cases they were taking in several million dollars a month.

DR. COOPER. That is correct. The Avalanche case is a good example.

CHAIRMAN BARTON. Under current law, does that, can that money be forfeited like in a drug case or does it stay in the account of the exploiter and they do their time and it is their money?

DR. COOPER. Recently, sir, in Kentucky, I testified in a deposition for that purpose so that money that was obtained by in this particular case from an individual who was making child pornography, and as a Federal employee had his own money from his retirement. That particular U.S. Attorney made the appropriate motions to have his retirement pay closed in a fund for the child victims for their mental health services for several years to come. So that degree of restorative justice is definitely available and it is something that I have only seen once, but would really like to see happen more.

CHAIRMAN BARTON. Well, is that something that we need to look at, at the Federal level, a special statute of enforcement and penalties for parental molestation and asset forfeiture is that something that would be helpful?

DR. COOPER. Definitely, sir. This was a stepfather to this child. There were several victims, but the primary victim was this child. I think that would be a very good idea.

CHAIRMAN BARTON. Is most of the money that changes hands done by credit card?

DR. COOPER. And PayPal accounts, yes, usually through credit accounts and PayPal.

CHAIRMAN BARTON. Is that something that we need to look at? Are there any under current law, penalties towards a credit card company that

knowingly and willfully accepts funds, transfers funds of a child pornographic nature?

DR. COOPER. I definitely believe that is something that the Congress should consider, sir, because we are doing the best we can do from the victim level, but when we have this much money driving the train, it is very hard to interrupt that kind of process without some type of very high level regulation or mandatory perusal.

CHAIRMAN BARTON. Okay. I think, Mr. Chairman, that is enough questions for this witness.

Thank you for your work in this effort area and thank you for testifying today.

DR. COOPER. Thank you, sir.

MR. WHITFIELD. Thank you, Mr. Chairman.

I might mention that on Thursday we are going to have another hearing on this issue relating to law enforcement and we are going to get into more detail about the methods of payment.

And at this time, I recognize Dr. Burgess for his 10 minutes.

MR. BURGESS. Thank you, Mr. Chairman.

Thank you, Dr. Cooper for being here and being so generous with your time this morning.

DR. COOPER. Yes, sir.

MR. BURGESS. You probably already answered this but let me ask it again just so I am sure that I understand it. I get the impression that of course child exploitation and child sexual abuse has been with us for a long, long time unfortunately.

DR. COOPER. That is correct.

MR. BURGESS. But get the impression that the Internet has caused a change in this. Is that a correct assumption?

DR. COOPER. That is true. I would agree. The Internet has made it all different. There are five different types of child sexual exploitation, but the Internet facilitates every single one of those types of child sexual exploitation.

MR. BURGESS. And you alluded a minute ago to somebody who took their pictures to Walgreen's to be developed and the developers obviously alerted someone if there was a problem or there may be a problem here, but the Internet and digital photography is where they cut out the middleman in many respects so that now the availability of creating images is can be done within the privacy of one's own home without involving a third party such as Walgreen's. Do you think that has had an effect?

DR. COOPER. Very much so, sir. I think the ability for collectors to be anonymous and for producers to be anonymous has made this a much more difficult crime for all of us to be able to attack. The greatest

individuals who suffer are the victims, because we see the images but we do not know who these children are. It is very challenging to try to track down where these images may have come from and who these children might be. It has been very challenging to do that.

MR. BURGESS. You used a word that I guess didn't even know was a verb but the word commodification of children and I guess just coming from a perspective where we have to be protective with the most vulnerable members of society, the fact that we are turning them into a commodity is a disturbing, a very disturbing concept for most of us up here. But, and the Chairman has asked this, but are there ways, other specific steps that you think we could take or that could be taken by legislative bodies to make it more difficult to commodify our children and to provide more protection to the most vulnerable members?

DR. COOPER. Yes, sir, I think that there are some steps that can be taken. One of the most important is to try to go back to our media the value of children, and to not allow children to be depicted in the media as a commodity, as we are beginning to see very, very commonly. This is one of the things that really contributes. In my discussions with outreach programs in various parts of the United States, this is one of the phenomena that is contributing to the compliant victim. When children see other kids on TV, especially teenagers on TV who are being treated in very sexually exploitive ways either through music videos, on videogames, et cetera, it causes children to believe themselves to be available in that manner. And that is the entertainment media and it is very challenging. I think we all have to pay attention to the huge messages that are being promoted every day, with respect to the whole commodification of children in the media. There is one thing, this is not obscenity per say, but it certainly is a message that all parents need to be more aware of when they see music videos with young teenagers who are being presented as if they were being prostituted, or as if they were being exploited and this is 24 hours a day on cable TV. It is really easy to see how kids will think this is okay for them.

MR. BURGESS. Or in fact during the presentation of the Oscars but let us--

DR. COOPER. Exactly right.

MR. BURGESS. Let us stay on this for a minute because this too predates the Internet. And I guess the question I would have is is the Internet a causer and effect here or is it merely a facilitator and now changes this behavior to one that can be accomplished at warp speed if you will?

DR. COOPER. It really does, sir. In fact, you can usually see some imagery on television and the next day it will be on the Internet and it will be the same imagery which will be on the Internet for the next 6

weeks. It may not be on TV anymore, but it will be on the Internet for the next six weeks and children can finally download that information or they can just look at it on their computers in their home and then as they get their cell phones with cameras and start to take pictures and transmit to each other. You can really understand how this would not be seen as terribly abnormal because they see it on the Internet every day in their bedrooms.

MR. BURGESS. So to some degree the Internet may be an accelerant for this fire and not in fact the cause of this?

DR. COOPER. That is correct.

MR. BURGESS. That is what this Chairman has done but that is what is going to make it so difficult for us legislatively to deal with this and we feel it is important work that we do need to take on. But for people who are parents who are concerned about their children, is there a particular type of profile that the parents ought to be aware of or particular types of behavior that they have to be aware of in their children that should cause some alarm bells to go off?

DR. COOPER. Well the first thing that I think is important for parents to understand, there used to be like the i-SAFETY Program is one but there are several programs. The National Center has one called Net Smarts as well. Parents really need to be educated from the preschool time period about the risks for child pornography and child sexual abuse because, remember that we have very young children who have been sexually abused these days and it is important for parents to understand how that can happen, and how to protect their children. I think the hardest part is for us to help parents recognize that these children are being abused within their own homes. There is almost always a non-absenting parent in that home, so we need to empower parents. Healthcare providers need to be talking to parents when children are infants about the importance of protecting their children, not just from the normal constant safety that we speak of, but the issues of sexual exploitation, sexual abuse which many parents would never think would be relevant information for an infant who is less than 12 months of age. However, the Internet is showing us that this is an important phenomenon that we need to be discussing with parents across the board. The majority of offenders are indeed men. So it is important for us to help parents understand that.

MR. BURGESS. What type of outreach program do you have for healthcare providers? Because that is, I have got to tell you as someone who just recently left the healthcare providing field, I do not know that this would have crossed my radar screen in dealing with a patient with a problem.

DR. COOPER. You are absolutely right. For those of us who work in child abuse, we are more tunnel-visioned with respect to child safety from abuse. General healthcare providers, family medicine, and pediatrics need to be much more aware of the fact that child pornography exists, that these are little children, they are not victimless and it is not a virtual crime, it is a real crime. We need to add to our ancillary guidance, in our well child checks, et cetera, sports physicals, questions to the children and also advice to parents about how to keep children safe but also how to make sure that they are not exposed every day to those mind changing media driven messages that can cause their pre-teens and teenagers to become compliant victims.

MR. BURGESS. That is an enormous task of education, re-education of healthcare professionals. Do you have some programs currently that are ongoing to do that, to accomplish that?

DR. COOPER. There are some online programs but I am a member of the American Academy of Pediatrics and it is my goal to try to bring this into our well child checks.

MR. BURGESS. Well, again, for parents who are watching this hearing today and I hope that some are, what are some of the things that they can themselves do to increase their involvement in their children's lives to put another barrier between their child and the potential for abuse?

DR. COOPER. The most important thing that I think parents should do is first of all communicate with their children from the time they are very young. Do not wait until they are 13 and 14 to start talking to them. The second point is to be aware of social networking sites such sites as MySpace, the FaceBook, Zanga.com, where children are beginning to do online diaries and put their own pictures of themselves which is a risk. That is a bit of a risk in particular because many children when they are 13 and 14 years of age will be a little exhibitionistic. That is just a part of being an adolescent but it is a little dangerous to be that way online as we have seen from the case of Justin Berry. He was only 13 and all he had to do was take his shirt off and all of a sudden men were responding to him in that situation. So I think talking to children from the very beginning, from the time they are very young, helping them to recognize and helping parents to recognize that the majority of offenders are not strangers. That is the other important point. Many parents speak to their children about being aware of strangers but the majority of sex offenders are acquaintances and/or relatives. The third point is to be careful not to let children have Internet access in their bedroom. They can have a computer in their bedroom, but not Internet access in their bedroom. That should be where parents can monitor their usage.

MR. BURGESS. Thanks again, Dr. Cooper. You have been very generous of your time and we really appreciate your rearranging your schedule to be with us today.

DR. COOPER. Thank you.

MR. BURGESS. Mr. Chairman, I will yield back.

MR. WHITFIELD. Thank you, Dr. Burgess.

And I recognize Mr. Walden for 10 minutes.

MR. WALDEN. Thank you, Mr. Chairman.

I do not know that I have got that many additional questions. You have done a marvelous job and my colleagues have asked all the questions I was thinking of as well.

DR. COOPER. Thank you, sir.

MR. WALDEN. As I listened to Dr. Burgess the things what can parents do, you certainly addressed those issues and enlightened us about how severe this problem is, so I appreciate your testimony today and the questions and unless you have anything else to add.

DR. COOPER. I remember that Mr. Barton had asked how could have individual have an interest in an 18-month-old and I wanted to respond to that question.

MR. WALDEN. Sure.

DR. COOPER. What we do know about individuals who sexually abuse infants and toddlers is that their sexual abuse is not really sexually driven from the standpoint of sexual desire for such a young child as a sexual partner, but the more common driving force with that young of a victim is the power and control motivation. And in fact interviews with convicted predators who have sexually abused children as young as 18 months have spoken of that fact. The cognitive distortion that we see in sex offenders is that their power and control is for the purpose of making that toddler a perfect sexual partner by the time they become an adolescent. So it is very important for us to recognize that cognitive distortions clearly already exist in sex offenders and the Internet can promote more of those cognitive distortions.

MR. WALDEN. Let me just ask one question as I have read through the testimony and heard about how the Federal agencies have responded in this case and we will hear more directly from them. What is your experience in terms of agency response--State, local, and Federal in these cases?

DR. COOPER. And that is a very good question. I will tell you that I began my work in child sexual exploitation with the U.S. Postal Inspection Service who has been incredibly excellent with respect to their recognition of child pornography as it is ordered online and delivered through the mail. They are very, very proactive and very hardworking group of people. The Internet Crimes Against Children's

Task Forces which are present in almost every State now usually will have a local law enforcement officer representative. For example, in my county in North Carolina, we have one person in our sheriff's department who sits on that team and then we have a State-level investigator who sits on that team, and then a fellow FBI-type investigator and then a customs individual. So I interact pretty regularly with each one of these individuals in a team standpoint whenever there is a new case. My role is to analyze the images and to make sure that they meet the definition of the law. I would say that they work very well together but they are not enough, clearly not enough individuals. Law enforcement training needs to be a continuously funded phenomenon. I speak in probably 10, at least 10 to 12 trainings a year in the United States that are all law enforcement trainings all about sexual exploitation online predators. So I think that funding for that continued education is going to be very important.

MR. WALDEN. All right, thank you very much. I would yield back.

We again appreciate your rescheduling and your testimony and the good work you do around the country.

DR. COOPER. Thank you, sir.

MR. WHITFIELD. Thank you, Mr. Walden.

And I will recognize the gentleman from New Jersey for 10 minutes. Mr. Ferguson.

MR. FERGUSON. Thank you, Mr. Chairman.

Dr. Cooper is there a link between being in possession of child pornography and actually assaulting a child?

DR. COOPER. Yes, sir, there is. That has been studied now in three different venues. The U.S. Postal Inspection Service first looked at that and found that in 35 percent of the cases that they had investigated there was also evidence of a contact offense having already occurred. The Toronto Child Sexual Exploitation Police Unit also looked at this question and nearly one out of two, 35 percent of their cases were also minimum contact offenses. Then of course the Federal Bureau of Prisons has looked at it from a different perspective. These are already incarcerated child pornographers who are in sexual treatment programs. In that particular situation where individuals are in therapy and will acknowledge under that umbrella whether or not they have or have not sexually abused children. Close to 76 percent of those individuals acknowledged that they had already sexually abused children at the time, by the time they were collecting child pornography. So we feel that there is definitely a link between collecting child pornography and offending against children. Sadly for me as a forensic pediatrician, now that I see younger children in my clinic, I am beginning to see children who are telling me about their victimization and I have seen what they are telling

me on the Internet. So I know that the aspect of a plan of action, the Internet providing a plan of action for offenders is clearly becoming evident.

MR. FERGUSON. So the evidence suggests that there is a link. Do we have an idea of that causality?

DR. COOPER. Yes. That we believe and what the research out of Ireland showed when the applied psychologist went into the prison system and this would be Taylor and Quail who go in the prison system to talk to convicted pornographers. The most important causality is that seeing child pornography makes would be offenders believe that this is acceptable behavior, that it is normal and that normal people do it. So, therefore, the normalization of sexual harm is what encourages them to proceed.

MR. FERGUSON. So with all of the images that are available online, with all of the material that is out there, I mean, are we creating child predators with the availability and the ease with which one can access child pornography, these exploitative images, this material? Are we, because that is so easily available, are we creating people who exploit and abuse children?

DR. COOPER. That is a very good question and I will tell you that there are reports of individuals who have nearly sexually offended against a child, who after beginning to see many of these images on the Internet, develop that kind of distortion that this is a common practice, and who may have fantasized, but never acted on a child and now are beginning to because of what they have seen on the Internet.

MR. FERGUSON. Those are all the questions I have. Thank you, Dr. Cooper, I yield back.

DR. COOPER. Thank you.

MR. WHITFIELD. Thank you very much, Mr. Ferguson.

And Dr. Cooper, we generally appreciate your being here today and as we said a couple times before rearranging your schedule, your testimony is certainly very important and your professional insights will be quite helpful to us.

DR. COOPER. Thank you.

MR. WHITFIELD. And we hope that we can stay in touch with you as we move forward on this issue.

DR. COOPER. And sir, if I may, I would like to be sure to leave a copy of our textbook and our CD-ROM with you for your use if it can be of any benefit.

MR. WHITFIELD. Thank you very much and we appreciate your being here.

At this time, I would like to call the second panel of witnesses. First, we have Mr. Justin Berry who is with us today. He was the topic of a



number of articles in the New York Times about how a 13-year-old young man becomes involved in this sordid online world. Justin, if you would have a seat. And then also we have Mr. Kurt Eichenwald who is a reporter with the New York Times. I am going to ask unanimous consent that we enter into the record five articles in the New York Times that Mr. Eichenwald wrote on this subject, as well as a speech that he gave at Marquette University. The title of the first article is "Through His Webcam a Boy Joins a Sordid Online World." The second one was "Where the Credit Card Trail leads." The third, "A Shadowy Trade Migrates Through the Web." Fourth, "Documenting a Crime That Thrives on Anonymity." Fifth, "Making a Connection with Justin," and then the speech at Marquette University.

[The information follows:]



December 19, 2005

## Through His Webcam, a Boy Joins a Sordid Online World

By **KURT EICHENWALD**

The 13-year-old boy sat in his California home, eyes fixed on a computer screen. He had never run with the popular crowd and long ago had turned to the Internet for the friends he craved. But on this day, Justin Berry's fascination with cyberspace would change his life.

Weeks before, Justin had hooked up a Web camera to his computer, hoping to use it to meet other teenagers online. Instead, he heard only from men who chatted with him by instant message as they watched his image on the Internet. To Justin, they seemed just like friends, ready with compliments and always offering gifts.

Now, on an afternoon in 2000, one member of his audience sent a proposal: he would pay Justin \$50 to sit bare-chested in front of his Webcam for three minutes. The man explained that Justin could receive the money instantly and helped him open an account on PayPal.com, an online payment system.

"I figured, I took off my shirt at the pool for nothing," he said recently. "So, I was kind of like, what's the difference?"

Justin removed his T-shirt. The men watching him oozed compliments.

So began the secret life of a teenager who was lured into selling images of his body on the Internet over the course of five years. From the seduction that began that day, this soccer-playing honor roll student was drawn into performing in front of the Webcam - undressing, showering, masturbating and even having sex - for an audience of more than 1,500 people who paid him, over the years, hundreds of thousands of dollars.

Justin's dark coming-of-age story is a collateral effect of recent technological advances. Minors, often under the online tutelage of adults, are opening for-pay pornography sites featuring their own images sent onto the Internet by inexpensive Webcams. And they perform from the privacy of home, while parents are nearby, beyond their children's closed bedroom doors.

The business has created youthful Internet pornography stars - with nicknames like Riotboy, Miss Honey and Gigglez - whose images are traded online long after their sites have vanished. In this world, adolescents announce schedules of their next masturbation for customers who pay fees for the performance or monthly subscription charges. Eager customers can even buy "private shows," in which teenagers sexually perform while following real-time instructions.

A six-month investigation by The New York Times into this corner of the Internet found that such sites had emerged largely without attracting the attention of law enforcement or youth protection organizations. While experts with these groups said they had witnessed a recent deluge of illicit, self-

generated Webcam images, they had not known of the evolution of sites where minors sold images of themselves for money.

"We've been aware of the use of the Webcam and its potential use by exploiters," said Ernest E. Allen, chief executive of the National Center for Missing and Exploited Children, a private group. "But this is a variation on a theme that we haven't seen. It's unbelievable."

Minors who run these sites find their anonymity amusing, joking that their customers may be the only adults who know of their activities. It is, in the words of one teenage site operator, the "Webcam Matrix," a reference to the movie in which a computerized world exists without the knowledge of most of humanity.

In this virtual universe, adults hunt for minors on legitimate sites used by Webcam owners who post contact information in hopes of attracting friends. If children respond to messages, adults spend time "grooming" them - with praise, attention and gifts - before seeking to persuade them to film themselves pornographically.

The lure is the prospect of easy money. Many teenagers solicit "donations," request gifts through sites like Amazon.com or negotiate payments, while a smaller number charge monthly fees. But there are other beneficiaries, including businesses, some witting and some unwitting, that provide services to the sites like Web hosting and payment processing.

Not all victims profit, with some children ending up as pornographic commodities inadvertently, even unknowingly. Adolescents have appeared naked on their Webcams as a joke, or as presents for boyfriends or girlfriends, only to have their images posted on for-pay pornography sites. One Web site proclaims that it features 140,000 images of "adolescents in cute panties exposing themselves on their teen Webcams."

Entry into this side of cyberspace is simplicity itself. Webcams cost as little as \$20, and the number of them being used has mushroomed to 15 million, according to IDC, an industry consulting group. At the same time, instant messaging programs have become ubiquitous, and high-speed connections, allowing for rapid image transmission, are common.

The scale of Webcam child pornography is unknown, because it is new and extremely secretive. One online portal that advertises for-pay Webcam sites, many of them pornographic, lists at least 585 sites created by teenagers, internal site records show. At one computer bulletin board for adults attracted to adolescents, a review of postings over the course of a week revealed Webcam image postings of at least 98 minors.

The Times inquiry has already resulted in a large-scale criminal investigation. In June, The Times located Justin Berry, then 18. In interviews, Justin revealed the existence of a group of more than 1,500 men who paid for his online images, as well as evidence that other identifiable children as young as 13 were being actively exploited.

In a series of meetings, The Times persuaded Justin to abandon his business and, to protect other children at risk, assisted him in contacting the Justice Department. Arrests and indictments of adults he identified as pornography producers and traffickers began in September. Investigators are also focusing on businesses, including credit card processors that have aided illegal sites. Anyone who has created, distributed, marketed, possessed or paid to view such pornography is open to a criminal charge.

"The fact that we are getting so many potential targets, people who knowingly bought into a child pornographic Web site, could lead to hundreds of other subjects and potentially save hundreds of other kids that we are not aware of yet," said Monique Winkis, a special agent with the Federal Bureau of Investigation who is working the case.

Law enforcement officials also said that, with the cooperation of Justin, they had obtained a rare guide into this secluded online world whose story illuminates the exploitation that takes place there.

"I didn't want these people to hurt any more kids," Justin said recently of his decision to become a federal witness. "I didn't want anyone else to live the life I lived."

#### **A High-Tech Transformation**

Not long ago, the distribution of child pornography in America was a smallish trade, relegated to back rooms and corners where even the proprietors of X-rated bookstores refused to loiter.

By the mid-1980's, however, technology had transformed the business, with pedophiles going online to communicate anonymously and post images through rudimentary bulletin board systems. As Internet use boomed in the 1990's, these adults honed their computer skills, finding advanced ways to meet online and swap illegal photos; images once hard to obtain were suddenly available with the click of a mouse.

As the decade drew to a close, according to experts and records of online conversations, these adults began openly fantasizing of the day they would be able to reach out to children directly, through instant messaging and live video, to obtain the pornography they desired.

Their dream was realized with the Web camera, which transformed online pornography the way the automobile changed transportation. At first, the cameras, some priced at more than \$100, offered little more than grainy snapshots, "refreshed" a few times per minute. But it was not long before easy-to-use \$20 Webcams could transmit high-quality continuous color video across the globe instantly.

By 2000, things had worked out exactly the way the pedophiles hoped. Webcams were the rage among computer-savvy minors, creating a bountiful selection of potential targets.

Among them was Justin Berry. That year, he was a gangly 13-year-old with saucer eyes and brown hair that he often dyed blond. He lived with his mother, stepfather and younger sister in Bakersfield, Calif., a midsize city about 90 miles north of Los Angeles. Already he was so adept at the computer that he had registered his own small Web site development business, which he ran from the desk where he did his schoolwork.

So Justin was fascinated when a friend showed off the free Webcam he had received for joining Earthlink, an Internet service provider. The device was simple and elegant. As Justin remembers it, he quickly signed up, too, eager for his own Webcam.

"I didn't really have a lot of friends," he recalled, "and I thought having a Webcam might help me make some new ones online, maybe even meet some girls my age."

As soon as Justin hooked the camera to his bedroom computer and loaded the software, his picture was automatically posted on spotlife.com, an Internet directory of Webcam users, along with his contact information. Then he waited to hear from other teenagers.

No one Justin's age ever contacted him from that listing. But within minutes he heard from his first online predator. That man was soon followed by another, then another.

Justin remembers his earliest communications with these men as nonthreatening, pleasant encounters. There were some oddities - men who pretended to be teenage girls, only to slip up and reveal the truth later - but Justin enjoyed his online community.

His new friends were generous. One explained how to put together a "wish list" on Amazon.com, where Justin could ask for anything, including computer equipment, toys, music CD's or movies. Anyone who knew his wish-list name - Justin Camboy - could buy him a gift. Amazon delivered the presents without revealing his address to the buyers.

The men also filled an emotional void in Justin's life. His relationship with his father, Knute Berry, was troubled. His parents divorced when he was young; afterward, police records show, there were instances of reported abuse. On one occasion Mr. Berry was arrested and charged with slamming Justin's head into a wall, causing an injury that required seven staples in his scalp. Although Justin testified against him, Mr. Berry said the injury was an accident and was acquitted. He declined to comment in a telephone interview.

The emotional turmoil left Justin longing for paternal affection, family members said. And the adult males he met online offered just that. "They complimented me all the time," Justin said. "They told me I was smart, they told me I was handsome."

In that, experts said, the eighth-grade boy's experience reflected the standard methods used by predatory adults to insinuate themselves into the lives of minors they meet online.

"In these cases, there are problems in their own lives that make them predisposed to" manipulation by adults, Lawrence Likar, a former F.B.I. supervisor, said of children persuaded to pose for pornography. "The predators know that and are able to tap into these problems and offer what appear to be solutions."

Justin's mother, Karen Page, said she sensed nothing out of the ordinary. Her son seemed to be just a boy talented with computers who enjoyed speaking to friends online. The Webcam, as she saw it, was just another device that would improve her son's computer skills, and maybe even help him on his Web site development business.

"Everything I ever heard was that children should be exposed to computers and given every opportunity to learn from them," Ms. Page said in an interview.

She never guessed that one of her son's first lessons after turning on his Webcam was that adults would eagerly pay him just to disrobe a little.

#### **The Instant Audience**

It was as if the news shot around the Web. By appearing on camera bare-chested, Justin sent an important message: here was a boy who would do things for money.

Gradually the requests became bolder, the cash offers larger: More than \$100 for Justin to pose in his underwear. Even more if the boxers came down. The latest request was always just slightly beyond the last, so that each new step never struck him as considerably different. How could adults be so organized at manipulating young people with Webcams?

Unknown to Justin, they honed their persuasive skills by discussing strategy online, sharing advice on how to induce their young targets to go further at each stage.

Moreover, these adults are often people adept at manipulating teenagers. In its investigation, The Times obtained the names and credit card information for the 1,500 people who paid Justin to perform on camera, and analyzed the backgrounds of 300 of them nationwide. A majority of the sample consisted of doctors and lawyers, businessmen and teachers, many of whom work with children on a daily basis.

Not long ago, adults sexually attracted to children were largely isolated from one another. But the Internet has created a virtual community where they can readily communicate and reinforce their feelings, experts said. Indeed, the messages they send among themselves provide not only self-justification, but also often blame minors with Webcam sites for offering temptation.

"These kids are the ones being manipulative," wrote an adult who called himself Upandc in a posting this year to a bulletin board for adults attracted to children.

Or, as an adult who called himself DLW wrote: "Did a sexual predator MAKE them make a site? No. Did they decide to do it for themselves? Yes."

Tempting as it may be for some in society to hold the adolescent Webcam operators responsible, experts in the field say that is misguided, because it fails to recognize the control that adults exercise over highly impressionable minors.

"The world will want to blame the kids, but the reality is, they are victims here," said Mr. Allen of the National Center for Missing and Exploited Children.

But there is no doubt that the minors cash in on their own exploitation. With Justin, for example, the road to cyberporn stardom was paved with cool new equipment. When his growing legion of fans complained about the quality of his Webcam, he put top-rated cameras and computer gear on his Amazon wish list, and his fans rushed to buy him all of it.

A \$35 Asante four-port hub, which allowed for the use of multiple cameras, was bought by someone calling himself Wesley Taylor, Amazon receipts show. For \$45, a fan nicknamed tuckertheboy bought a Viking memory upgrade to speed up Justin's broadcast. And then there were cameras - a \$60 color Webcam by Hawking Technologies from banjo000; a \$60 Intel Deluxe USB camera from boyking12; and a \$150 Hewlett-Packard camera from eplayermine.

Justin's desk became a high-tech playhouse. To avoid suspicions, he hid the Webcams behind his desk until nighttime. Whenever his mother asked about his new technology and money, Justin told her they were fruits of his Web site development business. In a way, it was true; with one fan's help, he had by then opened his own pornographic Web site, called justinscam.com.

His mother saw little evidence of a boy in trouble. Justin's grades stayed good - mostly A's and B's, although his school attendance declined as he faked illness to spend time with his Webcam.

As he grew familiar with the online underground, Justin learned he was not alone in the business. Other teenagers were doing the same things, taking advantage of an Internet infrastructure of support that was perfectly suited to illicit business.

As a result, while it helped to have Justin's computer skills, even minors who fumbled with technology

could operate successful pornography businesses. Yahoo, America Online and MSN were starting to offer free instant message services that contained embedded ability to transmit video, with no expertise required. The programs were offered online, without parental controls. No telltale credit card numbers or other identifying information was necessary. In minutes, any adolescent could have a video and text system up and running, without anyone knowing, a fact that concerns some law enforcement officials.

There were also credit card processing services that handled payments without requiring tax identification numbers. There were companies that helped stream live video onto the Internet - including one in Indiana that offered the service at no charge if the company president could watch free. And there were sites - portals, in the Web vernacular - that took paid advertising from teenage Webcam addresses and allowed fans to vote for their favorites.

Teenagers, hungry for praise, compete for rankings on the portals as desperately as contestants on TV reality shows, offering special performances in exchange for votes. "Everyone please vote me a 10 on my cam site," a girl nicknamed Thunderrockracin told her subscribers in 2002, "and I will have a live sleep cam!"

In other words, she would let members watch her sleep if they boosted her up the rankings.

#### **Fearing the Fans**

Justin began to feel he belonged to something important, a broad community of teenagers with their own businesses. Some he knew by their real names, others by the screen names they used for their sites - Strider, Stoner, Kitty, Calvin, Emily, Seth and so on. But collectively, they were known by a name now commonplace in this Internet subculture:

They call themselves "camwhores."

Justin chatted with the boys online, and sometimes persuaded the girls to masturbate on camera while he did the same. Often, he heard himself compared to Riotboy, another young-looking teenager whose site had experienced as many as 6,400 hits in a single week.

In conversations with Justin, other minors with for-pay sites admitted to being scared of certain fans. Some adults wrote things like "It wants to possess you." They had special wardrobe requests for the adolescents: in jeans with a belt, without a belt, with a lacy bra, showing legs, showing feet, wearing boxers with an erection, and others.

One 16-year-old who called himself hot boy 23 finally found the entreaties too much. "Hey guys," he wrote when he shut down his site, "I'm sorry, there are just too many freaks out there for me. I need to live a more normal life, too. I might be back someday and I might not. I'm sorry I had to ruin all the fun."

It was not only the minors operating Webcam sites for pay who faced frightening adults. Earlier this year, a teenage girl in Alabama posed seminude on her Webcam in a sexually charged conversation with someone she thought was another teenage girl. But her new confidant, it turned out, was an adult named Julio Bardales from Napa, Calif., law enforcement officials said. And when the girl stopped complying, she received an e-mail message from Mr. Bardales containing a montage of her images. Across them was a threat in red letters that the images would be revealed unless she showed a frontal nude shot over the Webcam. Mr. Bardales was subsequently arrested. The police said he possessed images of more under-age girls on Webcams, including other montages with the same threat.

Justin says that he did not fully understand the dangers his fans posed, and before he turned 14, he was first lured from the relative safety of his home. A man he met online hosted Justin's Web site from Ann Arbor, Mich., and invited him there to attend a computer camp. Justin's mother allowed him to go, thinking the camp sounded worthwhile.

Another time, the man enticed Justin to Michigan by promising to arrange for him to have sex with a girl. Both times, Justin said, the man molested him. Transcripts of their subsequent conversations online support the accusations, and a video viewed by The Times shows that the man, who appears for a short time in the recording, also taped pornography of Justin.

From then on, Justin's personality took on a harder edge, evident in the numerous instant messages he made available to The Times. He became an aggressive negotiator of prices for his performances. Emboldened by a growing contempt for his audience, he would sometimes leave their questions unanswered for hours, just to prove to himself that they would wait for him.

"These people had no lives," Justin said. "They would never get mad."

Unnerved by menacing messages from a fan of his first site, Justin opened a new one called jfwy.com, an online acronym that loosely translates into "just messing with you." This time, following an idea suggested by one of his fans, he charged subscribers \$45 a month. In addition, he could command large individual payments for private shows, sometimes \$300 for an hourlong performance.

"What's in the hour?" inquired a subscriber named Gran0Stan in one typical exchange in 2002. "What do you do?"

"I'll do everything, if you know what I mean," Justin replied.

Gran0Stan was eager to watch, and said the price was fine. "When?" he asked.

"Tonight," Justin said. "After my mom goes to sleep."

As his obsession with the business grew, Justin became a ferocious competitor. When another under-age site operator called Strider ranked higher on a popular portal, Justin sent him anonymous e-mail messages, threatening to pass along images from Strider's site to the boy's father. The site disappeared.

"I was vicious," Justin said. "But I guess I really did Strider a favor. Looking back, I wish someone had done that to me."

By then, fans had begun offering Justin cash to meet. Gilo Tunno, a former Intel employee, gave him thousands of dollars to visit him in a Las Vegas hotel, according to financial records and other documents. There, Justin said, Mr. Tunno began a series of molestings. At least one assault was videotaped and the recording e-mailed to Justin, who has since turned it over to the F.B.I.

Mr. Tunno played another critical role in Justin's business, the records show. When he was 15, Justin worried that his mother might discover what he was doing. So he asked Mr. Tunno to sign an apartment lease for him and pay rent. Justin promised to raise money to pay a share. "I'll whore," he explained in a message to Mr. Tunno.

Mr. Tunno agreed, signing a lease for \$410 a month for an apartment just down the street from Justin's house. From then on, Justin would tell his mother he was visiting friends, then head to the apartment for



his next performance. Mr. Tunno, who remains under investigation in the case, is serving an eight-year federal sentence on an unrelated sexual abuse charge involving a child and could not be reached for comment.

The rental symbolized a problem that Justin had not foreseen: his adult fans would do almost anything to ensure that his performances continued. At its worst, they would stand between him and the people in his offline life whom they saw as a threat to his Webcam appearances.

For example, when a girlfriend of Justin's tried to convince him to shut down his site in December 2002, a customer heaped scorn on her.

"She actually gets mad at you for buying her things with the money you make from the cam?" messaged the customer, a man using the nickname Angelaa. "Just try and remember, Justin, that she may not love you, but most of us in your chat room, your friends, love you very much."

#### **A Life Falls Apart**

In early 2003, Justin's offline life began to unravel. A former classmate found pornographic videos on the Internet from Justin's Web site, made copies and handed them out around town, including to students at his school. Justin was taunted and beaten.

Feeling embarrassed and unable to continue at school, Justin begged his mother to allow him to be home-schooled through an online program. Knowing he was having trouble with classmates, but in the dark about the reasons why, she agreed.

Then, in February, came another traumatic event. Justin had begun speaking with his father, hoping to repair their relationship. But that month, Mr. Berry, who had been charged with insurance fraud related to massage clinics he ran, disappeared without a word.

Despairing, Justin turned to his online fans. "My dad left. I guess he doesn't love me," he wrote. "Why did I let him back in my life? Let me die, just let me die."

His father did not disappear for long. Soon, Mr. Berry called his son from Mazatlán, Mexico; Justin begged to join him, and his father agreed.

In Mexico, Justin freely spent his cash, leading his father to ask where the money had come from. Justin said that he confessed the details of his lucrative Webcam business, and that the reunion soon became a collaboration. Justin created a new Web site, calling it mexicofriends, his most ambitious ever. It featured Justin having live sex with prostitutes. During some of Justin's sexual encounters, a traffic tracker on his site showed hundreds watching. It rapidly became a wildly popular Webcam pornography site, making Justin one of the Internet's most sought after under-age pornography stars.

For this site, Justin, then 16, used a pricing model favored by legitimate businesses. For standard subscribers, the cost was \$35, billed monthly. But discounts were available for three-month, six-month and annual memberships. Justin used the cash to support a growing cocaine and marijuana habit.

Money from the business, Justin said, was shared with his father, an accusation supported by transcripts of their later instant message conversations. In exchange, Justin told prosecutors and The Times, his father helped procure prostitutes. One video obtained by the F.B.I. shows Mr. Berry sitting with Justin as the camera is turned on, then making the bed before a prostitute arrives to engage in intercourse with

his teenage son. Asked about Justin's accusations, Mr. Berry said, "Obviously, I am not going to comment on anything."

In the fall of 2003, Justin's life took a new turn when a subscriber named Greg Mitchel, a 36-year-old fast food restaurant manager from Dublin, Va., struck up an online friendship with the boy and soon asked to visit him. Seeing a chance to generate cash, Justin agreed.

Mr. Mitchel arrived that October, and while in Mexico, molested Justin for what would be the first of many times, according to transcripts of their conversations and other evidence. Mr. Mitchel, who is in jail awaiting trial on six child pornography charges stemming from this case, could not be reached for comment.

Over the following year, Justin tried repeatedly to break free of this life. He roamed the United States. He contemplated suicide. For a time he sought solace in a return to his boyhood Christianity. At one point he dismantled his site, loading it instead with Biblical teachings - and taking delight in knowing the surprise his subscribers would experience when they logged on to watch him have sex.

But his drug craving, and the need for money to satisfy it, was always there. Soon, Mr. Mitchel beckoned, urging Justin to return to pornography and offering to be his business partner. With Mr. Mitchel, records and interviews show, Justin created a new Web site, justinsfriends.com, featuring performances by him and other boys he helped recruit. But as videos featuring other minors appeared on his site, Justin felt torn, knowing that these adolescents were on the path that had hurt him so badly.

Justin was now 18, a legal adult. He had crossed the line from under-age victim to adult perpetrator.

#### **A Look Behind the Secrecy**

In June, Justin began communicating online with someone who had never messaged him before. The conversations involved many questions, and Justin feared his new contact might be an F.B.I. agent. Still, when a meeting was suggested, Justin agreed. He says part of him hoped he would be arrested, putting an end to the life he was leading.

They met in Los Angeles, and Justin learned that the man was this reporter, who wanted to discuss the world of Webcam pornography with him. After some hesitation, Justin agreed. At one point, asked what he wanted to accomplish in his life, Justin pondered for a moment and replied that he wanted to make his mother and grandmother proud of him.

The next day, Justin began showing the inner workings of his online world. Using a laptop computer, he signed on to the Internet and was quickly bombarded with messages from men urging him to turn on his Webcam and strip.

One man described, without prompting, what he remembered seeing of Justin's genitals during a show. Another asked Justin to recount the furthest distance he had ever ejaculated. Still another offered an unsolicited description of the sexual acts he would perform on Justin if they met.

"This guy is really a pervert," Justin said. "He kind of scares me."

As the sexual pleadings continued, Justin's hands trembled. His pale face dampened with perspiration. For a moment he tried to seem tough, but the protective facade did not last. He turned off the computer without a final word to his online audience.

associate in Tennessee sent word that the F.B.I. had just raided a Los Angeles computer server used by an affiliated Webcam site. Then, to Mr. Mitchel's surprise, Justin himself appeared online under a new screen name and sent a greeting.

Mr. Mitchel pleaded with Justin to come out of hiding, inviting the teenager on an all-expense-paid trip to Las Vegas with him and a 15-year-old boy also involved in Webcam pornography. But Justin demurred.

"You act like you're in witness protection," Mr. Mitchel typed. "Are you?"

"Haha," Justin replied. Did Mr. Mitchel think he would be on the Internet if he was a federal witness? he asked. Justin changed the subject, later asking the whereabouts of others who lived with Mr. Mitchel, including two adolescents; Mr. Mitchel replied that everyone was home that night.

In a location in the Southwest, Justin glanced from his computer screen to a speakerphone. On the line was a team of F.B.I. agents who at that moment were pulling several cars into Mr. Mitchel's driveway, preparing to arrest him.

"The kids are in the house!" Justin shouted into the phone, answering a question posed by one of the agents.

As agents approached the house, Justin knew he had little time left. He decided to confront the man who had hurt him for so long.

"Do you even remember how many times you stuck your hand down my pants?" he typed.

Mr. Mitchel responded that many bad things had happened, but he wanted to regain Justin's trust.

"You molested me," Justin replied. "Don't apologize for what you can't admit."

There was no response. "Peekaboo?" Justin typed.

On the screen, a message appeared that Mr. Mitchel had signed off. The arrest was over.

Justin thrust his hands into the air. "Yes!" he shouted.

In the weeks since the first arrest, F.B.I. agents and prosecutors have focused on numerous other potential defendants. For example, Tim Richards, identified by Justin as a marketer and principal of justinsfriends.com, was arrested in Nashville last month and arraigned on child pornography charges. According to law enforcement officials, Mr. Richards was stopped in a moving van in his driveway, accompanied by a young teenage boy featured by Mr. Richards on his own Webcam site. Mr. Richards has pleaded not guilty.

Hundreds of thousands of computer files, including e-mail containing a vast array of illegal images sent among adults, have been seized from around the country. Information about Justin's members has been downloaded by the F.B.I. from Neova.net, the company that processed the credit cards; Neova and its owner, Aaron Brown, are targets of the investigation, according to court records and government officials. And Justin has begun assisting agents with Immigration and Customs Enforcement, who hope to use his evidence to bring new charges against an imprisoned child rapist.

associate in Tennessee sent word that the F.B.I. had just raided a Los Angeles computer server used by an affiliated Webcam site. Then, to Mr. Mitchel's surprise, Justin himself appeared online under a new screen name and sent a greeting.

Mr. Mitchel pleaded with Justin to come out of hiding, inviting the teenager on an all-expense-paid trip to Las Vegas with him and a 15-year-old boy also involved in Webcam pornography. But Justin demurred.

"You act like you're in witness protection," Mr. Mitchel typed. "Are you?"

"Haha," Justin replied. Did Mr. Mitchel think he would be on the Internet if he was a federal witness? he asked. Justin changed the subject, later asking the whereabouts of others who lived with Mr. Mitchel, including two adolescents; Mr. Mitchel replied that everyone was home that night.

In a location in the Southwest, Justin glanced from his computer screen to a speakerphone. On the line was a team of F.B.I. agents who at that moment were pulling several cars into Mr. Mitchel's driveway, preparing to arrest him.

"The kids are in the house!" Justin shouted into the phone, answering a question posed by one of the agents.

As agents approached the house, Justin knew he had little time left. He decided to confront the man who had hurt him for so long.

"Do you even remember how many times you stuck your hand down my pants?" he typed.

Mr. Mitchel responded that many bad things had happened, but he wanted to regain Justin's trust.

"You molested me," Justin replied. "Don't apologize for what you can't admit."

There was no response. "Peekaboo?" Justin typed.

On the screen, a message appeared that Mr. Mitchel had signed off. The arrest was over.

Justin thrust his hands into the air. "Yes!" he shouted.

In the weeks since the first arrest, F.B.I. agents and prosecutors have focused on numerous other potential defendants. For example, Tim Richards, identified by Justin as a marketer and principal of justinsfriends.com, was arrested in Nashville last month and arraigned on child pornography charges. According to law enforcement officials, Mr. Richards was stopped in a moving van in his driveway, accompanied by a young teenage boy featured by Mr. Richards on his own Webcam site. Mr. Richards has pleaded not guilty.

Hundreds of thousands of computer files, including e-mail containing a vast array of illegal images sent among adults, have been seized from around the country. Information about Justin's members has been downloaded by the F.B.I. from Neova.net, the company that processed the credit cards; Neova and its owner, Aaron Brown, are targets of the investigation, according to court records and government officials. And Justin has begun assisting agents with Immigration and Customs Enforcement, who hope to use his evidence to bring new charges against an imprisoned child rapist.

Justin himself has found a measure of control over his life. He revealed the details of his secret life to his family, telling them of all the times in the past that he had lied to them. He has sought counseling, kept off drugs, resumed his connection with his church and plans to attend college beginning in January.

In recent weeks, Justin returned to his mother's home in California, fearing that - once his story was public - he might not be able to do so easily. On their final day together, Justin's mother drove him to the airport. Hugging him as they said goodbye, she said that the son she once knew had finally returned.

Then, as tears welled in her eyes, Justin's mother told him that she and his grandmother were proud of him.

**The New York Times**  
nytimes.com

---

December 19, 2005  
The Customers

## Where the Credit Card Trail Leads

By KURT EICHENWALD

For almost six years, a little-known Internet company called Neova.net has been quietly processing credit card information for online businesses - among them, Justin Berry and other minors who operate for-pay Webcam sites.

Tracking down the company is challenging. Its Web site is just black-and-blue text on a white background, with little hint of the scope of its business. Its contact information shows it in London, but corporate records list its main offices in Boston, at an address for a private mailbox provider. And its server, the powerful computer that handles transactions and stores the business data electronically, is in California, Internet records show.

Just days after his decision to abandon his pornography business, Justin Berry accessed his operating account at Neova, downloaded the data of his for-pay Webcam site - including the names and credit card information of people who subscribed to his site - and provided it to The New York Times. Until then, Justin had never before known what kind of people paid to see an underage boy film himself in sexual situations.

"I really didn't want to know who they were," he said.

The names numbered more than 1,750; about 200, however, were customers who had signed up multiple times. The Times reduced the listing to a sampling of 300 people in eight cities and attempted to identify the adults who were paying to view child pornography.

In the analysis, The Times cross-referenced the names and locations of subscribers with publicly available records. Often, a name was traced to a company or organization through the subscriber's e-mail address. Subscribers whose identities were not clear, based on public information, were not counted in the sample.

Because of the possibility that some people whose information was on the list may have been victims of identity theft, and to guard the privacy of individuals, The Times is not publishing the names of adults whose credit card payments for Justin's sites were processed by Neova. The company and its principal, however, are targets of a federal investigation into online child pornography, according to court records and government officials; its customer records have been independently obtained by the government.

The detailed personal information accompanying the accounts indicates that virtually all of the customers subscribed using their real names. And the level of chargebacks - reversed payments that occur when customers dispute charges to their credit cards - was relatively low for the accounts, indicating that these subscriptions had in fact been ordered by the cardholders.

The analysis found that few of the subscribers fit the stereotype of online predators as people on the fringes of society. Instead, they included successful members of communities across the country, people whose education and language skills could help them win the trust of underage teenagers.

Of the 300 subscribers to Justin's site whose identities were checked, a large percentage were in professions that placed them in the proximity of children on almost a daily basis. There were pediatricians and elementary school teachers, as well as lawyers who represent children in court. But there were also subscribers whose careers seemed unrelated to children, including a public official in the West and the president of a privately held construction company who used his corporate credit card to sign up for the site.

Experts in the field of child sexual exploitation said such findings - particularly the prominence of adults having careers that placed them near children - were consistent with anecdotal evidence from law enforcement.

"These people go into these professions, like teacher and pediatrician, to get themselves close to kids," said Patrick A. Trueman, the former head of the Child Exploitation and Obscenity Section of the Justice Department, who is now senior research counsel for the Family Research Council, a Christian conservative organization that promotes policies on marriage and family. "Their desires drive their careers."

Neova.net is not the only online company whose computer records contain the names and identifying information of people paying for child pornography; other large payment processors have had such sites as their customers. In some instances, the processors are legitimate corporations that unwittingly play a role in its dissemination.

A pornographic Web site called bigfunhouse, for example, was dependent on a global Internet payment processing company for handling its credit card billings.

For years, bigfunhouse - which portrayed itself as the most popular site of its kind in America and Europe - offered to members a free link to a second site featuring Webcam videos of boys who were lured into one or two online sexual performances, according to Internet records and customers interviewed by The Times.

E-mail traffic reviewed by The Times showed that, in June, the company that processed credit card charges for bigfunhouse - Verotel, which is based in Amsterdam - received a message purportedly from a teenager whose image was on the site; the message stated that bigfunhouse was carrying child pornography. Verotel - one of the largest credit card processors for Web sites offering digital content, which says it is strongly committed to combating child pornography - replied that it had investigated the claim and had become convinced that it was not true, the e-mail messages showed.

In November, The Times asked Verotel about illegal images, and the company responded that there were none on the bigfunhouse site. The Times provided Verotel with specific information about illegal images, including the identities of people who had been arrested for possessing the material. Verotel severed its relationship with bigfunhouse. Within hours, the pornography site shut down.

The bigfunhouse Web site then changed its message to "Game over. We closed."

**The New York Times**  
nytimes.com

December 19, 2005  
The History

## A Shadowy Trade Migrates to the Web

By KURT EICHENWALD

In the last few decades, technology has transformed the world of child pornography. The business was severely hampered in the late 1970's, after Congress adopted the first federal law specifically prohibiting child pornography. It became illegal to use minors below the age of 16 in pornographic films and photographs; by 1984, the law was expanded to children under 18.

The crackdown slowed what had been a flood of child pornography to a comparative trickle. Pedophiles in the United States became dependent on video material created overseas or on Polaroid snapshots. But that required locating other adults with similar predilections - almost all of whom, studies show, are men - through personal advertisements in magazines, increasing the probability of being caught.

"In that day and age it was a lot harder to distribute child pornography," said Brad Russ, the director of training and technical assistance for many federally financed law enforcement units dealing with Internet crimes against children. "You were very vulnerable to detection."

The popularity of online communications, starting slowly in the 1980's and expanding rapidly in the 1990's, made possible, for the first time, anonymous gatherings of people with sexual attractions to children.

The result, experts said, was the creation of a virtual community of pedophiles who reinforced each others' beliefs that their feelings were no longer beyond the outer reaches of social norms.

"The Internet has let these people tell themselves that there are a host of others out there just like them," said Michelle Collins, the head of the exploited children unit with the National Center for Missing and Exploited Children, a private organization that works closely with law enforcement and other government agencies.

Soon, child pornography was being swapped and collected online with the vigor and obsession usually found among baseball card enthusiasts. Certain children - whose true identities were unknown - emerged as online stars. Helena, a girl of about eight, was featured in hardcore pornography that included images of her sexual encounters with a young boy, Gavin. By early 2000, experts said, the most desired images were the KG and KX series, hundreds of pornographic pictures of girls from what experts believe was a European kindergarten in sexual encounters with adult men.

But the sudden bounty of child pornography online did nothing to sate the desire of pedophiles. Instead, supply fueled a demand for more, for better, for more explicit - and videos replaced still pictures. As the 1990's drew to an end, law enforcement was just becoming aware of the technological skills of this adult subculture.



"Back in 2000, they were discussing instant messaging as the next step, one that wouldn't leave the tracks that are left on the Internet," said Philip Jenkins, a history professor at Penn State who spent that year tracking pedophile conversations online for his book, "Beyond Tolerance: Child Pornography on the Internet." "And they would talk about kids making the pornography themselves. That was the dream."

The flood of Webcams and their use by young people has created a law enforcement challenge, officials said, impeding efforts to find predators online. In the old days, police and federal agents would pose online as teenagers and arrest the adults who attempted to entice them into sexual situations. But now, law enforcement officials involved in such online impersonations said, it is common for an adult to demand that a teenager turn on a Webcam after the first few minutes of conversation. Police cannot use real children to lure wrongdoers, and they cannot broadcast underage pornographic images. That has left law enforcement officials having to make excuses for why they do not have a Webcam.

"Whenever we say the Webcam is broken or we don't own one," one law enforcement official said, speaking on condition of anonymity, "they just move on, looking for the next kid."



December 19, 2005

## Documenting a Crime That Thrives on Anonymity

KURT EICHENWALD

Reporting about child pornography on the Internet presents complicated journalistic and legal issues, both in gathering the information and in doing so while not violating laws against possession of such images.

In reporting this series, The New York Times interviewed boys and girls who were operating Webcam sites, as well as adult customers, law enforcement officials and experts on child safety.

Some minors contacted on the Internet declined to reveal their identities or locations, but guided The Times to sites where their customers posted messages. In each instance, The Times encouraged the youths to shut their sites, speak with their parents or seek counseling.

To verify information received from minors and found online, The Times obtained an array of documents, including copies of online conversations and e-mail messages between minors and adult admirers; records of payments to minors; membership lists from Webcam sites that charge fees; and information about companies that facilitate their operation. The Times also examined sites maintained by children and adults, and defunct sites stored in online archives.

To confirm Justin Berry's story, The Times reviewed and obtained access to thousands of pages of evidence, including files he retained on his computer over several years, original documents, financial records, credit card processing data and other information. The paper also interviewed members of his family and people he knew at various stages of his life.

Decisions in the reporting were reviewed with Times lawyers to ensure legal compliance. While it was occasionally necessary to review offensive images, The Times avoided downloading child pornography or independently subscribing to sites containing such material. In each instance that The Times located illegal images on the Internet, information about them was provided to law enforcement officials.

[Copyright 2005 The New York Times Company](#) | [Home](#) | [Privacy Policy](#) | [Search](#) | [Corrections](#) | [XML](#) | [Help](#) | [Cont](#)

**The New York Times**  
nytimes.com

---

December 19, 2005  
Reporter's Essay

## Making a Connection With Justin

By KURT EICHENWALD

My reporting on Webcam pornography began inadvertently last May, when an online search for financial fraud cases led to an odd posting describing what was said to be an international criminal investigation of a group of Web companies.

Searching for clues about that inquiry took me on a trail to other sites and posted messages. Eventually, I came across entries about someone named Justin, who, based on what I read, seemed to be an adult pornography star. Perplexed about how he was linked to a fraud case, I searched further at archive.org, which keeps copies of old Web sites, and discovered a photograph of a boy who appeared to be about 14 years old.

This, supposedly, was Justin - not an adult, but a child.

The original posting about the investigation proved to be a fake, and the more postings I read about Justin, including hundreds on a Yahoo message board set up by his fans, the more I came to suspect that his lurid story might also be an Internet fable. But I wanted to be sure.

Eventually, I found a lead: a screen name for Justin, which I could use to send him an instant message. My first attempts failed; Justin later said that he blocked these messages because the nature of my questions convinced him that I was with law enforcement.

The only way to know if Justin was real, I decided, was to meet him in person. And to do that, I had to win the confidence of whoever was answering to his screen name. At The Times, it is standard practice for a reporter to identify himself at the outset, but doing that too soon would mean I might never know the truth. I decided to try to engage this person in conversation and persuade him to meet with me. At that time, I would disclose my identity and only then would I begin the real reporting that could be used in an article.

I contacted Justin again; this time, I mimicked the tone of the members of the Yahoo site, simply identifying myself as a fan. From there began an off-and-on, online conversation that went on for weeks, mostly about the music that I write as a hobby; Justin assumed that that was my career, and I did not try hard to dissuade him.

Soon thereafter, I proposed meeting in Los Angeles, and Justin agreed. My wife, Theresa, whom I had kept abreast of what was happening, worried that this could be a setup, and made me promise to take precautions. I did, but when I saw Justin at the airport, I was reassured. Although he was 18, he looked much younger and did not seem physically capable of harming me.

I immediately identified myself as a Times reporter, and Justin, though taken aback, continued to speak

to me; for more than an hour, we discussed my background, until he was willing to proceed. Over the next two days, I interviewed the person I now knew was Justin Berry. By then, I was aware that Justin was addicted to cocaine and marijuana. With no expectation that he would agree, I asked him to stop. I also urged Justin to quit responding to messages from his adult admirers. Justin agreed to both requests.

Today, he has a simple explanation for why he listened so readily. "I didn't want to die," he said. "The things I was involved in were horrible, but I could never find a way out. I wanted for it all to end so badly, so I was ready to do anything."

Days after the initial meeting, Justin called, sounding terribly upset. A man was visiting him who, I believed from our interview, had molested Justin in the past and had provided him drugs to keep him compliant. Given the situation, Times editors agreed to fly Justin from Bakersfield, Calif., to Dallas, where I could interview him while he worked through his drug withdrawal.

After arriving, Justin angrily told of molestations at the hands of multiple men since he was a young teenager. He took me inside his online world, showing corners of the Internet where predators spoke among themselves.

Justin's physical condition was weak, and with the approval of my editors I introduced him to a doctor. He was suffering both from malnutrition and a mild venereal disease. His eardrums were irreparably damaged from years of untreated infections. Scars, from what appeared to be a whipping, were found on his back, although Justin could not remember who or what caused them.

Withdrawal - coupled with the trauma of recounting his experiences - worsened his emotional state. Justin often became terrified in public places, convinced that men he saw might be either members of his site or people working with his former business partners. He would burst unexpectedly into tears. At my suggestion, Justin agreed to seek counseling.

As his emotional and physical health improved, Justin said he would fully cooperate with a story about self-generated child pornography on the Internet, allowing The Times to print his name. My editors and I decided to delay accepting his offer, however, until we were certain that Justin was competent to make the decision, something that would only be accomplished if he continued his recovery from drugs.

Justin disclosed the names of other children at risk, and told of a trove of evidence about his online pornography business: computer hard drives, kept at his mother's home in California, that contained years of financial data, including records of client payment, saved online conversations and other information.

Editors agreed that The Times needed to review the evidence to verify Justin's story; if it supported what he said, The Times would attempt to persuade him to contact law enforcement. Though the role of journalists is to report news rather than report illegal activity to law enforcement, in this instance The Times decided it was important that authorities learn what Justin knew so that they could take any steps needed to protect the children he said were still at risk.

We flew to California and I examined the hard drives. The review convinced me that Justin's story was true. I connected him with a lawyer - Stephen M. Ryan with Manatt, Phelps & Phillips - who agreed to represent him and who contacted prosecutors. Two weeks later, at Justin's request, I accompanied him to Washington for his first meeting with the government. By then, someone I contacted had offered to give Justin a place to live, and after his interview, he headed to that new location.

Today, Justin Berry is a different young man from the sickly and troubled person who showed up in Los Angeles. He has gained 10 pounds and stayed off drugs, while continuing with his counseling sessions. And recently, on his second try, he passed the entrance exams required for the college he plans to attend starting in January.

Justin now speaks of using the lessons of his life to help other children in trouble. He has hopes of being able to use his experiences to inform both parents and teenagers of the dangers on the Internet, while at the same time working hard on his continued recovery from his lost years online.

Excerpt of Kurt Eichenwald, Marquette University, Burleigh Ethics Lecture, March 29, 2006

...The decision to convince a source to become a federal witness created an array of other ethical issues, some of which were foreseeable, some of which definitely were not. In talking to my editors, it was clear that there an almost certain probability that we would witness a performance by the Justice Department that would be spectacular, but it would be one that would have very little relationship to their real performance in a criminal case. They would know that we were there, they would know that we'd been involved in this case from the beginning. So we had to be very careful not to fall into a portrayal of "Look how aggressive and strong and wonderful the Justice Department was." We understood that our presentation of their actions was going to have to be cautious. Our presence was going to effect the story, and we had to be careful to be aware of that.

We shouldn't have worried. To our amazement, what emerged instead was a display of abject, utter incompetence by the Justice Department's Child Exploitation and Obscenity Section, or CEOS. In no time, both the performance of CEOS and my ongoing interviews with government officials made clear that this critical division of the federal effort to combat child sex abuse suffered from horrifically poor leadership, which was widely viewed within law enforcement circles as an arrogant impediment to the successful prosecution of such cases.

In the course of my reporting in the months that followed, law enforcement officials told me that CEOS would make arguments against criminal prosecutions that would make a defense lawyer blush; That is actually a quote from a cop. I was told of specific cases where local police had to cut out CEOS in order to successfully pursue the

bad guys, instead going hat-in-hand to individual US Attorney's offices to get the job done. The most stunning moment was when I telephoned a former Justice Department official who worked with two Republican Administrations, and mentioned that I wanted to discuss the current chief of CEOS. With no further prompting, this former official replied, "He should be fired." I have never experienced a moment like that in two decades of reporting at the Times.

Now, please understand, I don't walk into this situation as some starry-eyed idealist, with unrealistic expectations of how a criminal case should work. I am fascinated by law enforcement, I have a deep affection for what they do, and I have been on the inside enough to recognize the personnel, bureaucratic and professional issues that can lead to difficulty. But what I was witnessing at CEOS went far beyond anything I had ever experienced....

When CEOS was contacted by Steve Ryan on July 14, we had come off of our horrific week. A letter was sent, or a contact was made, CEOS was told that Justin was being hunted, that his life was in danger, they were told that other children were in danger, they were told that evidence was being destroyed....CEOS was told the situation was urgent and needed immediate attention by law enforcement.

And then nothing happened. Days passed. Finally, Justin's lawyer, Mr. Ryan, was informed that CEOS needed him to prepare a written "proffer," which would describe in some detail the information Justin could provide to the government. That is not an unreasonable request. The proffer was written and delivered within a few hours. And then more days passed. Finally, CEOS announced that the prosecutors would not meet with Justin until he or his lawyer decided which US Attorney's office had

jurisdiction over the case. Now the concept that they had approached CEOS for the purpose of prosecuting did not seem to enter the minds of anyone in CEOS. Arguments were presented that *every* office had jurisdiction, since this was a 50 state case; that was rejected by CEOS. “Tell us which U.S. Attorney has jurisdiction or we won’t meet with you.”

I got a phone call and Ryan told me about this, and he said, “Well, who do you think?” It was almost a joke. I suggested that we pick the US Attorney’s office in Baltimore, since then CEOS couldn’t come back and say “We have to arrange air travel, it is going to take another few weeks.” Plus, the FBI has its innocent images group in Maryland, they would be right there, they work on child pornography. That was conveyed to CEOS; despite the critical importance given this supposed issue, the Baltimore’s US Attorney’s office was never brought into this case.

It became obvious – no matter how urgent the situation, no matter how many times CEOS was told that the witness’s life was in danger, no matter how many times they were told of other children in peril, no matter how many times they were told about evidence being destructed –they would not act with any exigency. This presented critical issues for me as a journalist. Did I need to rush a story – as weak and under-reported as it was at that point – into the paper? Did the unusual circumstances I found myself in require for *The Times* to act on behalf of children in danger? Did we need to do a story that there was a witness, a quick knockoff story? I didn’t know. And if we did do a story, would we place those children – who were in the clutches of adults exploiting them – in immediate danger? Could the children end up being harmed by us reporting what the government wasn’t doing. It was an impossible situation.



A decision was made. Justin and I would go to Washington on July 25 and July 26. CEOS would be notified ahead of time that their witness was coming in town. If they wanted to meet with him, they could. If not, the next step for me was to move full-speed at getting a weaker version of the story about kids in danger into the paper. CEOS was notified by Steve Ryan on July 22 that he would be in town for those two days, after which he would approach other state law enforcement officials. At the last minute, CEOS agreed to a meeting. The FBI agents on the case were literally rounded up at the last minute, informed of the case on the morning of July 25, 11 days after CEOS was first notified of this horrible series of events taking place....

The interviews unfolded over the following two days. While I was not in the room, I saw Justin periodically during that time. He was traumatized, he was going through drug withdrawal, he was exhibiting signs of paranoia, and was simply overwhelmed by everything that was happening to him. I worried about whether he would actually remember to specify the information about the kids in danger. I worried that the prosecutors might not be bright enough to ask the questions. I knew that I needed to be sure. So, once the meeting was over, before everyone left the room, I walked in and said, "I want to make sure certain details have not been lost in this flurry of information." I then proceeded to name the children in danger, give their locations, and describe – specifically – the Internet addresses that Justin had showed me that would prove these minors were being sexually exploited by adults. I was, perhaps, crossing a line, but I told them nothing other than the information that the Times wanted conveyed, which was the reason we had entered into this unusual situation.

But there was another side of it. Part of me also wanted to be sure that no one could ever argue that CEOS was not told this critical information. I was very glad I did so weeks later, when a Justice Department official – for what would be the first of many times – told me in explaining away the government’s abject failure in this case that CEOS had never been told all of the information that had, in fact, been repeated by me.

I was not the only one who underscored certain information. In my presence, Justin’s lawyer, Steve Ryan, a former federal prosecutor who took on mob families, stressed that one individual in the criminal conspiracy laid out by Justin was the “hub” of the entire enterprise, while Justin was merely a spoke. This “hub,” who processed credit cards for sites like Justin’s, could potentially lead not only to more sites, but more crimes and more customers. This person was deep inside the business infrastructure, much deeper than Justin, and could lead prosecutors in directions that Justin knew nothing about. Mr. Ryan said that any prosecutor worth his salt would use Justin’s information to immediately go after the hub. No such effort was undertaken.

Instead, weeks passed in silence. I now know from other reporting, involving an array of sources both inside and outside the government, that CEOS bungled even the most basic elements of the criminal investigation. Requests for subpoenas for financial records from investigating agents lay dormant on prosecutors’ desks for weeks, slowing the inquiry to a crawl. Information in Justin’s possession, which Mr. Ryan would not allow to be turned over until his client received immunity, went uncollected, with prosecutors saying they could not make a ruling on the immunity request until the US Attorney’s offices in locations where Justin committed crimes signed off on the deal. Throughout the month of August, Ryan was told no one was available to sign off on the

deal in those two US Attorney's offices, because prosecutors were on vacation. It was not until months later I was told that, in fact, the calls to at least one of those prosecutors' offices was not placed until September – and indeed, one of them may never have been called. Meanwhile, CEOS kept sending out signals that Justin, the person who stepped forward, might well be the only person indicted because of his actions in his final few weeks in the business, because of his decision to help lure other kids into pornography. This saber-rattling appeared to me at the time to be either a sign of abject incompetence or an attempt to actually drive Justin into fleeing the country, a possibility that was never far from being realized...

By early September, more than 50 days had passed with no sign of progress. The children we knew to be in danger were still in danger. In the time since Justin had come to Dallas, I had seen videos of these kids posted on the sites. Justin was going out of his mind, as was I. Justin suggested to his lawyer that he would plead guilty, just to get the immunity issue out of the way, if prosecutors would simply rescue the children in danger; Ryan talked him out of that idea.

I was in a position, as a journalist, of not knowing what to do once again. Every day I worried: Were the kids being harmed while CEOS dithered? What in the world was going on? What was my responsibility as a journalist? I was not yet ready for the large scale story. I had a lot of reporting left to do...

But there also was a looming deadline. As Justin had told CEOS, one of the predators who had molested him was planning to take a 15 year old boy in mid-September on a trip to Las Vegas – the very type of trip that had been used in the past when Justin was abused. None of us ever imagined that, with mid-September fast

approaching, that boy would still be in danger. I began to wonder – at what point could we be deemed to have responsibility for whatever happened to that boy, given what we knew? I called my editor and told him of my concern. His conclusion was simple: We needed to commit some journalism. While the webcam story still had a long way to go, we could crash a story into the paper about CEOS's failure to act on information from a witness.

I began making calls, first contacting the former head of CEOS to be sure what I was witnessing could not, somehow, explainable. I was assured it was not. From there, over the Labor Day weekend, I began gathering string. But apparently, I also made waves. Before the weekend was out, someone I interviewed contacted an official in the Justice Department. That information was passed on to the office of the head of the criminal division. Tuesday morning, the day after labor day, my phone rang first thing. My first two calls were from people in the Justice Department: What, they asked, was I up to? All hell was breaking loose, I was told.

At that point, one Justice Department official contacted me and began explaining how difficult it was to make decisions on issues of immunity. I replied that immunity was up to them, I had no stake in that issue. The official continued by asking the rhetorical question: what would the mother of one of the other minors that Justin helped recruit into pornography in his final days in the business think if she found out that Justin had been given immunity? I replied, "I don't know. What's she going to think when she finds out that you guys left her son in the hands of the adult sex offender who filmed the pornography for more than fifty days?" There was a lengthy, uncomfortable pause. The official said he needed to check into what was really going on.

Within 24 hours, Justin Berry's lawyer was notified that he would receive immunity. The all-important sign off from the US Attorney in Virginia came the next day, after a hastily arranged conference call with Justin. Everything seemed ready to go. I had no idea that the incompetence I had witnessed had only just begun. Over the next few days, there was a breakdown between the Justice Department and the FBI as CEOS struggled to take charge of the suddenly-high-profile case. At one point, things became so bad that the FBI – albeit temporarily – stopped cooperating with the prosecutors in CEOS. This, while the children are still in danger.

The following Monday, I received a telephone call from Justin's lawyer. The government was desperately hunting for their new witness, and couldn't find him. They needed his help for a takedown, an arrest that was about to happen. Did I know where he was?

Luckily, I did. And I was stunned at this opportunity. If I played my cards right, I would be able to witness the takedown of a major participant in these crimes – at least seeing it from Justin's side. I left my office and drove to a place I believed Justin was, and he was there. From there, I gave him a ride while he called his lawyer; the CEOS prosecutors wanted him to go immediately to the FBI office in Dallas, where he would place a call to the home of the man they were about to arrest. That way, they could be sure the man was home before they arrived.

Justin reacted very badly to this, and very logically. He had never called that man before on his home phone, ever. Doing so would be an automatic tipoff that something was up. He had disappeared for months now, and suddenly, he is calling the man on a phone he had never called before. Worse, this was also one of the men who Justin had

identified as one of his molesters. He was not comfortable with the instructions that he was going to have to engage in having long-term idle banter with a man who had sexually abused him. But CEOS insisted.

We set off for the FBI office. Before we traveled even a mile, Justin's cell phone rang. It was the FBI, ordering Justin to ignore the instructions from CEOS. They feared, just as Justin had warned, that such a call would place the target on notice. Justin agreed, and telephoned his lawyer about the development. Five minutes later, the lawyer called back: The head of CEOS reversed the order again, insisting that Justin immediately go and place the phone call – the one that the FBI said could wreck the case. If Justin did not do so, CEOS made clear he would be deemed as having violated the cooperation provisions of his immunity agreement.

The reversals continued. FBI, CEOS, CEOS, FBI. I gave up and pulled into a sandwich shop. Justin told his lawyer to let the two sides straighten it out. We ate. Not long afterwards, Justin received a call from the FBI: they were in charge. But they wanted him to get online, as fast as possible, and have a conversation with the target by instant message. The arrest was about to happen. By that point, we were far from the place where Justin had his computer set up. There was only one place we could go to do this: my office. My gamble paid off...I got to be there as the takedown took place. That scene is portrayed in the story.

Finally, it seemed, things were getting better. Then two days later, I received a telephone call on my cell phone from Justin, at about 5 o'clock in the morning. He didn't even bother to say hello. "Are they trying to get me killed?" he asked.

A new and horrific problem had emerged. The previous day, contrary to any level of logic and reasoning, the affidavit in support of the arrest warrant of the first target was unsealed by the government. It revealed everything – potential defendants, the role of the primary witness, everything but Justin’s name. And if you didn’t happen to stumble across that document in the court file, you didn’t have to worry: The US Attorney for the Western District of Virginia gave a statement to the press about it. The story was written up in the newspaper and posted on the Internet. Anyone looking into the arrest of the individual who was part of the criminal conspiracy could know with a click of a button that the witness against him was Justin Berry.

That day, CEOS called Justin’s lawyer, apologizing profusely for the latest blunder and offered to do anything to help him feel safe. Justin had one suggestion, which he offered up to his lawyer: “Tell them to stop being so stupid.”

By the time we reached the end of this line of missteps, incompetence and miscommunication, I was eager to portray it in the paper. But there was an issue. I had my ethics protections in place. Each time I wrote about what had happened, my reviewers came back and said, it sounded too much like we were attacking CEOS for blowing the case we gave them. I tried to broaden the piece, only to find that I was losing the underlying story about webcam pornography in an effort to tell what had happened at the Justice Department. We made a simple decision: We would let the facts speak for themselves. We would tell about more than 50 days of inaction. That would convey to readers everything they needed to know.

MR. WHITFIELD. I might also add that in my opening statement, I talked about Mr. Eichenwald being so disturbed and interested in this issue that he came to testify, but I would like to set the record straight that we did subpoena Mr. Eichenwald because he is a reporter and so we appreciate him complying with our subpoena and being here in response to that. We also have Mr. Steve Ryan with us today who is an attorney with Manatt, Phelps & Phillips, and it is my understanding, Mr. Berry, that he, Mr. Ryan, is representing you and acting as your legal counsel. Is that correct?

MR. BERRY. Yes, sir.

MR. WHITFIELD. Okay. And as you all know, this is an Oversight and Investigations hearing and we do take testimony under oath. Do either of you have any difficulty or object to testifying under oath? Now, Mr. Eichenwald, do you have legal counsel with you today?

MR. EICHENWALD. I do, sir.

MR. WHITFIELD. And would you identify him?

MR. EICHENWALD. He is David McCall, the gentleman behind me who is the counsel for the New York Times.

MR. WHITFIELD. Okay, and Mr. David McCall who is the legal counsel with the New York Times, we appreciate your being here, Mr. McCall. Now, I understand you are not going to be testifying. Mr. Ryan may actually testify depending on how the questions go.

[Witnesses sworn]

MR. WHITFIELD. Thank you, all of you are sworn in now and I will recognize Mr. Justin Berry for his opening statement. And Justin, we do appreciate your being here today. We know it has been a difficult road for you and your being willing to testify can be a tremendous help to many young people throughout the country and also to the committee as we search for ways to deal with this issue so thank you.

**TESTIMONY OF JUSTIN BERRY, C/O STEPHEN M. RYAN,  
ESQ., MANATT, PHELPS & PHILLIPS LLP; AND KURT  
EICHENWALD, REPORTER, THE NEW YORK TIMES**

MR. BERRY. Thank you. Chairman Whitfield, Ranking Member Mr. Stupak, and other members of the committee, my name is Justin Berry and I am 19 years old. I am here to speak upon the danger facing this Nation's children, one that threatens not only their emotional health, but their physical safety. This danger is Internet child pornography, particularly involving the use of inexpensive web cameras which are used by adult predators to exploit children.

I speak from experience. For 5 years, beginning when I was 13 years old, I operated a pornographic website featuring images of myself fluttered on the Internet by webcams. I was paid by more than 1,000 men to strip naked, masturbate, and even have sex with female prostitutes while on camera. My business was assisted by adult criminals, including companies that process credit card payments.

I am not proud of the things I have done nor will I personally attempt to avoid responsibility for those decisions. While I did not comprehend the magnitude of what was happening when I was 13, as I grew older, I progressively became corrupted and acted in shameful ways. Still, I repeatedly attempted to pull away from this sick business, but each time I



fell back into this criminal world that had first seduced me and eventually controlled me.

My experience is not as isolated as you may hope. This is not the story of a few bad kids whose parents paid no attention. There are hundreds of kids in the United States alone who are right now wrapped up in this horror. Within each of your congressional districts, I guarantee there are children who have used their webcams to appear naked online, and I guarantee you there are also children in your district on the Internet right now being contacted and seduced by online sexual predators. I was an honor student and I was class president. My mom had used all the latest child protective software. She checked what was happening in my room. She occasionally took away my computer keyboard but she was no match for the child predators who worked hard to make sure my child porn shows continued.

In my personal opinion, the law enforcement effort is no match for them either. Until recently, I never understood why these child predators always laughed about the Government. Now, I know that the child predators are at least partially right. They have little to fear from law enforcement. Based on my case, efforts to prosecute these people are riddled with mistakes and bureaucracy. Unless something changes, hundreds or even thousands of children will be lost forever.

I obtained a webcam at 13 after signing up for an account with earthlink.net. The company, as a promotion, sent me a free Logitech webcam. As a child drawn to computers, I was enthralled. I plugged the device into my computer and then followed the instructions on the software. Within minutes my webcam image was loaded onto a website called spotlife.com.

Like many young teenagers, I hoped my webcam would improve my social life. I did not have a lot of friends and I was very lonely. I hoped the webcam would help me meet other teenagers online and hopefully a few girls my age. That never happened. No teenager out of the webcam pornography business ever contacted me but I did hear from my child predators. Within minutes of appearing on spotlife, I received an instant message from an adult male. This man I now know was a child predator. I did not understand at that time.

More child predators followed. Looking back today, my thoughts seem foolish but at 13, I believed these people were my friends. They were kind. They complimented me. They wanted to know about my day, and they were endlessly patient in listening to me, and they were generous. In no time, one of these men told me he wanted to send me a gift. He showed me how to set up a wish list on Amazon.com which allowed everyone who knew my code name to send me a present without requiring me to disclose my address. Soon I was swamped with videos,

CDs, and computer equipment including better webcams all free from my new friends. I always rushed back from school to scoop of the packages that were on my doorstep before my mother got home from work.

My new friends were kinder and more generous to me than anyone I had ever known. I trusted them, and that is when everything changed. One afternoon, a few weeks after setting up my webcam, one of these men approached me online with a proposal. He would pay me \$50 if I took off my shirt for a few minutes while sitting in front of my webcam. He explained to me how to set up an account on Paypal.com, an instant online money payment system. I was excited about the \$50, an amount that struck me at the time was a huge sum of money. Taking off my shirt seemed harmless, I did it at the pool. The money arrived and I took off my shirt. My viewers complimented me and it felt good.

The weeks that followed are a blur, but I now understand that by removing my shirt, I had signaled that I could be manipulated. More gifts and money arrived along with increasingly explicit requests. They wanted me to take off my pants, remove my underwear, and eventually masturbate on camera. The seduction was slow. Each request only went a bit further than the last and the horror of what was happening did not strike me at that time.

I wish I could say I hated what was happening. Perhaps that would absolve some of my sense of guilt. But the truth is I did not. As more clothes came off, more people contacted me. The compliments were endless, the gifts and payments terrific. I thought I had achieved online what eluded me in real life. I was popular. Everyone wanted to know my thoughts. Everyone wanted to give me things. I was the king of my own universe. All I had to do in exchange was strip and masturbate while alone in my room.

Men began to reach out to me. One man, Ken Gourlay approached me online to discuss my interest in computers. He operated his own web hosting company called Chain Communications. I was awed. Here was someone running a real Internet business, talking to me, a 13-year-old kid and treating me as an equal. In the months that followed, Ken raised the possibility of hiring me at Chain as an executive director of sales and marketing. It seemed like a dream come true.

As I was working for him, Ken recommended that I attend elite computer camp at the University of Michigan where I could obtain advance certifications. My mother agreed to send me there that summer while I was still 13. At that time, I thought it was just luck that Ken and Chain were both based in Ann Arbor, Michigan. I now know that I had been set up. Ken picked me up at camp one day to show me Chain and

he took me to his home where I was sexually molested by Ken for what proved to be first and many times by him and other adult men.

With the help of my family and my psychologist, I know understand that my molestation by Ken was the turning point that sent me on a path to self-destruction. Afterwards, Ken apologized, promising me it would never happen again, but it did.

By this time, I had formalized my webcam business. I had opened a site called justinscam.com, where child predators could come and watch, and offer me money and gifts to do what they wanted. After my first molestation, I began to act out sexually. I was reckless. Part of me wanted to die. And every day on camera, part of me did.

The next stage emerged with the help once again of Ken Gourlay. I decided I should sell monthly memberships for a new site jfwy.com. Ken offered to set up the membership section and host the business at Chain. People could now, using the site programmed by Ken, pay me a monthly membership fee through Paypal and watch all they wanted.

Another computer executive, Gilo Tunno, was one of my members. He had been an engineer at Intel and a principal designer of the Pentium 4 processor. I was so impressed. So when Gilo Tunno told me he wanted to hang out with me in Bakersfield, California where I lived and bring me presents, I agreed. I met him and we went to his hotel. At some point, he gave me a \$1,500 projector and other gifts. We talked about Intel and computers. And then he molested me.

I look back on those events with Gourlay and Tunno and feel ashamed. All of my explanations seem inadequate. How could I get myself into that situation? How could I not see it? But this is one of the issues I wish to stress. Webcams and instant messaging give predators power over children. The predators become part of that child's life. Whatever warnings the child may have heard about meeting strangers, these people are no longer strangers. They have every advantage. It is the standard seduction of child predators multiplied on a geometric scale.

I no longer cared about anything other than getting as much money as possible. When another teenager in my town found the videos from my website and distributed them to my classmates, I felt compelled to leave. My father lived in Mexico. I wanted to establish a relationship with him. My mother said I could visit him for a week.

My week-long visit to Mexico was extended again and again. At one point, my father asked where all my money was coming from. I told him about my business and he offered in his words to help maximize the earning potential. I had already established a new site called mexicofriends.com which featured me engaging in sex with Mexican women. My father helped by hiring prostitutes for me to have sex with

on camera. The number of members, of paid members skyrocketed. I was 16 years old.

I became even more self-destructive. I abused marijuana terribly and consumed so much cocaine that I am amazed I survived. My life was a swirl of drugs, money, and sex. When a paying member of my site, Greg Mitchel, offered to come to Mexico and pay me gifts, I accepted. He, too, sexually molested me. But I no longer cared, I just wanted his money. I had become exactly what my members viewed me to be, what their degrading conversations convinced me I was: a piece of meat for sale to the highest bidder.

Just after my 18<sup>th</sup> birthday I tried to leave the business. Money was still coming in from mexicofriends but I wanted nothing to do with it. I used it to purchase clothes and other items for homeless people in California. I rented a truck and delivered the materials myself. I was looking for my own redemption but I failed. I was still addicted to drugs and Greg Mitchel urged me to return to the business as his partner. Together, he said, we could set up a new website, justinsfriends.com. I resisted for months, but I could not find my way in the real world anymore. Depressed and high on drugs every day, I agreed to return to porn. The site was fully operational in June of 2005.

That same month, I met Kurt Eichenwald, a New York Times reporter who was working on a story about webcam pornography. He urged me to quit drugs and get out of the business and I did. He asked for my help in exposing this world and I agreed. When I told him of the other children who were being exploited and molested by adult men, he convinced me it was important to tell law enforcement what I knew. I agreed even though I feared this meant that I could be sent to prison. I believed that the Government would protect the children being abused. I believed they would act quickly. I was wrong.

My lawyer, Stephen Ryan of Manatt, Phelps & Phillips, a former Federal prosecutor, contacted prosecutors of the Department of Justice and was put in touch with the Child Exploitation and Obscenity Section on July 14, 2005. He informed them that the adults I had worked with suspected I was seeking out law enforcement. He told them my life was potentially in danger and that evidence was being destroyed. He provided the DOJ with a written proffer of my testimony and described the physical evidence of IP addresses, credit card information, and other proof I could make available. Mr. Ryan insisted that DOJ provide me with immunity for the testimony to protect me. He was confident they would respond promptly. Mr. Ryan was wrong also.

Almost 2 weeks passed. Finally, we informed the Child Exploitation and Obscenity Section that I was flying to Washington, not at government expense, and would be available to meet with them for 2

days, July 25 and July 26. At almost the last minute, CEOS scheduled the meeting.

In our meetings, I identified children who were currently being exploited and molested, as well as other men who were committing the crimes. I identified the adult child molesters such as Mr. Mitchel, Mr. Tunno, and others. I told of the Internet locations where evidence of these crimes could be found. I informed them that I had names, credit card numbers, IP addresses of approximately 1,500 people who paid to watch child pornography from my websites and identified the businessmen, the adult businessmen who facilitated the credit card payments necessary for these business. The FBI case agents I spoke with were very professional and of the highest integrity. I cannot say enough good things about them. The Child Exploitation and Obscenity Section did not make me confident.

Weeks passed seemingly without progress. I cannot describe the agony of that time. Each night I wondered were the children I knew being molested that night? Were they being filmed? Why was no one stopping this? I understood it would take time to decide whether I should have immunity or not, but why couldn't they rescue the children in danger?

In late August, my lawyer informed CEOS in writing that if they did not act, he would take me elsewhere to get State law enforcement officials to begin the work on the matter. Mr. Ryan began discussions with the California Attorney General Lockyer, whose staff agreed to consider taking the case. Also at that time, I believe the New York Times was preparing a story about the Government's failure to do anything about my case. I remember Kurt asking me what I would tell other cam kids who wanted to disclose their ring of predators to law enforcement. I told Kurt knowing my message would be heard by other kids that no one should ever step forward again. I got the distinct feeling that the CEOS prosecutors did not know what to do with me or my information.

Then, everything changed. It was so sudden that I have come to believe the CEOS feared the New York Times was going to report the delay. Whatever the cause, I was granted immunity. My lawyer turned over the physical evidence. The following week on September 12, 2005, Greg Mitchel was arrested. I expected this to be the first of many prosecutions. Again, I was wrong.

I wish I could say the prosecution story had a happy ending. It did not. At that time, I was concerned I would be killed by the adults who would be harmed by my testimony and were frantically searching for me. After the Mitchel arrest, a sensitive government document was deliberately unsealed from court records. It is my understanding that this

was done by the U.S. Department of Justice. While the names were blacked out, the document clearly identified potential defendants under investigation, as well as the fact that I was a witness against them. Worse, it warned all the adult perpetrators across the country that I was cooperating with law enforcement. The local U.S. Attorney quoted in the newspapers based on the release of the document. All of it appeared on the Internet where the adult perpetrators looking for me could read it.

I feared for my life. CEOS then offered me government protection which I need in part because CEOS or the U.S. Attorney's office had deliberately stopped the release of the affidavit. I declined the offer. I did not trust CEOS to protect me. I feared the actions of CEOS from that day forward although not nearly as much as I feared the anger of the predators.

Today, I have been off drugs for 9 months and just finished my first quarter at college. My grades are good and I have friends.

Had I not met Kurt Eichenwald, I would have never had this chance at a new life. I will never be able to repay what he has done for me. In a profession which is taught to get the story, he did that, but he treated me with the compassion of a Good Samaritan. I have my life back.

Every day, I have regrets, not just for the dreadful decisions I made in the past years but for failing to have the impact that I had hoped on this illegal trade.

I have never been asked by law enforcement about any of the 1,500 names I provided them. Some of those who molested me, like Mr. Gourlay, and who made all of this possible, are continuing to live their lives, unaware or uncaring about any government inquiry. People like Mr. Brown who operate the credit card infrastructure of web cam child pornography have been permitted to continue their work, seemingly undisturbed by any law enforcement effort. I have watched as my former members go online to attack me, boldly proclaiming themselves as my former customers and having no fear that their self-disclosure could result in their arrest. Events have proved them right.

Since I left the child pornography business last summer, I have risked everything to tell these facts to persons who care, like this committee. It is my hope that Congress will do everything it can to see to it that children are protected and that our law enforcement effort is competent to combat this evil. Thank you.

[The prepared statement of Justin Berry follows:]

PREPARED STATEMENT OF JUSTIN BERRY, C/O STEPHEN M. RYAN, ESQ., MANATT, PHELPS  
& PHILLIPS LLP

Chairman Whitfield, Ranking Member Mr. Stupak, and other Members of the Committee.

My name is Justin Berry and I am 19 years old. I am here to speak about a danger facing this nation's children, one that threatens not only their emotional health, but their physical safety. This danger is internet child pornography, particularly involving the use of inexpensive web cameras which are used by adult predators to exploit children.

I speak from experience. For five years, beginning when I was 13 years old, I operated a pornographic website, featuring images of myself loaded onto the internet by webcams. I was paid by more than 1,000 men to strip naked, masturbate and even have sex with female prostitutes while on camera. My business was assisted by adult criminals, including companies that process credit card payments.

I am not proud of the things I have done. Nor will I personally attempt to avoid responsibility for those decisions. While I did not comprehend the magnitude of what was happening when I was 13, as I grew older, I progressively became corrupted and acted in shameful ways. Still, I repeatedly attempted to pull away from this sick business. But, each time, I fell back into this criminal world that had first seduced me, and eventually controlled me.

My experience is not as isolated as you might hope. This is not the story of a few bad kids whose parents paid no attention. There are hundreds of kids in the United States alone who are right now wrapped up in this horror. Within each of your Congressional districts I guarantee there are children who have used their webcams to appear naked online, and I guarantee you there are also children in your district on the Internet right now being contacted and seduced online by sexual predators. I was an honor student, I was class president. My mom used all the latest child protective software. She checked what was happening in my room. She occasionally took away my computer keyboard. But she was no match for the child predators, who worked hard to make sure my child porn shows continued.

In my personal opinion, the law enforcement effort is no match for them either. Until recently, I never understood why these child predators always laughed about the government. Now I know the child predators are at least partially right. They have little to fear from law enforcement. Based on my case, efforts to prosecute these people are riddled with mistakes and bureaucracy. Unless something changes, hundreds, or even thousands, of children will be lost forever.

#### **THE BEGINNING**

I obtained a webcam at 13 after signing up for an account with earthlink.net. The company, as a promotion, sent me a free Logitech webcam. As a child drawn to computers, I was enthralled. I plugged the device into my computer, and then followed the instructions in the software. Within minutes, my webcam image was loaded onto a website called spotlife.com.

Like many young teenagers, I hoped my webcam would improve my social life. I didn't have a lot of friends and I was very lonely. I hoped the webcam would help me meet other teenagers online, maybe even find a few girls my age. That never happened. No teenager outside of those in the webcam pornography business ever contacted me. But, I did hear from many child predators. Within minutes of appearing on spotlife, I received an instant message from an adult male. This man, I now know, was a child predator. I did not understand that at the time.

More child predators followed. Looking back today, my thoughts seem foolish, but at 13, I believed these people were my friends. They were kind. They complimented me. They wanted to know about my day, and were endlessly patient in listening to me.

And they were generous. In no time, one of these men told me he wanted to send a gift. He showed me how to set up a “wish-list” on Amazon.com, which allowed anyone who knew my codename to send me a present, without requiring me to disclose my address. Soon, I was swamped with videos, cd’s and computer equipment – including better webcams – all free from my new friends. I always rushed back from school to scoop up whatever package was on my doorstep, before my mother got home from work.

My new friends were kinder and more generous to me than anyone I had ever known. I trusted them. And that was when everything changed. One afternoon, a few weeks after setting up my webcam, one of these men approached me online with a proposal. He would pay me \$50 if I took off my shirt for a few minutes while sitting in front of my webcam. He explained how to set up an account on Paypal.com – an instant online money payment system. I was excited about the \$50 – an amount that struck me at the time as a huge sum of money. Taking off my shirt seemed harmless; I did it at the pool. The money arrived, and I took off my shirt. My viewers complimented me, and it felt good.

### **BECOMING A PLAYER IN THE WEBCAM PORN INDUSTRY**

The weeks that followed are a blur, but I now understand that, by removing my shirt, I had signaled that I could be manipulated. More gifts and money arrived, along with increasingly explicit requests. They wanted me to take off my pants, remove my underwear, and eventually masturbate on camera. The seduction was slow; each new request went only a bit further than the last, and the horror of what was happening did not strike me at the time.

I wish I could say that I hated what was happening. Perhaps that would absolve some of my sense of guilt. But the truth is, I did not. As more clothes came off, more people contacted me. The compliments were endless, the gifts and payments terrific. I thought I had achieved online what eluded me in real life: I was popular. Everyone wanted to know my thoughts. Everyone wanted to give me things. I was the king of my own universe. All I had to do in exchange was strip, and masturbate, while alone in my room.

Men began to reach out to me. One man, Ken Gourlay, approached me online to discuss my interest in computers. He operated his own web hosting company, called Chain Communications, and I was awed. Here was someone, running a real Internet business, talking to me, a 13-year-old kid, and treating me as an equal. And, in the months that followed, Ken raised the possibility of hiring me at Chain, as executive director of sales and marketing. It seemed like a dream come true.

As I was working for him, Ken recommended that I attend an elite computer camp at the University of Michigan, where I could obtain advanced certifications. My mother agreed to send me there that summer, while I was still 13. At the time, I thought it was just luck that Ken and Chain were based in Ann Arbor. I now know I had been set up. Ken picked me up at camp one day, to show me Chain. He took me to his home. There, I was sexually molested by Ken, for what would prove to be the first of many times by Ken, and other adult men.

With the help of my family and my psychologist, I now understand that my molestation by Ken was a turning point that sent me on a path to self-destruction. Afterwards, Ken apologized, promising me it would never happen again. But it did.

By this time, I had formalized my webcam business. I had opened up a site called justinscam.com, where child predators could come and watch, and offer me money and gifts to do what they wanted. After my first molestation, I began to act out sexually. I was reckless. Part of me wanted to die. And every day on camera, part of me did.



### MEMBERSHIP SITES

The next stage emerged with the help, once again, of Ken Gourlay. I decided that I should sell monthly memberships for a new site, jfwy.com. Ken offered to set up the membership section and host the business at Chain. People could now, using the site programmed by Ken, pay me a monthly fee through Paypal, and watch all they wanted.

Another computer executive, Gilo Tunno, was one of my members. He told me he had been an engineer at Intel and a principal designer of the Pentium 4 processor. I was so impressed. So when Gilo Tunno told me he wanted to hang out with me in Bakersfield, California — where I lived — and bring me presents, I agreed. I met him and we went to his hotel. At some point he gave me a \$1,500 projector and other gifts. We talked about Intel and computers. And then he molested me.

I look back on those events with Gourlay and Tunno and feel ashamed. All my explanations seem inadequate. How could I get myself into that situation? How could I not see it? But this is one issue I wish to stress. Webcams and instant messaging give predators power over children. The predators become part of the child's life. Whatever warnings the child may have heard about meeting strangers, these people are no longer strangers. They have every advantage. It is the standard seduction of child predators, multiplied on a geometric scale.

I no longer cared about anything other than getting as much money as possible. But when another teenager in my town found videos from my website and distributed them to my classmates, I felt compelled to leave. My father lived in Mexico. I wanted to establish a relationship with him. My mother said I could visit him for a week.

### MEXICO

My week long visit to Mexico was extended and extended again. At one point, my father asked where my money came from. I told him about my business. And he offered, in his words, to help “maximize the earnings potential.” I had already established a new site, called mexicofriends.com, which featured me engaging in sex with Mexican women. My father helped by hiring prostitutes for me to have sex with on camera. The number of paid members skyrocketed. I was 16 years old.

I became even more self-destructive. I abused marijuana terribly, and consumed so much cocaine that I am amazed I survived. My life was a swirl of drugs, money and sex. When a paying member of my site, Greg Mitchel, offered to come to Mexico and bring me gifts, I accepted. He, too, sexually molested me. But I no longer cared. I just wanted his money. I had become exactly what my members viewed me to be, what their degrading conversations convinced me I was: a piece of meat, for sale to the highest bidder.

Just after my 18th birthday, I tried to leave the business. Money was still coming in from mexicofriends, but I wanted nothing to do with it. I used it to purchase clothes and other items for homeless people in California. I rented a truck and delivered the materials myself. I was looking for my own redemption. But I failed. I was still addicted to drugs, and Greg Mitchel urged me to return to the business as his partner. Together, he said, we could set up a new website, justinsfriends.com. I resisted for months, but could not find my way anymore in the real world. Depressed and high on drugs every day, I agreed to return to porn. The site was fully operational in June, 2005.

### GETTING OUT

That same month, I met Kurt Eichenwald, a *New York Times* reporter who was working on a story about webcam pornography. He urged me to quit drugs and get out of the business, and I did. He asked for my help in exposing this world, and I agreed. And when I told him of other children who were being exploited and molested by adult men, he convinced me it was important to tell law enforcement what I knew. I agreed, even

though I feared this meant I could be sent to prison. I believed that the government would protect the children being abused. I believed they would act quickly. I was wrong.

My lawyer, Stephen Ryan of Manatt, Phelps & Phillips, a former federal prosecutor, contacted prosecutors of the Department of Justice (“DOJ”) and was put in touch with the Child Exploitation and Obscenity Section (known as “CEOS”) on July 14, 2005. He informed them that the adults I had worked with suspected I was seeking out law enforcement. He told them my life was potentially in danger, and that evidence was being destroyed. He provided DOJ with a written proffer of my testimony, and described the physical evidence of IP addresses, credit card information, and other proof I could make available. Mr. Ryan insisted that DOJ provide me with immunity for my testimony to protect me. He was confident they would respond promptly. Mr. Ryan was wrong also.

Almost two weeks passed. Finally, we informed the Child Exploitation and Obscenity Section that I was flying to Washington, not at government expense, and would be available to meet with them for two days, July 25 and July 26. At almost the last minute, CEOS scheduled the meeting.

In our meetings, I identified children who were currently being exploited and molested, as well as the men who were committing the crimes. I identified the adult child molesters such as Mr. Mitchel, Mr. Tunno, and others. I told of the Internet locations where evidence of these crimes could be found. I informed them I had the names, credit card number and computer IP addresses of approximately 1,500 people who paid to watch child pornography from my sites, and identified the adult businessmen who facilitated the credit card payments necessary for these businesses. The FBI case agents I spoke with were professional and of the highest integrity. I cannot say enough good things about them. But the Child Exploitation and Obscenity Section did not make me confident.

Weeks passed, seemingly without progress. I cannot describe the agony of that time. Each night I wondered, were the children I knew being molested that night? Were they being filmed? Why was no one stopping this? I understood it would take time to decide whether I should have immunity. But why couldn’t they rescue children still in danger?

In late August, my lawyer informed CEOS, in writing, that if they did not act, he would take me elsewhere to get state law enforcement officials to begin work on the matter. Mr. Ryan began discussions with California Attorney General Lockyer, whose staff agreed to consider taking the case. Also, at that time, I believe the *New York Times* was preparing a story about the government’s failure to do anything about my case. I remember Kurt asking me what I would tell other camkids who wanted to disclose *their* ring of predators to law enforcement. I told Kurt, knowing my message would be heard by other kids, that no one should ever step forward again. I got the distinct feeling that the CEOS prosecutors did not know what to do with me or my information.

Then, everything changed. It was so sudden that I have come to believe the CEOS feared that the *New York Times* was going to report the delay. But whatever the cause, I was granted immunity. My lawyer turned over the physical evidence. The following week, on September 12, 2005, Greg Mitchel was arrested. I expected this to be the first of many prosecutions. Again, I was wrong.

I wish I could say the prosecution story had a happy ending. It did not. At that time, I was concerned I would be killed by the adults who would be harmed by my testimony and who were frantically searching for me. After the Mitchel arrest, a sensitive government document was deliberately unsealed from court records. It is my understanding this was done by the U.S. Department of Justice. While names were blacked out, the document clearly identified potential defendants under investigation, as well as the fact that I was the witness against them. Worse, it warned all the adult perpetrators across the country I was cooperating with law enforcement. The local U.S.

Attorney was quoted in the newspapers, based on the release of the document. And all of it appeared on the Internet, where the adult perpetrators looking for me could read it.

I feared for my life. CEOS then offered me government protection, which I needed, in part, because CEOS or the U.S. Attorney's Office had deliberately sought the release of the Affidavit. I declined their offer. I do not trust CEOS to protect me. I feared the actions of CEOS from that day forward, although not nearly as much as I feared the anger of the predators.

### CONCLUSION

Today, I've been off drugs for nine months, and just finished my first quarter at college. My grades are good, and I have friends.

Had I not met Kurt Eichenwald, I would never have had this chance at a new life. I will never be able to repay what he has done for me. In a profession which is taught to "get the story," he did that, but he treated me with the compassion of the Good Samaritan. I have my life back.

But every day, I have regrets, not just for the dreadful decisions I made in past years, but for failing to have the impact I had hoped on this illegal trade.

I have never been asked by law enforcement about any of the 1,500 names I provided them. Some of those who molested me, like Mr. Gourlay, and who made all of this possible, are continuing to live their lives, unaware or uncaring about any government inquiry. People like Mr. Brown, who operate the credit card infrastructure of webcam child pornography, have been permitted to continue their work, seemingly undisturbed by any law enforcement effort. I have watched as my former members go online to attack me, boldly proclaiming themselves as my former customers, and having no fear that their self-disclosure could result in their arrest. And events have proved them right.

Since I left the child pornography business last summer, I have risked everything to get to tell these facts to persons who care, like this Committee. It is my hope that the Congress will do everything it can to see to it that children are protected and that our law enforcement effort is competent to combat this evil. Thank you.

MR. WHITFIELD. Well, Justin, thank you very much for your testimony. It was quite revealing and we genuinely appreciate the information that you provided.

Mr. Eichenwald, you are recognized for your opening statement.

MR. EICHENWALD. Mr. Chairman and members of this committee, my name is Kurt Eichenwald and I am a senior writer with the New York Times. My appearance today is somewhat unusual. As a matter of policy, the Times instructs its reporters to decline requests to testify in judicial and legislative settings because it can serve to undermine our work if we are seen by the public as an extension of the Government. In this instance, the Times accepted a subpoena from the committee on my behalf after the committee agreed that I would be asked to provide only published or publicly disclosed information. To the extent that the committee seeks information about reporting processes, I will have to respectfully decline to answer. Nor do I believe it is my place to offer policy suggestions. Within that framework, I offer the following testimony which may assist the committee in its exploration of this important issue.

On December 19, the New York Times published a front page article that was the culmination of my 6 month investigation into the world of webcam child pornography. This was an extraordinary project not only for me, not only for the Times, or for journalism in general. This was an instance in which the very reporting could by its very nature result in a crime committed by the reporter. There was a great deal of consultation with the lawyers, a great deal of consultation with the FBI to ensure that at no point did I violate a law. Through that care, we were able to lay bare a nightmarish Internet world that grew without attracting significant attention from law enforcement or child advocates. As a citizen, I was dumbfounded by what I found. As a father, I was terrified.

Like most people, I gave little thought during my life to the scourge of child pornography, but I now know that we are fighting a losing battle. The predators are sophisticated in the use of computers and talented in their manipulation of children. They count on our willingness to avert our eyes from the unpleasant to succeed in their pursuit of illegal images of minors. And we have been far too willing to comply. That is part of why the child pornography business has exploded in the past decade. As many of you noted in your opening statements it is now a \$20 billion a year industry.

Webcam pornography has emerged in just the last few years but it is already a significant part of this illicit industry. I have submitted copies of my articles which explain facets of this business, as well as the events that led to my discovery of Justin, who served as my guide into this world, showing me the mechanisms used to seduce children into degrading and harmful behavior.

Let me stress, this is not a problem involving just Justin Berry or a handful of bad kids. Hundreds of minors have been lost to the lure of performing in online pornography. I interviewed a number of them. They include children from every walk of life, wealthy and middle class, poor, honor students and those struggling with their grades, children of divorce and with intact families. The only shared characteristic I found was a loneliness that these minors feel is alleviated by meeting people online and in person through the webcam business.

Entire infrastructures have emerged to sustain this business, including both witting and unwitting corporate participants. You have already heard how predators have turned the ingenuity of some of our greatest online companies against our children. Wish lists with companies like Amazon.com and American Eagle Outfitters, a wonderful convenience for gift giving, have become mechanisms for seducing children. Online payment systems such as Paypal.com have been used to facilitate transfers of cash. Communications programs from companies like AOL and Yahoo! are used both for direct conversations between

predators and children, and for the transmission of illegal video images. We have heard a lot today about chat rooms. They are no longer necessary. A predator can reach each child individually through these communication systems. Many of these programs and services can be obtained by children in minutes without requiring accurate identification, or proof of your age on parental consent.

In addition to the unsuspecting companies, there are businesses that know exactly what they are doing. In my reporting, I discovered credit card processors who provided support for webcam child pornography. I found web hosting companies that offered servers for the illegal businesses. I even found a company that provided streaming video to sites operated by minors on condition that the company president be allowed to watch the pornographic performances for free.

I also located scores of marketing sites known as portals which were used to direct potential customers to the webcam child pornography sites. These portals, many of which temporarily shut down since publication of my article, underscore the scope and magnitude of this business. I have provided the committee with the listing maintained by a single portal of the almost 600 teenage webcam sites that it marketed. Perhaps most disturbing was that major American and international companies advertised on these marketing portals for child pornography. The advertisements, copies of which have also been provided to the committee appeared immediately above images used by boys and girls to market their pornographic sites. Apparently, these companies were attempting to win business both from customers and the teenage pornographers themselves as it offered services to help efficiently run for-pay sites. The advertisers included Logitech and Creative Webcam, both webcam manufacturers, as well as Verotel, an international credit card processing company. I might note that the advertisements I found on archive.org for some of these portals which you know the addresses for are as we speak being changed. I do not know how it is possible but ads that were there when I began my reporting are now disappearing. Fortunately, I maintained copies.

But the for-pay sites of adolescents are only one level of this illicit business. I am told thousands of other children have become unknowing participants in the online pornography industry. These minors perform not for money or gifts, but because they have been tricked into stripping and masturbating online for what they believe is a single viewer. These performances are recorded and then posted on for-pay pornography sites without the knowledge or consent of the minors. In my reporting, I found websites dedicated to offering webcam videos of hundreds of girls and boys who had been duped into such performances. Surprisingly, a predator showed me a site he found so offensive involving hundreds and

hundreds of boys who had been lured into, tricked into a single online performance. I note this because each one of those videos had an image of the child, a non-pornographic image that the potential customer could use to decide which video to watch. We talk about the safety of putting computers outside the children's bedroom. I checked. Of the numbers I examined, about 40 to 50 to 60 percent of the single frame images advertising these pornographic videos were from computers in dining rooms, living rooms, offices, only the minority were in what appeared to be the child's bedroom. That site boasted of being the largest such site in the world. It was shut down only after I called for a comment from its credit card processor, Verotel, the same company advertising its services on the portals.

There is a business infrastructure for this part of the industry as well. There are people who make their living trolling the Internet for children with webcams, luring them into sexual performances, and selling the resulting pornographic videos. To aid such people and others in disguising their true identities, there is software available that allows anyone to make a recorded video appear to be a live webcam transmission. The result is that a middle age man can portray himself as a teenage boy or girl, complete with the video needed to convince any doubters. In my reporting, I discovered a group of predators who took bets among themselves about how many online approaches it would require to convince a girl with a webcam to take off her clothes with the resulting recorded video shared among the bettors. By the time I found this group, they had played their game dozens of times. They appear to have never failed to convince their target to strip.

To aid in their hunt for adolescents, these adults again use legitimate businesses. Justin explained how predators used [spotlife.com](#) to find him. Numerous listings of children, including sites such as [myspace.com](#) and [buddypick.com](#) are now the favorite sites, the virtual Sears catalog for pedophiles. Using these sites in combination, predators can search for children by age, location, and sex. They can obtain enormous amounts of identifying data including whether a child operates a webcam. I have witnessed conversations among child predators online where they discussed the latest minor located from these sites. Often predators share information obtained from the minor, both from site posting and from direct conversations. Even social networking sites that boast of being safe engage in reckless behavior requiring personal data from minors before allowing access to their sites, reinforcing the children's false view that providing such information is harmless.

When I explained how predators used these systems to the producers for Oprah Winfrey, they asked me for a demonstration. We limited my search to minors within 20 miles of my location. Meaning if I was a

pedophile, I could personally meet those minors within the hour. The producers timed me. It took only a minute and 30 seconds before I was in direct contact with a 16-year-old girl. By that time, I knew her name, address, school, plans for the evening, and other identifying information, including the younger sisters' names and ages. We repeated the test searching for a boy within the same distance, this time we wanted to make it harder, asked me to make sure the kid had a webcam. I was in contact with a 14-year-old in two and a half minutes. In both instances, I told these minors what I was doing and advised them not to speak with strangers online. Both replied contrary to the obvious that they never did.

From what I have witnessed, it is difficult to protect a child once he or she has accepted the predators as allies. They assist children with strategy and money in outwitting their parents so that the shows could go on. That is exactly what happened in Justin Berry's case. These predators are insidious. They advise the minors to make sure that they claim to be over 18, suggesting that otherwise the children might get in trouble. Then when the predators are caught, they claim they were deceived by the child's often laughable claim to having been an adult, even the children who had not yet reached puberty.

Of course, as you see in Justin's story, there is the possibility and I would say the probability that a child performing online will be molested. After my story, a university professor emailed me and made postings about the Internet to complain that statistically few viewers of child pornography become molesters. As you have heard, his statistics are bogus, but his argument applied to this circumstance is ludicrous. These are not instances where pedophiles are obtaining images of children they cannot identify. Here, a single child is being set upon by hundreds of predators all in direct daily contact. The entreaties to meet begin quickly. Numerous minors told me of predators pleading for meetings, more than a few, I believe agreed to go.

I have found oftentimes that adults react to these facts with incredulity. They cannot comprehend how a child could be so easily lured into pornography or speak so readily to a stranger. I think our first panel today gave quite a number of answers to those questions. You also have to understand the environment where the minors find themselves. They are not being approached by some stranger in the park. Rather, they are in their own homes feeling safe. They feel comfortable on the Internet in ways we may not recognize. Internet communication has all the elements of true social interaction, but remains shallow. So it is both socially fulfilling and emotionally non-threatening. There is no one else there, just a small solid device nearby. There is a level of unreality about it and on the part of the minors a simple lack of comprehension.

There also appear to be few protections. You have heard that the predators often laugh at Federal law enforcement. They believe arrest is rare and prosecution followed by jail time even rarer. I was dumbfounded by the willingness of online pedophiles to identify themselves, to publicly discuss their crimes in non-protected publicly accessible sites and chat rooms. What became obvious as I disclosed in my article, is that our Federal law enforcement effort to combat this threat appears to be hobbled by fractured responsibilities, bureaucratic mindsets, and a simple inability to respond.

In interviews with law enforcement personnel around the country, I repeatedly heard of frustrations about the Child Exploitation and Obscenity Section, or CEOS, serving as an impediment in the aggressive pursuit of criminal cases. For example, one law enforcement official told me that CEOS often makes arguments against bringing cases in child pornography cases that would embarrass a defense lawyer.

I saw the reasons for this aggravation in Justin's case. From the time that the Government was notified of Justin's information to the point where the children in direct danger were saved, more than 50 days passed. As you heard, efforts by Justin's lawyer to push the Government into action were met with silence. Requested subpoenas were not issued for weeks. Delays were imposed because bureaucratic approvals were sought from people on vacation. Important data offered to the Government by Justin has even at this late date not been collected. It has only been reviewed by me. As for the material the Government did collect, weeks passed before a forensic computer specialist could examine it, about average for the Justice Department.

Some people identified as perpetrators literally could not get themselves arrested if they tried. As I reported in the Times, one of these potential defendants, Justin's father, who at the time lived in Mexico, attempted, through his lawyer, to turn himself in at the American consulate in Mexico City. I personally witnessed a conversation where Justin was informed that CEOS had held that this potential defendant could not be prosecuted because even though he was playing a role in broadcasting child pornography into the United States, he did so from across the border. When the problem of Mr. Berry attempting to surrender himself to the Government presented itself, there was a great deal of discussion as I understand it among law enforcement personnel. They discussed until Mr. Berry changed his mind. He has since fled Mexico.

These kind of problems spread throughout the Government; for example, agents of Immigration and Customs Enforcement, ICE, an excellent organization from what I have seen, have been months investigating a child rapist who had separately been identified to CEOS



by Justin as one of his molesters. This is Mr. Tunno who Justin spoke about a few minutes ago. Indeed, Justin possessed video evidence of the crime that had been emailed to him by Mr. Tunno. These ICE agents at the time were unknowingly searching for Justin who they knew solely as a boy from Bakersfield that they suspected had been abused by this serial molester. Those agents heard 4 months after Justin's meetings with CEOS that the boy they were searching for was already a Federal witness. That information was not passed on to them by CEOS, instead, they learned it from me, a newspaper reporter in the course of an interview.

Justin Berry stepped forward at a time the Government did not know he existed. He is, to experts' knowledge, the first such teenage witness to ever turn over this kind of vast evidence to the Government. Given the way his case was handled, including the meager results and the longstanding threat that it would be Justin who would be prosecuted, it is hard to imagine other teenagers wrapped up in this world will risk their freedom or safety to follow in his footsteps.

Each year, each week, each day, the predators are becoming more sophisticated with computers facilitating the growth and evolution of child pornography. It is why this business is exploding. My reporting has shown me that we are woefully behind.

Thank you.

[The prepared statement of Kurt Eichenwald follows:]

PREPARED STATEMENT OF KURT EICHENWALD, REPORTER, THE NEW YORK TIMES

My name is Kurt Eichenwald and I am a senior writer with the New York Times. My appearance today is somewhat unusual. As a matter of policy, the Times instructs its reporters to decline requests to testify in judicial and legislative settings, because it can serve to undermine our work if we are seen by the public as an extension of the government. In this instance, the Times accepted a subpoena from the committee on my behalf after the committee agreed that I would be asked to provide only published or publicly disclosed information. To the extent that the committee seeks information about reporting processes, I will have to respectfully decline to answer. Nor do I believe it is my place to offer policy suggestions. But, within that framework, I offer the following testimony, which may assist the committee in its exploration of this important issue.

On December 19, the Times published a front page article that was the culmination of my six month investigation into the world of webcam child pornography. The story laid bare a nightmarish Internet world that grew without attracting significant attention from law enforcement or child advocates. As a citizen, I was dumbfounded by what I found. As a father, I was terrified.

Like most people, I gave little thought during my life to the scourge of child pornography. But, I now know we are fighting a losing battle. The predators are sophisticated in the use of computers and talented in their manipulation of children. They count on our willingness to avert our eyes from the unpleasant to succeed in their pursuit of illegal images of minors. And we have been far too willing to comply. That is part of why the child pornography business has exploded in the past decade, making it a multi-billion dollar industry.

Webcam pornography has emerged in just the last few years, but is already a significant part of this illicit industry. I have submitted copies of my articles which explain facets of this business, as well as the events that led to my discovery of Justin Berry, who served as my guide into this world, showing me the mechanisms used to seduce children into degrading and harmful behavior.

Let me stress: this is not a problem involving just Justin or a handful of bad kids. Hundreds of minors have been lost to the lure of performing in online pornography. I interviewed a number of them. They include children from every walk of life – wealthy and middle class, honor students and those struggling with their grades, children of divorce and with intact families. The only shared characteristic I found is a loneliness that these minors feel is alleviated by meeting people online – and in person – through their webcam business.

Entire infrastructures have emerged to sustain this business, including both witting and unwitting corporate participants. You have already heard how predators have turned the ingenuity of some online companies against our children. Wish lists with companies like Amazon.com and American Eagle Outfitters – a wonderful convenience for gift giving – have become mechanisms for seducing children. Online payment systems, such as paypal.com, have been used to facilitate transfers of cash. Communications programs from companies like AOL and Yahoo are used both for direct conversations between predators and children, and for the transmission of illegal video images. Many of these programs and services can be obtained by children in minutes, without requiring accurate identification or proof of either age or parental consent.

But, in addition to the unsuspecting companies, there are businesses that know exactly what they are doing. In my reporting, I discovered credit card processors who provided support for webcam child pornography. I found web hosting companies that offered servers for the illegal businesses. I even found a company that provided streaming video to sites operated by minors, on condition that its president be allowed to watch the pornographic performances for free.

I also located scores of marketing sites, known as portals, which were used to direct potential customers to the webcam child pornography sites. These portals – many of which have temporarily shut down since publication of my article – underscore the scope and magnitude of this business. I have included as an exhibit to my remarks the internal listing maintained by a single portal of the almost 600 teenage webcam sites that it marketed. Perhaps most disturbing was that major American and international companies advertised on these portals. The advertisements appeared immediately above images used by boys and girls to market their pornographic sites. Apparently, these companies were attempting to win business both from customers and teenagers themselves, as they offered services to help efficiently run for-pay sites. The advertisers included Logitech and Creative Webcam, both webcam manufacturers, as well as Verotel, an international credit card processing company.

But the for-pay sites of adolescents are only one level of this illicit business. Untold thousands of other children have become unknowing participants in the online pornography industry. These minors perform, not for money or gifts, but because they have been tricked into stripping and masturbating online for what they believe is a single viewer. Those performances are recorded and then posted on for-pay pornography sites, without the knowledge or consent of the minors. In my reporting, I found websites dedicated to offering webcam videos of hundreds of girls and boys who had been duped into such performances. One that boasted of being among the largest such sites in the world was shut down only after I called for a comment from its credit card processor, Verotel – the same company advertising its services on the portals.

There is a business infrastructure for this part of the industry as well. There are people who make their living trolling the internet for children with webcams, luring them into sexual performances and selling the resulting pornographic videos. To aid such

people in disguising their true identities, there is software available that allows anyone to make a recorded video appear to be a live webcam transmission. The result is that a middle aged man can portray himself as a teenage boy or girl, complete with the video needed to convince any doubters. In my reporting, I discovered a group of predators who took bets among themselves about how many online approaches it would require to convince a girl with a webcam to take off her clothes, with the resulting recorded video shared among the bettors. By the time I located this group, they had played their game dozens of times; they never failed to convince the target to strip.

To aid in their hunt for adolescents, these adults again use legitimate businesses. Justin explained how predators used [spotlife.com](#) to find him. Numerous listings of children – including sites such as [myspace.com](#) and [buddypic.com](#) – are now the favored sites, the virtual Sears catalogue for pedophiles. Using these sites in combination, predators can search for children by age, location and sex. They can obtain enormous amounts of identifying data, including whether a child operates a webcam. I have witnessed conversations among child predators online, where they discuss the latest minor located from these sites. Often, predators share information obtained from the minor – both from site postings and from direct conversations. Even social networking sites that boast of being “safe” engage in reckless behavior, requiring personal data from minors before allowing access to their sites – reinforcing the children’s false view that providing such information is harmless.

When I explained how predators used these systems to producers for Oprah Winfrey, they asked me for a demonstration. We limited my search to minors within 20 miles of my location – meaning, if I was a pedophile, I could personally meet these minors within the hour. The producers timed me. It took only one minute and thirty seconds before I was in direct contact with a 16 year old girl. By that time, I knew her name, address, school, plans for the evening and other identifying information, including her younger sisters’ names and ages. We repeated the test, searching for a boy with a webcam within the same distance. I was in contact with a 14 year old in two and a half minutes. In both instances, I told these minors what I was doing, and advised them not to speak with strangers online. Both replied, contrary to the obvious, that they never did.

From what I have witnessed, it is difficult to protect a child once he or she has accepted the predators as allies. They assist children – with strategy and money – in outwitting their parents, so that the shows can go on. And these predators are insidious. They advise the minors to claim they are over 18, suggesting that otherwise, the children might get in trouble. Then, when the predators are caught, they claim they were deceived by the child’s often laughable claim to being an adult – even with children not yet in puberty.

Of course, as you see in Justin’s story, there is the possibility that a child performing online will be molested. After my story, a university professor emailed me to complain that statistically, few viewers of child pornography become molesters. His argument, applied to this circumstance, is ludicrous. These are not instances where pedophiles are obtaining images of children they cannot identify. Here, a single child is being set upon by hundreds of predators, all in direct, daily contact. The entreaties to meet begin quickly. Numerous minors told me of predators pleading for meetings; more than a few agreed to go.

I have found oftentimes that adults react to these facts with incredulity. They cannot comprehend how a child could be so easily lured into pornography, or speak so readily to a stranger. The answer comes from an understanding of the environment where the minors find themselves. They are not being approached by a predator in the park. Rather, they are in their own homes, feeling safe. They feel comfortable on the internet, in ways we may not recognize. Internet communication has all of the elements of true social interaction, but remains shallow. So it is both socially fulfilling, and emotionally non-

threatening. There is no one else there, just a small, silent device nearby. There is a level of unreality about it, a simple lack of comprehension.

There also appear to be few protections. You have heard that the predators often laugh at federal law enforcement. They believe arrest is rare, and prosecution followed by jail time even rarer. I was dumbfounded by the willingness of online pedophiles to identify themselves, to publicly discuss their crimes. But what became obvious, as I disclosed in my article, is that our federal law enforcement effort to combat this threat appears to be hobbled by fractured responsibilities, bureaucratic mindsets, and a simple inability to respond.

In interviews with law enforcement personnel around the country, I repeatedly heard of frustrations about CEOS serving as an impediment to the aggressive pursuit of criminal cases. For example, one prominent law enforcement official told me that CEOS often makes arguments against bringing cases in child pornography cases that would embarrass a defense lawyer.

I saw the reasons for this aggravation in Justin's case. From the time that the government was notified of Justin's information to the point where the children in direct danger were saved, more than 50 days passed. Efforts by Justin's lawyer to push the government into action were met with silence. Requested subpoenas were not issued for weeks, delays were imposed because bureaucratic approvals were being sought from people on vacation. Important data offered to the government by Justin has, even at this late date, not been collected and has only been reviewed by me. As for the material that the government did collect, weeks past before a forensic computer specialist could examine it – about average for the Justice Department. Some people identified as perpetrators literally could not get themselves arrested if they tried: As I reported in the Times, one of these potential defendants, Justin's father, who at the time lives in Mexico, attempted through his lawyer to turn himself in at American consulate in Mexico City. I personally witnessed a conversation where Justin was informed that CEOS had held that this potential defendant could not be prosecuted because, even though he was playing a role in broadcasting child pornography into the United States, he did so from across the border.

The problems spread throughout the government. For example, agents with Immigration and Customs Enforcement (ICE) had for months been investigating a child rapist who had separately been identified to CEOS by Justin as one of his molesters; indeed, Justin possessed video evidence of the crime. These ICE agents at the time were unknowingly searching for Justin, whom they knew solely as a boy from Bakersfield who they suspected had been abused by this serial molester. Those agents heard four months after Justin's meeting with CEOS that the boy they were searching for was already a federal witness. But that information was not passed to them by CEOS; instead, they learned it from me, a newspaper reporter, in the course of an interview.

Justin Berry stepped forward at a time the government did not know he existed. He is, to experts' knowledge, the first such teenage witness to ever turn over this kind of vast evidence to the government. Given the way his case was handled – including the meager results -- it is hard to imagine other teenagers wrapped up in this world will risk their freedom or safety to follow in his footsteps.

Each year, each week, each day, predators are becoming more sophisticated with computers, facilitating the growth and evolution of online child pornography. My reporting has shown me, we are woefully behind. Thank you.

MR. WHITFIELD. Mr. Eichenwald, thank you for your testimony. I also want to thank you for the articles that you wrote in the New York Times which bring this matter to the attention of the entire country. We really appreciate your testimony.

At this time, I am going to recognize the full committee Chairman, Mr. Barton of Texas, because he has a meeting down at the White House and he is so interested in this issue and wanted to ask some questions.

CHAIRMAN BARTON. Thank you, Mr. Chairman. I want to thank you and Mr. Stupak for allowing me to go out of order. I appreciate that. I do have an engagement at the White House in 15 minutes so I am going to have to leave after these questions.

I have been listening in my office on the television to the testimony of both witnesses and I do want to thank each of you for appearing. It is a great credit to your courage, Mr. Berry, that you are here and it is a great credit to the journalism profession, Mr. Eichenwald, that you are here. I must remind my friend from the New York Times that when this committee does issue a subpoena it is outweighed. I mean, you seem to think you are doing us a favor by showing up and you are, but you would have showed up whether you wanted to or not if you had insisted not to be here. Having said that, we are very pleased that you are here, do not think this is any kind of an argumentative situation.

My first question is to you, Mr. Berry. I cannot fathom how you could conduct the activities that you conducted in your home with a mother who appears to have been as concerned as you indicated she was. How did you get around her efforts to prevent you from doing what you did?

MR. BERRY. To tell you the truth, that is probably the most asked question that I have recently encountered. My mother is great, she is wonderful, I love her a lot, and she cares for me more than I can imagine. Her efforts were no match for the pedophiles. They were no match for the predators. Whenever I needed to, whenever I felt that I needed some more space outside my home, one of the perpetrators came down to Bakersfield, California where I lived and rented me an apartment on the street. When I was--

CHAIRMAN BARTON. So you did this outside your home?

MR. BERRY. It started in my home, went to the apartment which this individual that I had--

CHAIRMAN BARTON. Where did your mother think you were when you were at this apartment?

MR. BERRY. I would tell her I was going to a friend's house or something like that. Being as I was not 18, I could not rent the apartment myself so this individual signed the lease and after that, I had recently, I had graduated high school early at 16 and my mom told me I could not move out of the house until I graduated high school, so I took care of that. After a few months had passed, I had moved to Mexico with my father.

CHAIRMAN BARTON. Your father encouraged this apparently. He thought he could profit by it.

MR. BERRY. Correct. I told my father about the business when he asked where all my money was coming from and he helped me.

CHAIRMAN BARTON. Well what did your mother think about where all this money, or did you hide your money from your mother?

MR. BERRY. Living two separate lives and having to come home and be the Justin that I was for the family, and then living a different life in Mexico was very difficult.

CHAIRMAN BARTON. Now you indicated that you were an honor student and that you were president of your class. Is that right?

MR. BERRY. Correct.

CHAIRMAN BARTON. But you also said you were very lonely. Can you reconcile that? I mean how can you be the president of the class and be lonely?

MR. BERRY. For me, I am not sure on why I felt certain ways or why I did certain things. All I know is these people, I thought they were my friends.

CHAIRMAN BARTON. Did your friends at school, were they aware of what was going on or did you hide that from them, too?

MR. BERRY. I hid this from everyone for years. I did not tell anyone until recently.

CHAIRMAN BARTON. So where you actually lived, your what we call traditional friends in school, in church, and the neighborhood thought you were just a normal teenager.

MR. BERRY. That liked to sit on the computer a lot, yeah.

CHAIRMAN BARTON. Which is fairly normal for teenagers these days, that is what teenagers do.

Mr. Eichenwald, what should we do about these credit card companies that knowingly or maybe even unknowingly foster this kind of activity? Are there some remedies that are not in current law that you would recommend?

MR. EICHENWALD. Mr. Barton, in truth, I do not know. The danger of a reporter is that we come in and we know what we have reported, we know what we have found, and it gives us the view of an expert. I do not know the laws governing credit card companies. I do not know what standards are in place now which is why I was saying I do not think it is my place to offer policy pronouncements. I think anything I would say would be hardly uninformed.

CHAIRMAN BARTON. Do you care to, either one of you, foster an opinion about we are having a markup starting this evening and then beginning, and then continuing tomorrow on the new video services bill in which one of the big debating points right now is the concept of

Internet neutrality and freedom of the Internet. Are their exceptions to total freedom of the Internet and if so is this one of them? Should there be some laws, explicitly Internet, concerning Internet behavior for child pornographic activities.

MR. EICHENWALD. I have never understood why there was a difference between the Internet and the mails and walking down the street with a bag in your hand. Child pornography is illegal and those who facilitate child pornography are committing a crime. If a credit card company is involved in the business and it can be demonstrated that they are for example involved in multiple lines of child pornography, if I was a prosecutor, I would certainly like to have that case. The bottom line issue, I think sometimes we tend to think ourselves too much into a spiral. If someone is engaging in an act that is illegal, they should be prosecuted whether they are an individual, a company, or whatever other level of involvement there is here. I can tell you for however disturbing these issues have been and I deeply appreciate what I have heard from the members about how disturbing these things are, I can tell you that the reality of what I have witnessed over the last number of months is far worse than anything you can imagine. It is far worse than anything you would want to imagine.

CHAIRMAN BARTON. Right.

MR. EICHENWALD. This working on the story resulted in many, many months of being unable to sleep. There were images I could not get out of my head when the lights went out. Ultimately, I have been, as a result of my reporting diagnosed with post traumatic stress disorder. Fortunately, the Times is making sure I am taking care of that. I say all that to underscore that if there are people involved in this business, whether they are on the Internet or not, this has nothing to do with freedom, this has to do with sexual abuse, and those people should be prosecuted.

CHAIRMAN BARTON. Mr. Berry, do you have a comment on that?

MR. BERRY. No, sir, I do not.

CHAIRMAN BARTON. Okay. Last question. You ask topical questions. We have had a testy relationship with the Justice Department. We, being the committee in this investigation, although the Attorney General has been very cooperative and we are getting cooperation, could they have done more in your case, Mr. Berry to go after the perpetrators and if so, what should they have done that they have not done?

MR. BERRY. When we came forth to the Department of Justice and told them, when I went and spoke with them and told them about the children who were being abused and molested and exploited by these adult perpetrators, sitting there and wondering every night, were these children that I knew being molested, why weren't they safe, and having

to wait there 50 plus days, almost 2 months knowing that these children are in the hands of these perpetrators, that ripped me apart.

CHAIRMAN BARTON. Mr. Ryan, would you want to comment on that?

MR. RYAN. I would, Mr. Chairman.

Chairman Barton, let me give an example of a question that I think the Chairman might ask on Thursday of the Department. Given that we turned over approximately 1,500 IP addresses, matching credit card information, and other identification for people who are paying for child pornography, as a policy call, I am not sure you would want to prosecute all 1,500 of those cases. But I sure think that you would want law enforcement to get search warrants and go get the computers of those people and leave their wives and daughters and other people in their house asking that person why it was that the FBI or ICE or another, the Postal Service who do excellent work, had dropped by to seize it. I think the Department needs to explain whether its policy is to indict those people or to do something with them. I think--

CHAIRMAN BARTON. Well we want them to do their investigation and we have every indication from staff interviews that they are conducting an active investigation. I do not want to come across as being too negative. My question is, is it a fair policy question that even given limited resources and all the various issues that you had to deal with at the Federal level in determining to go ahead and prosecute, is it a fair statement that Mr. Berry, and you as his attorney, feel like they could have been more aggressive with the information that you provided them?

MR. RYAN. Yes, sir.

CHAIRMAN BARTON. Mr. Eichenwald, do you have a comment on the generic ability to prosecute these types of cases?

MR. EICHENWALD. I do. Also on the comment of an aggressive, they are aggressively investigating. I have written about law enforcement issues for almost 20 years. Normally, I am not in this field, I am dealing with corporate crime, the most complex area of criminal prosecution. There you are dealing with thousands of pieces of paper, sometimes millions of pieces of paper. You are dealing with multiple witnesses, many of whom have financial interests not to testify. I have never seen a case in my experience move slower than this one. There were identified again at the beginning, multiple levels of people. You had identified particular perpetrators who had access to specific children, children whose names we knew, children whose faces we could describe, we knew where they lived, who were being filmed and molested. I must admit, I, to this day, do not understand what was happening over those 55 days. I do sit in horror worrying about the day I hear that on day 35,



something happened to one of those children that was preventable. I cannot explain what happened there.

Then there is the next level. I mentioned in my opening comments, my opening remarks the credit card processor. Justin mentioned the credit card processor. I was there at the beginning when Mr. Ryan was speaking to CEOs on, I believe it was on July 26 and saying the centerpiece of this case is meova.net, the company that is processing the credit cards. Justin Berry is a spoke. Meova is processing credit cards for child pornography. They are the hub. Not only that, the individual who was the president of meova.net had previously been subject to a child pornography investigation which he had escaped by saying oh, he did not know there was child pornography involving what he was doing. Mr. Ryan strongly recommended that the way to maximize the impact of Mr. Berry's information was to immediately go after meova.net and to immediately seize its information, arrest its president because you had direct evidence that he was processing credit cards for child pornography. Hopefully flip him or a member of his organization to make this case branch out in the many directions it seemed like it could go. To date, none of that has happened because meova.net is still around. The president of the company, we are now 9 months later, the president of the company is still wandering around.

In the Enron case, which I covered, it took 6 months until you had a senior executive indicted. A month later you had another senior all the way up to the chief financial officer. We are 9 months down the line and we have two low-level people who were molesting children or filming children, and they were arrested 55 days after the information was provided to the Government. You then have the areas of people who were involved in the infrastructure of this business who were identified by Justin where their information was contained in the documents and files turned over by Justin. These people are not secret. I wrote about them in the New York Times. I had always believed that I would be able to name people in the paper by the time the story ran. It never occurred to me that there would be no action by the Government.

I also want to recount a story that was probably the more horrific moment in terms of my interactions with Justin. Eventually, at a point when I really was wrestling with do we have to write a story about the Government's failure to do anything here. Eventually, Justin was granted immunity. One individual who was endangering children was arrested, a few weeks later another individual who was endangering children was arrested. Justin kept coming back to me and saying what about the other men who molested me? What about what they did? Finally there was a day he said to me with tears in his eyes, why is it the Justice Department does not care about the men who molested me? To

this date, none of those men have been prosecuted. None of those men have been arrested, except for Mr. Mitchel who had the distinction of being the sole person who was identified as endangering other children who also had molested Justin Berry. So, if you ask if this is an active investigation or what more could they have done, in truth, the better question is what less could they have done.

CHAIRMAN BARTON. Well, I have spoken directly with the Attorney General of the United States on this and am absolutely confident that he is personally committed to actively pursuing the specifics and the generic investigation. We will have the Justice Department here on Thursday. And again, they have an active criminal investigation underway so they are not going to be able to talk on the specifics, but the fact that you two here are testifying in an open hearing, and being as brave as each of you are, is going to help activate those investigations even more, I am very sure. But I appreciate your testimony and again, I want to thank Mr. Stupak and Mr. Whitfield for letting me go out of order. I appreciate that.

MR. WHITFIELD. Thank you.

At this time, I recognize the gentleman from Michigan, Mr. Stupak.

MR. STUPAK. Thank you.

And before the Chairman leaves, Mr. Chairman, I hope we could if Justice is coming in Thursday, we could pin Justice down because as you were asking Mr. Eichenwald his comments just sitting here, I already knew Justice would say well it is an active investigation, therefore we cannot answer half of our questions. So I hope we would take Justice in closed session or something because if we let them off the hook, this is just going to drag on and on. We have seen it so many times in this committee so I would hope that--

CHAIRMAN BARTON. We are not going to let anyone off the hook.

MR. STUPAK. All right, very good.

And since we are on the lines of law enforcement and having been there for a number of years myself, Mr. Ryan or Mr. Eichenwald if you care to comment on action by the Government. I see a number of things and tell me what I am missing or what else should be on this list. First, I am sure is their lack of financial resources. Next, the lack of cooperation I have heard between ICE and FBI and Justice, inadequate laws either updated or not caught up with the computer, or conflicting laws between State and Federal, and the credit card processing which I bring up again because we have seen it last year in this committee alone on the Internet pharmacy where people are buying drugs improperly, illegally to great harm. We also saw it in masking of drug testing and now we see it on child pornography. Credit card processing seems to be as you said the hub of the wheel if you will, and not just merely a spoke. And we have

had MasterCard, Visa, and all the rest of them in here and they keep saying we will get back with you on how we can best crack down on this and yet to this day we have never heard that happen. When I look at the problems of law enforcement and the issues or excuses they use not to move forward on this, is there anything else missing? Financial resources, lack of coordination, inadequate laws, conflicting laws, or processing of credit cards, any other area we should explore if we are going to do true law enforcement, truly aggressive enforcement?

MR. RYAN. Congressman, I think there are very few impediments to prosecution in this area and frankly, there may be distractions in the post 9/11 world that have taken some of the squads that may have worked this area before, and that would be quite legitimate that there may have been an emphasis on counterterrorism and other issues. If I could be bold enough, I would recommend to the committee that you privately convene the credit card industry at a roundtable here with staff, the members coming in the late part of that meeting and ask them what they would like to do here, because I think the kind of credit card companies we are talking about here are not Visa and MasterCard or the standard companies. These are companies we believe are heavily involved in an illegal business knowingly. So the question then is how can we identify those companies and I believe there are ways of doing that and I think industry knows them as well. And I do believe that cooperation between the business community and the law enforcement community in the area of child pornography can be increased without violating personally identifiable information of normal citizens and I think that is the challenge for the Congress with regard to that. The challenge for law enforcement here I would rather have a horse that I had to say whoa to rather than one I've got to hit all the time and say giddy up. I think the question for this committee in a sense with Justice is not so much if a law is inadequate, as is the level of energy enough and is the ambition of the 26, 27-year-olds, which we all were at one point, prosecuting the Department of Justice being unleashed on these people.

MR. STUPAK. Well, but the credit card processing if its MasterCard or Visa that are being embarrassed then what I am saying, wouldn't they have a greater interest to try to see who is processing these credit cards and for what purpose.

MR. RYAN. I think the legitimate credit card industry could be uniquely helpful to the committee privately in helping the committee understand, and helping law enforcement understand, what it is that they may be able to do to help on this problem.

MR. STUPAK. Sure. You brought up 9/11 and I do not want to necessarily tie this in here, but it seems like on 9/11 we did not have coordination or Justice talking to this agency or that agency, and it seems

now when we are 5 years post we are still not cooperating or talking with each other from a law enforcement point of view. And the victims here are children around this country.

MR. RYAN. Well let me say something. As a prosecutor for the Department of Justice, and I treasure the time that I spent there, I think it is the responsibility of the lead prosecutor in these cases to marshal the agents and their energy. The 1811s are not responsible for these cases; the prosecutors are responsible for coordinating with them so that the good work that the agents do will result in prosecutions to tell them what element is still missing that they want them to go get. And I think that we have to ask the Department of Justice about its leadership role in this case.

MR. STUPAK. Part of this, I do not know if it is inexperience or what, but why would you put Justin Berry, your witness here, disclose his identity as he testified to in the court case which actually threatened his life and had made him now a greater victim than what he may have been?

MR. RYAN. I have to say Mr. Berry is one of the bravest and frankly he is a very smart young man. He understands the danger that he undertook. He was at the height of danger last summer when these people were really looking for him and they are amateurs in a lot of ways, but amateurs can kill you just the same as professionals.

MR. STUPAK. And certainly I would echo those comments but at the same time who left them out there? Law enforcement, if you will, Justice left him hanging. He is still out there.

MR. EICHENWALD. I would interject--there was a point after the Justice Department unsealed the affidavit that revealed Justin's role in this case, there was a lot of backpedaling and apologizing. And Justin was offered, I know this because it happened while I was sitting there, Justin was offered whatever levels of protection could be brought forward. At this point, we are 70 days into it and Justin truly had absolutely no faith in the Justice Department and he said to me if I ask for something, they will know my address and if they know my address, how do I know they are not going to open the document and unseal it somewhere. And there was a point where he was told that the Justice Department would do anything he asked to make him feel safe. And his response was telling. His response was tell them to stop being so stupid.

MR. STUPAK. Well, Justin, thank you again for being here and for helping parents and young people across this Nation. Let me ask you this question and if you can answer it. Is there any reason why a 13-year-old needs a webcam?

MR. BERRY. That is a very simple answer, no.

MR. STUPAK. And they put this out as a promotion if you would sign up with their service?

MR. BERRY. Correct.

MR. STUPAK. Okay. And the spotlife.com was that pre-noted or anything or--

MR. BERRY. Spotlife.com, I do not believe it exists at the current date. There are other sites that are similar and just like it. That company is owned by Logitech which is the manufacturer of the webcams. So spotlife.com was a way that Logitech, I guess they envisioned that these webcams they can communicate through the Internet, meet new people. It was a site like that.

MR. STUPAK. It just made it all so convenient.

MR. BERRY. It just did.

MR. STUPAK. Let me ask this. You mentioned that your mother had child protection programs, took away your keyboard, but the folks you were dealing with were sophisticated enough to work around that. Explain that for me, how did you get around it? Because I am sure that parents buy things and say we have this protection out here.

MR. BERRY. You know, I am not a computer genius, I know a little bit, however, with the help of these people. Let us just say my mom takes away my keyboard.

MR. STUPAK. Okay.

MR. BERRY. And the next day I hop on the Internet and I say, okay, I need another keyboard, what am I going to do here? Let us say I am discussing this with these people, I could have ten keyboards FedEx'd to my house by same day delivery if I needed it.

MR. STUPAK. Sure.

MR. BERRY. These pedophiles are no match for any parent out there.

MR. STUPAK. If you can answer this, maybe you cannot. What was the greater gift if you will that you received when you first started down this unfortunate road? Was it the physical presents that were left at your doorway or was it the compliments, the companionship, the popularity, or as you said the king of the universe. Was that the motivating force or was it the physical gifts?

MR. BERRY. I really could not tell you exactly what I was thinking or what drove this. All I know is these people are the most manipulative and the most relentless people that I have ever encountered in my life.

MR. EICHENWALD. If I could add, I have the unfortunate distinction of having read many of the conversations that Justin had with these predators. And when he says they are relentless, that is truly the correct word. They would act to remove any impediment to these shows. The moment depicted in the story was when Justin had a girlfriend and she found out what was going on and was basically begging him to stop.

And this, every element of his life was repeated to these people and they begin telling Justin how terrible it is she is saying this, how terrible. She is willing to let you spend your money on her, but she does not want you to earn it. And the line that I quoted was from one person, "She may not love you, Justin, but your friends in this room do." That is the entire mindset. They will remove anybody. They will take care of any impediment. They are 1,500 people acting to subvert the actions of a single parent and they win.

MR. STUPAK. Let me ask one more thing, if I may, Mr. Chairman.

MR. WHITFIELD. Yes, certainly.

MR. STUPAK. We talked earlier with Dr. Cooper about the benefits of your personal gratification or else the commercialization if you will of this pornography. But you brought in a third element, the advertising that are on these sites. I mean, have we become as a society so accepting of it that we advertise on these sites? I mean, I was shocked to hear that. Could you explain that a little bit more?

MR. EICHENWALD. The advertising is not taking place directly on the children's sites. The minors or there have been sites that have been put up called portals which are basically--the advertising is not taking place directly on the children's sites. If you are looking for webcam child pornography, it is hard to find. You have to know where to go. Well the portals solved that problem. The portals are a listing of webcam sites which a customer goes in and votes for their favorite site. The more outrageous the behavior of the child, the more votes the child gets. These votes become this self-reinforcement, this element of a kid feels good about herself or himself because they are getting more votes than other people and so they do things to get votes. I saw people who said I will let you watch me sleep. I saw, if you do this, I will do that. There were some very explicit offers of what would happen if people voted for them. Getting higher votes moves you higher up the list. Being higher up the list gets more customers. That little competition is going on right beneath an ad for Logitech or an ad for Verotel.

The companies, I do not know if they simply do not look at what is going on in the places they advertise but the committee has some samples of a particularly well-known portal and what was there. And you have, you know, I am a 14-year-old, you watch me in my bed, I mean, they are not being subtle. They are not making a secret. And also you get down to what is it people think is being paid for? These are children in front of a camera charging money. What in the world does anyone imagine is going on there? And so I think what we have is not that we are just, we have fallen so far is that we fall to the level of well I can deny it. You know, I do not explicitly know what this is.

MR. STUPAK. Sure.

MR. EICHENWALD. But anybody who looked at it for 10 seconds would know exactly what it is.

MR. STUPAK. Thank you again, Mr. Chairman.

Thank you, witnesses.

MR. WHITFIELD. Justin, in your testimony, you talked about spotlight as and I believe that was the vehicle by which you were first introduced into this world. Is that correct?

MR. BERRY. That is correct.

MR. WHITFIELD. And would you elaborate on that just a little bit about exactly what spotlight was. I know there are other similar vehicles today but would you elaborate on that just a little bit?

MR. BERRY. What spotlight.com was was an Internet website similar in nature to what he, Kurt, spoke about, however this is a little bit different. What it does is it was a website which allowed viewers like yourself, the nice lady sitting next to you, whoever it might be to go on these websites, browse through a directory, and view the different web cameras that are hooked up through this software. Thereafter that the guests of the website if there was contact information on there, could contact that person with a camera and after that they would begin speaking. So it is basically an automobile to communicate with the webcam user themselves.

MR. WHITFIELD. And you had a webcam at that time. Correct?

MR. BERRY. Yes, sir.

MR. WHITFIELD. And then you, I think in your testimony you, someone contacted you and said that if you would take your shirt off, they might give you \$50?

MR. BERRY. Yes, sir.

MR. WHITFIELD. And that was the first time that you had ever had an experience like that. Is that correct?

MR. BERRY. Correct.

MR. WHITFIELD. And so it just kind of went on from there?

MR. BERRY. From there it escalated.

MR. WHITFIELD. Okay. Now I read a lot of this testimony and I read the newspaper articles that you wrote, Mr. Eichenwald, and of course talked to Mr. Ryan some. I have not talked to the Attorney General, although the Chairman has, but I must say without hearing from their side, it does appear to me that the child exploitation and obscenity section of the Justice Department has a lot of explaining to do because you did give them 1,500 names with addresses, with credit card numbers and everything else, and I find it just unbelievable the different stories that I have heard about this investigation and it appears that this center, this section in the Justice Department is failing miserably on this issue. So I am looking forward to Thursday when they do come and testify.

Hopefully, we can get some answers from law enforcement and follow up on this as well.

But Mr. Eichenwald and Mr. Ryan, I know that when Greg Mitchel was, he was convicted I believe. Was he convicted?

MR. RYAN. Mr. Chairman, he was indicted, arrested, has plead guilty, and on April 12 he will be sentenced.

MR. WHITFIELD. Okay. But one of the reasons that he is going to be convicted and will be sentenced is because of the evidence that Justin provided. And what is the explanation for the Justice Department unsealing that information?

MR. RYAN. Mr. Chairman, I wrote a letter recently to the Department and I would ask that you put that letter and the Department's response to me in the record. We summarize it as follows. The understanding that I have is that the unsealing of the affidavit that identified Mr. Berry not by name but for those who are looking for him, identified that he was cooperating. I believe the Department's position is that it was a mistake that it was done. In my experience when a prosecutor makes a mistake, and we do make mistakes as lawyers, you try and put the milk back in the bottle. That is you reseal the affidavit. I am not aware that any effort was ever made to reseal the affidavit but that affidavit once it was released would have given notice to everyone in the business who had done facilitation of the business like the credit card business to dump the server box for example, drop it off a bridge, put it in a dump, erase the random access memory, you know, do various things. But I do believe, I take at face value the Department's representation that they really had not intended to do that and that it was a mistake which is in the letter that I received last night about 5:00 in preparation for this hearing.

MR. WHITFIELD. Okay. So they basically said it was a mistake but that was a mistake some time ago and there has been no effort to reseal. Is that your understanding?

MR. RYAN. You know, traditionally, Mr. Chairman, these things do happen at a court. It could be the fault of the prosecutor, it could be the fault of a court official.

MR. WHITFIELD. Right.

MR. RYAN. What you simply do is reseal the information--

MR. WHITFIELD. Right.

MR. RYAN. --and try and pull it off the Internet which you can do.

MR. WHITFIELD. Right. Ryan, at the time that you were negotiating with the Justice Department for immunity for Mr. Berry, there was valid reason for Justin to be concerned, right, about his life. I mean, did you feel at any time that his life was in danger?



MR. RYAN. Mr. Eichenwald and I both observed emails of people who were frantically looking for him at various points. One of those was--well there were these emails that reflected that. It was our judgment that it was best for him to be at a location that is not identified. We have never altered that practice. Mr. Eichenwald and I continue today to advise Justin to not describe for example here where he lives. And it is just best for him that way. And I have to say that law enforcement offered us their protection. But I took seriously the concern that some of these child molester perpetrators might hurt him if they knew where he was. I actually took it as a potential threat.

MR. EICHENWALD. Mr. Chairman, I was a direct witness to the magnitude of the hunting that was going on. The most frightening day in all of this in an array of frightening days, Mr. Mitchel had somehow figured out that Justin had possession of his mother's cell phone and was sending text messages to it. And Justin was very upset by this and basically gave me the cell phone which by the way is still in my possession. That cell phone, he would say, I have money for you. There was another child that Mr. Mitchel was filming. He would say, Justin this other child is very upset, he wants you to call him, please call, very manipulative acts. And then there was the day when the message arrived and I looked at it and it was my home telephone number and with no other explanation. And apparently, Mr. Mitchel in his efforts to find Justin had somehow obtained Justin's cell phone records and found that he had called a number he did not recognize. I showed that message to Justin. I showed Justin all the messages that came in. And he panicked. He looked at it, I think rightfully as a potential threat to my family. And he devised what I thought was a fairly brilliant response. We were planning to go the next day to Bakersfield for me to examine some of the hard drives that contained the conversations I mentioned earlier and Justin contacted Mr. Mitchel and engaged in a rambling conversation which was basically all fake saying send me my money, wire it to me, send it to Bakersfield. The idea being he would pick it up in Bakersfield and then no one would ever come and look for anyone in my home where I have two children.

MR. WHITFIELD. Right.

MR. EICHENWALD. That took place the evening before we left and by the time we arrived in Bakersfield the next morning, there were people hunting for Justin at the airport and they had already gone to his home the night before around, I believe it was around 10:00 at night thinking that he was with his mother. And from what we were told by his mother, there was a hotel by hotel search going on. We had hoped to go to Justin's house to pick up these hard drives. We obviously could not and we ended up going to stay at the home of a friend of Justin's

mother and all of the equipment was brought over to us. But the speed with which we were talking, he was talking to somebody in Virginia and suddenly there are people hunting for him in California who I believed was a very strong suggestion of the level of potential danger that this young man was facing.

MR. WHITFIELD. Thank you. And in his testimony he talked about Ken Gourlay who actually is going to be testifying or appearing later. And that Ken Gourlay talked him into going to a computer camp up in Michigan and subsequently molested him there according to the testimony. Did Justin tell you that Ken Gourlay molested him?

MR. EICHENWALD. Yes. And there has been nothing that has been more emotionally traumatic for Justin than in recounting the events involving Ken Gourlay. I was very surprised he was able to get through his testimony today. He has never been able to have a full presentation/discussion about what happened with Ken Gourlay without either becoming enraged or beginning to sob. And he also at one point showed me a video in which Mr. Gourlay, it was taken in Mexico in which Mr. Gourlay is in the video, walks behind the camera and begins operating the camera and the video becomes pornographic so I had no doubt that the things being described by Justin and Mr. Gourlay's involvement were--

MR. WHITFIELD. So there is no question in your mind from the evidence that you saw that Mr. Gourlay was involved in production of child pornography.

MR. EICHENWALD. Not at all.

MR. WHITFIELD. Thank you.

At this time, I would recognize the gentleman, Dr. Burgess from Texas.

MR. BURGESS. Thank you again, Mr. Chairman.

Mr. Eichenwald, do you, I think you spoke to it but there were times you were concerned for your own safety. Is that correct?

MR. EICHENWALD. I was more concerned for my children. I know people who might feel my looking at people who do accounting fraud and I normally do not have to worry about are they going to come and balance my kids' checkbooks and there was a very large emotional element in this for me in terms of dealing with the reality of what was happening to other children, seeing my own children, realizing that Justin's members in my hometown included a pediatrician, included teachers, included a lawyer who represents children and family issues. And I probably became more than a little paranoid about the safety of my own children but there were instances such as this situation with Mr. Mitchel where I was truly concerned for the safety of my kids.

MR. BURGESS. And Justin, were you concerned about your mother's safety during this time?

MR. BERRY. Throughout all of this, I was very concerned. I was very concerned about the safety of me, the safety of my little sister. I just--these people are relentless.

MR. BURGESS. And when you say there were people hunting for you at the airport in Bakersfield when you arrived, how does that occur? How does someone hunt for someone in an airport? Were you paged over the air, were there people that you recognized?

MR. BERRY. Actually, when we got to the airport, Kurt and I, my mother was there to pick us up from the airport.

MR. BURGESS. We have got five of those.

MR. BERRY. All right.

MR. BURGESS. Okay, go on, maybe six.

MR. BERRY. All right. When my mother came to the airport to pick us up, she informed Kurt and I that my father had been looking for me and Kurt as well. Whenever we arrived, she said that staying at the house was not an option because an individual had come by that previous night asking if I was there as well, and let me know what was going on in that situation when I arrived.

MR. EICHENWALD. When we arrived on our plane it was one of those situations, I failed to turn off my phone when I was in flight and as we landed, the message--

MR. BURGESS. I am shocked.

MR. EICHENWALD. Yeah, I am sorry. We landed. I immediately had a message and my phone rang, his phone rang. His phone rang with a phone call. It was his mother who was fairly frightened who was saying there are people here. There were people who had come as well as people who were up from Mexico, including his father. They had come up the night before because they were involved in these activities and we were told that there were people at the airport who were looking for Justin.

MR. BURGESS. Would you have been able to identify them?

MR. EICHENWALD. I would not have been, I will say, no.

MR. BURGESS. Justin, would you have been able to identify those people at the airport? Did you call law enforcement and say arrest these men?

MR. BERRY. Well I never saw anyone with my own eyes, no.

MR. EICHENWALD. And law enforcement as you can imagine when we were at, the Bakersfield circumstances were high pressure enough. It was immediately after these events that Justin contacted Mr. Ryan and solidified that relationship and Mr. Ryan immediately contacted the

CEOS. That is why when I say it was July 14, the reason why is we were in Bakersfield on July 13.

MR. BURGESS. Let me go back to something just for a minute if I could, Justin. I appreciate you being here and know this must be difficult but you said that someone rented an apartment on your behalf while you were still in high school or just graduated from high school?

MR. BERRY. That is correct. Gilo Tunno who was originally of Portland, Oregon, at the time. I had been contacted by this individual over the Internet instant messaging and spoken with him. He offered to come to Bakersfield, California, and rent an apartment, sign the lease in his name because I was not 18 at the time.

MR. BURGESS. But and so this was an apartment that someone rented that they allowed you to use. They did not rent you an apartment, did they?

MR. BERRY. No, they rented it for me.

MR. BURGESS. Now is it--

MR. EICHENWALD. When Mr. Tunno arrived in Bakersfield, I have the records from that apartment rental. He rented the apartment and then made sure there were two things in the apartment, Internet access and cameras. This was not Mr. Tunno's apartment. This was Justin's apartment that was rented for him by Mr. Tunno for the purpose of making sure that the shows continued. Justin's mother was coming by his room too much and so that was going to be a problem. Once the apartment was rented, there was no problem anymore.

MR. BURGESS. Now has this person been arrested?

MR. EICHENWALD. That is the individual I mentioned who was arrested subsequently for raping an 8-year-old boy. That was the fellow who was being investigated by the Immigration and Customs Enforcement agents who were trying to figure out who the kid was in Bakersfield who they believed had been molested by Tunno. And again, that was information--they only learned that Justin-- they spent 4 months of their time trying to find somebody who was already a Federal witness and they learned that Justin was a Federal witness. They learned that this boy had come forward not only saying yes, he had been molested but that there is video evidence of it in the course of an interview with me.

MR. BURGESS. Well Mr. Eichenwald, I mean you said it so eloquently, you are concerned about where are the arrests of the people that molested Justin and I guess I would ask the same question and what has been done to preserve evidence, what has been done to make certain that prosecution of these individuals is still possible?

MR. EICHENWALD. I am not sure I understand.

MR. RYAN. Let me, I want to make sure that something is clear. This particular individual is a guest of the United States before Justin

came forward to law enforcement. He was convicted based on other activities. Law enforcement did catch him, the ICE agent. We are cooperating with the case agents to help on additional work in that case.

MR. BURGESS. I see. But Mr. Eichenwald, you had or gave us testimony that Justin had said to you when are they going to arrest the people who molested me. And I guess I would ask the same question. What is being done in that regard? What is being done to hold those individuals accountable, to present evidence, to preserve evidence?

MR. EICHENWALD. I could not tell you. Again, some of the evidence regarding some of those individuals is contained on the laptop computer that Justin described to the Government back in July. No one has ever picked it up. I mean, that is why we talk about an active investigation when you say there are four hard drives, I believe it was four hard drives, it may have been six. The number of hard drives and there is a laptop computer all of which contain evidence. And they picked up the hard drives but they do not pick up the computer. I mean, it is sort of you are left scratching your head. I cannot tell you what is being done. I cannot tell you why things are the way they are.

MR. BURGESS. Well if we can get some answers when the Department is in here on Thursday. Mr. Eichenwald, I just commend what you did. A good deal of likelihood that Justin would not be alive today had you not intervened. It certainly, I mean it is a fantastic story that you just literally stumbled upon one day. Is that correct?

MR. EICHENWALD. One of the very strange things about the webcam pornography business is that if one, I mentioned the competition. If one site or one group of sites become successful, the competitors will start to launch very devious ways of attacking them. What happened for me is I came across one of these devious attempts to attack a site. I had just come back from a book tour on my last book about Enron and decided I wanted to do something international on the same area I deal with so I did a search for, a did a Google search for Interpol fraud alerts and in the course of looking through what popped up, I came across what purported to be a posting by a Tallahassee law firm about an Interpol investigation involving eight, I believe it was State Attorneys General who were looking at fraud, a fraud case involving a series of websites.

Most of those websites were a credit process or many of those websites were credit card processors. The posting was detailed, I was delighted. This was a story that was wrapped up in a bow. I just had to figure a little bit out. I would call the law firm and I have something in the paper. As I went down looking at what each site was I came across a site called Mexicofriends. Given that it was a fraud case and it was called Mexicofriends, I thought money laundering, there was something good here. Mexicofriends at that point was a dead site so I stuck the

word Mexicofriends into Google as a single word, and found a bunch of people talking about somebody named Justin who was obviously a porn star. I did not understand what, that had to do with fraud, but it sounded like it was getting to become a more interesting story on some level.

And eventually once I had what I could get out of those listings, I went to something called archive.org which is a site that preserves images of old websites and in the course of looking at what are these things that I have not been able to find, I put in mexicofriends.com and up popped an image that it looked like something you would find in a seventh grade school book. It was not pornographic, it was a photograph of Justin at the age of 14. Now right now he is 19 and I think he looks about 16. When he was 14, he looked like he was about 12 or 11. And as I am looking at that, I very quickly came to realize that this image, this person I am looking at was Justin. Is the person who I had already knew was some sort of porn star. And the level of disconnect in my head was huge. I did not know what I was looking at, what I was dealing with. I do know that I was abjectly horrified. And I did not at that time think wow a news story. In fact, my thought was I have to figure out if this is real.

And about that same time I found out that the original posting, the Tallahassee law firm I was going call, the Tallahassee law firm and say well what is this and what about this kid, it ended up that the original posting was a fake. It had been posted, I believe by a competitor to a number of sites that use different credit card processors to say there is a criminal investigation so all the customers should not go there, they should come over here. I subsequently understood the bulletin board it was posted on was one used by webcam operators.

So once I realized that was fake, now I just had a kid out there wrapped up in child porn but maybe that was false too because all I had was an image that could have been cropped out of any seventh grade school book and I began trying to figure out if it was real, not for the purpose of doing a story because truthfully I did not, it did not occur to me there would be a story there, not bother to get law enforcement. There was a posting for Justin's instant message address. Actually, there were postings for his email which he never responded to any of them, apparently he did not use them anymore. And then there was a posting for his instant message address. I put that in my buddy list. He eventually signed on. I tried to contact him twice. Both times I was too aggressive in my questioning. I started off by saying something like how old are you and he immediately blocked me. But after that, I went onto a third screen name and tried a much slower approach and it was not until a number of days after that, I cannot tell you how long it was when I finally became convinced that he was a real person and that he was a real

teenager because I was asking him what do you want to accomplish in your life? What is it you want to do? And he replied I want my mother and my grandmother to be proud of me. And at that moment, I knew I was dealing with an abused, sexually abused child. And subsequent to that, made a rapid arrangement to meet him in Los Angeles at which point I revealed, and at that point I began to realize there was a story here and I was in the problem of not having identified myself as a reporter. So when we met, I immediately identified myself as a reporter, explained who I am, what I do, and after about an hour of questions from him and then began asking him details about this webcam world.

MR. BURGESS. Mr. Chairman, you have been very generous. I just would ask if I could ask a question to be answered in writing by Mr. Eichenwald. I know you must have thought about the issue of freedom of the press for a place like Myspace and yet restriction of online predators and I actually would be very interested in the journalist take on freedom of the press versus controlling the abuse of the Internet for child pornography.

So with that, I will yield back.

MR. WHITFIELD. At this time, I recognize the gentlelady from Tennessee, Mrs. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman. I appreciate that and I am going to be respectful of your time and of the committee member's time today. We truly appreciate the time that you have given.

Mr. Eichenwald, your series is riveting and having read through that it is well done. I am glad you did it. But you know, I think that reading it and listening to you and Justin today, it just shows us time and again the frustration that our constituents have and rightfully so many times in trying to deal with the Government, in trying to deal with government agencies, and trying to deal with the bureaucracy, whether it is with this issue or whether it is with other issues. And I thank you for what you did and for the accountability that you have called us into by placing some criticism and some questions and laying those on the table for us to consider. Addressing the moral security of this Nation, there is nothing greater that we do. And it is a responsibility that we take as being a very important responsibility and our constituents should be able to trust that we are mindful of the need to protect and address the moral security of this great Nation.

Mr. Eichenwald, reading your articles and then looking through the testimony and I know you said that it is hard to get in here and kind of quantify the scope of online child pornography and you mentioned there are five, you had at least 585 sites that were created by teenagers. Is that correct?

MR. EICHENWALD. That is an internal listing off a single portal. I have actually provided that listing to the committee.

MRS. BLACKBURN. And so that was one portal.

MR. EICHENWALD. That was one portal.

MRS. BLACKBURN. Wow. Okay, and do we have any way of knowing when you are on the Internet, when you go through one of the servers how many sites there are that deal with child pornography? Do we have any idea of the scope of the number of those sites?

MR. EICHENWALD. I have, I know that what I have read in the interviews with law enforcement and interviews with folks from the National Center for Missing and Exploited Children whatever number we were to pick today would not be true tomorrow because the number is growing and growing very, very quickly. I just saw last night in fact that there is an organization that basically does Internet security and spam, capturing spam and one of the interesting things they do is they analyze the spam that they capture. And just last night, I saw this, they have come out with a report that the fastest growing piece of spam they are getting now is for new child pornography sites.

MRS. BLACKBURN. Okay. Now do we know how many of those within this universe of new sites that continue to pop up on an ongoing basis, do we have any idea if most of those sites are housed on U.S. soil or offshore?

MR. EICHENWALD. The best analysis actually comes out of Britain. Right now the British are from what I have read, the British identify two areas of the world as being the primary locations for the production of child pornography. Eastern Europe is number one and the United States is number two.

MRS. BLACKBURN. Okay, I thank you. Thank you very much.

Justin, how long--and I never found this in your reading. How long did it take before you mom picked up that something was not right with all of this new equipment and your attraction to the Internet? How long did it take her to kind of chew into this?

MR. BERRY. Up until recently here, when I told her.

MR. EICHENWALD. And if I could add in, I mean, Justin's mom, you know, he comes at--what happened when he was 13 and 14, he was a 13 and 14-year-old. I hear about it as a parent. His mom began to notice there were problems, that he was not acting quite the same way, that he was behind closed doors more often she tried to get him to come on out, open the door, she began to sense he was withdrawing. She took him to see a mental health counselor who diagnosed him at the time as having ADD which he does not have. In fact, at the time, from what I have heard the belief now is that he was already experiencing problems from trauma, from the trauma of what was happening to him. And in terms of



the equipment, he did have his own website development company and he was actually designing websites through real companies and actually getting paid for it. And so it was not unusual for him to have money or equipment. You know he could hide the more outrageous sums and just make sure that anything that she caught onto he would just say well that is from my website development business.

MRS. BLACKBURN. Okay. Mr. Ryan, let us go to the cell phone records. I think that all three of you mentioned that one of the predators, Mr. Mitchel had purchased Justin's cell phone records. Do you know what avenue he traveled to purchase those records?

MR. EICHENWALD. I do not know if he purchased them or not. I just know that he--

MRS. BLACKBURN. He had those.

MR. EICHENWALD. He suddenly was instant messaging Justin; a phone that he believed reached Justin but it was actually reaching me. He instant messaged my home phone number.

MRS. BLACKBURN. Okay. Well the cell phone record issue is one that this committee is addressing and whether it is pedophiles or identity thieves or drug traffickers or those that would seek to do an individual harm getting access to those records. That is something that is of great concern to us.

I want to again thank you all for your time and for being here.

And Mr. Chairman, I will yield back my time so that we can move onto the other panels today but I thank you. We will have some other questions that we will submit to be answered in writing.

MR. WALDEN. [Presiding] Thank you. The gentlelady yields back her time.

I want to thank all of you for being here today obviously. And Mr. Eichenwald, I read the comments that you gave in a speech to Marquette University where you were somewhat less than kind, but obviously truthful about your views regarding CEOS. And in those comments, you said it became obvious no matter how urgent the situation, no matter how many times CEOS was told that the witness's life was in danger, no matter how many times they were told of other children in peril, no matter how many times they were told about evidence being destructed, they would not act with any exigency. Is it as bad as you say it is?

MR. EICHENWALD. I can only speak to this circumstance.

MR. WALDEN. Right.

MR. EICHENWALD. And in this circumstance it was as bad as I say it is. It was very hard to understand. And I need to take a step back and let you recognize the strangeness of this situation. There has been a wide belief that the New York Times made the decision to persuade Justin Berry to become a Federal witness because we were offended by the fact

that there were people who paid him for pornography. That is completely untrue. I would have been delighted to simply write the story and expose this but when Justin began to reveal that there were real children that he knew of who were being harmed and exploited and abused by real adults that he knew of and proceeded to show me evidence of this or certainly things that were suggestive that this was happening, I went to the executive editor and said we cannot just sit here and work on a story while children are being molested and raped. And so I was authorized to go back and tell Justin you need to become a Federal witness. The whole idea that there would be some huge delay when someone is coming in and saying this is what is happening, I have personal knowledge of it, I being Justin. I mean there is one of the individuals, probably the individual he was most worried about I know from a filing in Mr. Mitchel's case that the Government obtained a videotape of this boy on July 26, the second day that Justin Berry was speaking to them. And so they were--

MR. WALDEN. That was a result of that discussion?

MR. EICHENWALD. As a result of that discussion they were aware that this existed. They knew that Justin specifically knew this kid. And they knew that he had said a man who molested me was in the room when that video was taken and other videos are being filmed. There was where Justin had a very difficult day when a video of that kid was posted that had been filmed obviously in a hotel room. And it was a question of how bad is this going to get. And so during that whole period of time, the difficulty for me was not having enough to write. Not having--I cannot prove anything yet.

MR. WALDEN. Right.

MR. EICHENWALD. My reporting was not sufficient, but knowing in my gut and in my heart what is going on and also knowing that all anybody had to do was go serve a search warrant and they would have all that they needed.

MR. WALDEN. And 1,500 names and credit card information data points that were given to the Justice Department and all the other information that you brought forward, do you know if the Department of Justice has arrested any of those people? Justin, do you want to--

MR. BERRY. I know that Mr. Mitchel has been under arrest, Mr. Tunno has been previously arrested. He is working with that on a different case.

MR. WALDEN. Right.

MR. BERRY. Mr. Richards is another individual who was endangering children and there are others that have molested me that have not been arrested.

MR. WALDEN. All right.

MR. EICHENWALD. I would also mention that Mr. Tunno's arrest had nothing to do with this case.

MR. WALDEN. Right, yeah, I understood that from the other testimony.

Mr. Ryan, you were a Federal prosecutor. Correct?

MR. RYAN. Yes, sir.

MR. WALDEN. I am not an attorney but explain to me this affidavit process. When the affidavit was released and made public--

MR. RYAN. Congressman, it is very traditional in law enforcement. There is a covert phase of your investigation and the covert phase is very, very important because during that covert phase, you can get ready, for example, to serve search warrants in Boston.

MR. WALDEN. Right.

MR. RYAN. And in Roanoke, and in Bakersfield all at the same time. And we are very good at that as a Justice Department.

MR. WALDEN. Right.

MR. RYAN. I mean as a youngster, I was taught the business by agents and older prosecutors. In this case, an affidavit that depended on Justin's testimony was the basis for the arrest warrant and search of Mr. Mitchell's residence. That was a very important case and I credit the Justice Department and CEOS for prioritizing that.

MR. WALDEN. Okay, but what about the release of that information and the exposure of Justin and the exposure of these other men.

MR. RYAN. That case it was unforgivable in my opinion.

MR. WALDEN. But has it been resealed today?

MR. RYAN. No.

MR. WALDEN. Should it have been resealed?

MR. RYAN. Yes.

MR. WALDEN. If you were the prosecutor in charge, what would have happened?

MR. RYAN. If I had been anywhere near this case, I would have just immediately filed a one page application with the court to reseat the affidavit.

MR. WALDEN. And have you asked the Justice Department to reseat this or was that your role?

MR. RYAN. I said unprintable things to the Department of Justice when this was released. I asked them why frankly they could screw up a one car funeral by--

MR. WALDEN. What was the reaction to you about A, releasing this and B, did you make a request that it be resealed and what did they say if you did?

MR. RYAN. The conversations on that, I would have to--let me try and recall them as best I can for the record but the bottom line is nothing happened. And--

MR. WALDEN. So you did ask them to reseal and they have not resealed?

MR. RYAN. You know, I do not recall asking them to reseal it. I do remember telling them at the time that it was an outrageous piece of malpractice--

MR. WALDEN. Did they explain why they released the information--

MR. RYAN. There is a letter that is the best department explanation that I received last night at 5:00.

MR. WALDEN. And what does that letter say and could you provide it for the committee?

MR. RYAN. I can.

MR. WALDEN. Mr. Ryan, it is intriguing to me. This happened in September, right, that the affidavit was released?

MR. RYAN. Yes.

MR. WALDEN. And you got the letter how many hours before our hearing?

MR. RYAN. Well I raised it in a different context. Mr. Berry was never contacted to participate and provide a victim witness statement in the sentencing of Mr. Mitchel and I thought that since the Department had relied on his information to obtain the arrest and search warrant that they would be interested in using him as the key victim because he had been abused by Mr. Mitchel and it was in that letter that I pointed out, I guess ironically, that the Department had released the affidavit, they might want to come back and ask us for the information so that the court would know about the abuse.

MR. WALDEN. All right.

Mr. Berry, I just have less than 2 minutes and I have to ask you what may be a difficult question for you to answer. But you have testified that during a certain summer, Mr. Gourlay who I think is here in the audience, took you to his home and sexually molested you, you were 13 years of age. And he was what, in his 20's at that time?

MR. BERRY. I believe so, yes.

MR. WALDEN. And were you scared? Were you upset?

MR. BERRY. Upset is not even the word.

MR. WALDEN. And he promised it would never happen again and yet it did?

MR. BERRY. That is correct. He promised me it would never happen again and it did.

MR. WALDEN. And he took advantage of you again. The question, I think probably a lot of parents have is having been through what you

have been through, having seen that happen and happen again, why were you not able to cut off contact with Mr. Gourlay? And this is not an attack on you, but what is it that allows somebody to grip you like that to the point that you were scared, you were upset, you were all these things and yet being in your life.

MR. BERRY. As a 13-year-old being molested and abused, I do not know exactly what my thoughts were. All I know is that I buried those emotions until recently and right now it really hurts.

MR. WALDEN. What advice would you have for other young people who may be in a similar predicament? How could they break it off where at that age you were not able to? What would you tell them?

MR. BERRY. Yeah, truthfully I am not too sure. I am really not. I do not know if I would listen myself. I was pretty stubborn as a kid as most teenagers are.

MR. WALDEN. I understand that. All right, well thank you for your courage and for being here today. My time has expired.

The Chair recognizes the gentleman from New Jersey.

Actually, Mr. Ferguson, we are going to recess for 5 minutes to take a bit of a break and give our witnesses a bit of a break. We forget that sometimes and the committee will resume its business in 5 minutes.

[Recess.]

MR. WHITFIELD. The hearing will reconvene and the Chair will recognize the gentleman from New Jersey, Mr. Ferguson, for his 10 minutes of questions. Mr. Eichenwald is coming back in so Mr. Ferguson you are recognized.

MR. FERGUSON. Give Mr. Eichenwald a chance to take his seat.

MR. EICHENWALD. My apologies.

MR. FERGUSON. Get back settled, not at all.

Mr. Eichenwald, in your testimony, you referred to sites like mspace.com and buddypick.com and you called them a virtual Sears catalog for pedophiles. Can you explain why that is the case and if you would, would you try and be concise? Why do you believe that is the case?

MR. EICHENWALD. Kids put up the images. They put up their contact information, many times to attract attention to their site; they pose in provocative ways. There will be shirtless shots. There will be everything there to suggest which kid is comfortable with what. And whenever there is a kid who is found who is more explicit than the usual, not illegally explicit, just explicit, just sexualized, I have watched these conversations. Those kids begin to be discussed by the predators. There are postings about them and the links to their sites are posted.

MR. FERGUSON. I know you said that you were not here to make public policy recommendations, I understand that. But what do you believe the ISPs should do with regard to these sites?

MR. EICHENWALD. The ISPs have a responsibility. I truthfully do not know. I mean the reason I do not make public policy pronouncements is because I simply do not know the mechanics and mechanisms. And ultimately, I am not sure what an ISP is capable of doing or should be required to do. I think I would say Steven Ryan knows a lot about that.

MR. RYAN. Congressman, I think this is--

MR. FERGUSON. Just pull the microphone closer to you, please and turn it on.

MR. RYAN. My technological guru. Congressman, I think the legitimate ISPs do a lot in this area. The problem of course is they have to balance the rights of privacy of legitimate subscribers and also not invading communications. I think it would be very useful for the committee frankly to have a roundtable discussion without the press here, with staff, with the Members coming in at the end to find out what the ISP industry can do in this area. I really do think that industry could be an important partner with law enforcement. There is a center that has been established in Pittsburgh that is a cooperative center between State and Federal law enforcement and in my corporate capacity when I am representing corporations, we have established relationships with that Internet clearinghouse center for law enforcement and we do make referrals there. So I think there is important work that is being done by the private sector with the law enforcement community in this area. I think it would benefit the committee to know more about that.

MR. FERGUSON. Okay, I appreciate that.

Justin, Mr. Berry, your testimony, you mentioned that child predators over the Internet are laughing at law enforcement. What do you mean when you say that?

MR. BERRY. When I was still in this business, I talked to or spoke with one of the child predators and told them I was going to turn them in to law enforcement. Their response to that was they laughed at me and they told me that I would be the one in trouble. And that I would be the one being prosecuted for child pornography. I wish I could say that would be true or would not be true. These people, the law enforcement efforts I do not know what is going on in all the cases. All I know is what is going on in this case and it seems that they are right.

MR. FERGUSON. These folks are technologically savvy.

MR. BERRY. Some are, some are not.

MR. FERGUSON. I am talking about the folks that you described as the predators, the folks that are laughing at law enforcement. These are folks that are Internet savvy, they are technologically savvy.

MR. BERRY. Like I said, some are, some are not.

MR. FERGUSON. Why do you think it is difficult for law enforcement to find these folks, the folks that are making and distributing this material and buying these images of children?

MR. BERRY. Maybe asking them would be a better question. I do not know if--

MR. FERGUSON. Well we will. I promise we will. I wondered if you maybe had any theory or any thoughts with regard to this.

MR. BERRY. I have been heavily disappointed by what has happened in regards to this case. And I can see if that is a reflection on the United States and how they feel and how they prosecute child pornographers, well I can see why they would feel that way.

MR. EICHENWALD. Congressman, there is one individual I would strongly recommend the committee speaking with. I will have to get you his name later. He is an art professor at a university who as an experiment in 2000, spent many months trafficking among the predators basically doing what I have been doing and watching their conversations. And actually it was from what I interviewed him in the course of my article and he is the first one who told me about how the predators truly laugh at the Federal enforcement effort. That they believe the only people who get caught are the ones who are just too dimwitted to figure out how to handle the situation. A lot of it does have to do with the technological capacity of the people who are the predators. They share information on how to avoid leaving footprints, how to avoid leaving any evidence that they have been to sites, any evidence of what they put on their computers. Mr. Tunno, who we have heard about a number of times, who is involved in this situation, actually had invented a computer that had no hard drive so when it was unplugged from the wall, the illegal images or whatever other evidence was on the computer would disappear. These are smart people. They are sophisticated people. They know that, if child pornography is what they want, they know how to get it, requires them to be technologically sophisticated and unfortunately they are ahead of the game.

MR. FERGUSON. I am advised by staff that professor's name is Philip Jenkins.

MR. EICHENWALD. That is it, yes.

MR. FERGUSON. He has been interviewed by the committee staff. That is the professor you were talking--

MR. EICHENWALD. He is a wonderful resource because he is a person who has been for many months and he wrote a fabulous book

about this--for many months talking with these people and his information dates back to 2000. But from a historical basis in particular, it really underscores the obsessive nature of the online predator as well as the technological sophistication and their contempt for Federal law enforcement.

MR. FERGUSON. Now Mr. Chairman, we are obviously continuing our investigation into this subject and I would imagine and I would hope frankly as we learn about whatever inadequacies there may be in the law, that as we look at legislation to correct and address problems in the law in terms of prosecution, information available to those clearinghouses and whatever else, I would respectfully suggest that we might name that legislation for Justin Berry. He has been through a lot and he has experienced a lot. He has done some difficult things and courageous things. By his own admission he has made mistakes and it has taken a lot for him to appear before the committee today. And I would hope that we would consider that.

I have a couple of more questions for Mr. Berry. What do you think would be a fair sentence for the men that you say molested you?

MR. BERRY. These people, these predators are not going to stop. If you arrest them, they are going to go back and find another kid and they are going to keep doing it until they are put away. I would hope they would get life.

MR. FERGUSON. You testified, Mr. Berry, that you now see Ken Gourlay's molestation of you as the beginning of your downturn, the beginning of this spiral that you entered into in your teenage years. Why do you think that?

MR. BERRY. When I was molested by Ken, before that I was a happy kid. I went to school, I played in sports, I had a few friends. Afterwards, now that I look back in retrospect, my life from there on has changed dramatically. I would have never imagined I would have done the things that I have done and I am not proud of it. I cannot say exactly how it affected me, all I know is to this day right now I am seeing a psychologist and I am a pretty messed up kid.

MR. FERGUSON. Thanks very much for being here today and we appreciate your testimony. Mr. Eichenwald, we appreciate your testimony as well the work that you have done in uncovering this situation.

And I yield back, Mr. Chairman.

MR. WHITFIELD. Thanks, Mr. Ferguson and we appreciate your suggestion and I do think that we obviously are going to be looking at legislation to enforce the firewalls relating to this issue and it is a complex issue and we will need to work on that. Your suggestion in



naming that after Justin Berry is something we definitely will consider and will follow.

Mr. Walden?

MR. WALDEN. Mr. Chairman, if I might.

Mr. Berry is there anybody in this room who you believe molested you?

MR. BERRY. Yes, Ken Gourlay.

MR. WALDEN. Thank you.

MR. WHITFIELD. Are there any other questions of this panel? Okay, well I am going to thank the three of you very much for your time, for your testimony. Justin, we know that it was quite difficult for you and we look forward to staying in touch with you through our committee and wish you the very best in pursuit of your college degree. And Mr. Ryan, thank you very much for your testimony. And Mr. Eichenwald, we once again thank you for the articles you wrote in the New York Times to focus attention on this issue.

And with that, we will release this panel and we will call up the next panel which will actually be the third panel. And that is one person and that is Mr. Ken Gourlay who is accompanied by his attorney. I believe his name is James Rasor with the Rasor Law Firm in Royal Oak, Michigan.

And Mr. Gourlay, if you would have a seat at the table. Now Mr. Gourlay, you are aware, you have watched the other panels and you are aware that the committee is holding an investigative hearing and in doing so we have the practice of taking testimony under oath. Do you have any objection to testifying under oath today?

MR. GOURLAY. No, sir.

MR. WHITFIELD. Under the rules of the House and the rules of the Energy and Commerce Committee, you are entitled to be advised by legal counsel about your constitutional rights. Do you desire to be advised by counsel during your testimony today?

MR. GOURLAY. Yes, sir.

MR. WHITFIELD. And would you identify your counsel for the record, please?

MR. GOURLAY. Mr. James Rasor.

MR. WHITFIELD. And you are Mr. Rasor?

MR. RASOR. Good afternoon, Mr. Chairman.

MR. WHITFIELD. Okay, thank you.

MR. RASOR. Jim Rasor of the Rasor Law Firm in Royal Oak. A pleasure to be before the committee today.

MR. WHITFIELD. Okay.

MR. RASOR. And I think this has raised some very interesting questions in testimony.

MR. WHITFIELD. Thank you. Now I want to make it aware that the legal counsel will not be testifying in this panel but will be here for the purpose of the advising Mr. Gourlay on his constitutional rights.

[Witness sworn]

MR. WHITFIELD. You are now under oath, Mr. Gourlay and do you have an opening statement that you would like to make?

MR. GOURLAY. No, sir.

MR. WHITFIELD. All right. Mr. Gourlay, you heard Justin Berry testify under oath that you initially contacted him online when you saw him on his webcam and then you continued to contact him through instant messaging regarding his interest in computers. He was a 13-year-old boy at the time and you were a man in your 20's. According to Mr. Berry's sworn testimony today you invited him to attend a computer camp near your home in Michigan and during that trip you sexually molested him, the 13-year-old boy, for the first of what would be many times. In addition, Mr. Berry testified that you and your company, Chain Communications or [www.thechain.com](http://www.thechain.com), were involved in commercial enterprise which made money from the sexual exploitation of minor children over the Internet. Mr. Gourlay, did you ever have sexual contact with Justin Berry when he was under the age of 18 years old?

MR. GOURLAY. I will decline to respond based on Fifth Amendment privilege.

MR. WHITFIELD. Are you refusing to answer any questions that we may ask you today based on the right against self-incrimination afforded to you under the Fifth Amendment of the U.S. Constitution?

MR. GOURLAY. Yes, sir.

MR. WHITFIELD. And is it your intention to assert this right in response to all further questions from the subcommittee today?

MR. GOURLAY. Yes, sir.

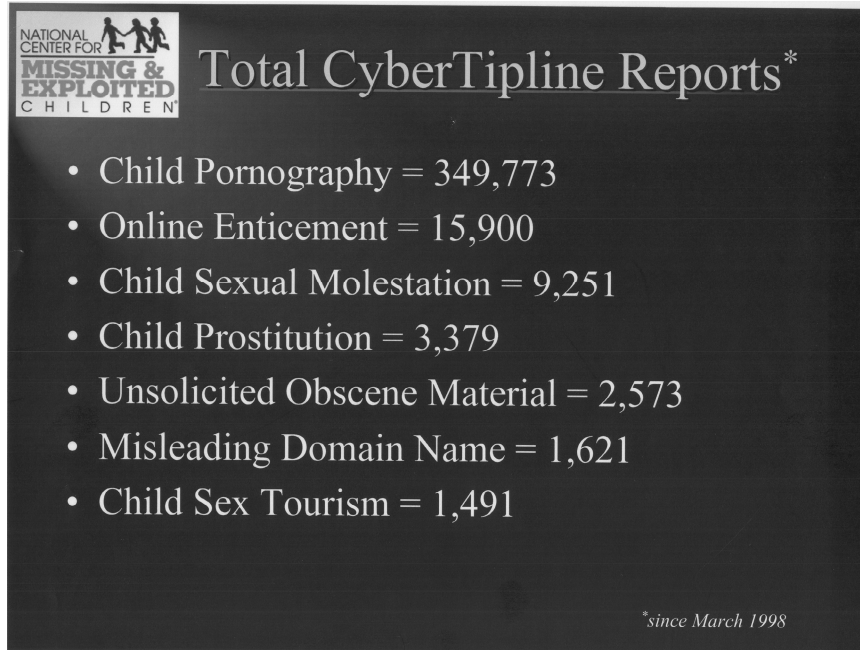
MR. WHITFIELD. Given that if there are no further questions from the members, I will dismiss you at this time subject to the right of the subcommittee to recall you if necessary. So at this time, you are excused.

Okay, at this time, I would call up the fourth panel of witnesses and that is Mr. Ernie Allen who is the President and Chief Executive Officer for the National Center for Missing and Exploited Children and is located in Alexandria, Virginia. Mr. Allen, we appreciate your being here today. I have enjoyed our conversations with you prior to this hearing and the great work that your National Center for Missing and Exploited Children is performing and I would like to recognize you 5 minutes for your opening statement on this important subject matter.

**TESTIMONY OF ERNIE ALLEN, PRESIDENT AND CHIEF  
FINANCIAL OFFICER, NATIONAL CENTER FOR  
MISSING AND EXPLOITED CHILDREN**


MR. ALLEN. Thank you, Mr. Chairman, members of the committee. I am delighted to be here as you discuss this important issue.

I have submitted written testimony but per your request, I would like to do a brief summary focusing particularly on the scope of the problem of child pornography. You have heard from other witnesses this morning that this is an exploding problem not just in the United States but around the world. You have heard that the latest estimates are that commercial child pornography is a \$20 billion industry and non-commercial child pornography is an even larger share of Internet child pornography. But I would like to make a couple of key points that I think are important to this Congress. One is that while this is a global phenomenon, we believe that the majority of the consumers are Americans. Secondly, we believe that the majority of the victims are Americans, and we also believe that the age of the victims being used and exploited in child pornography is becoming younger and younger and the images are becoming more graphic and more violent.



What I would like to do briefly is direct your attention to the screen. You have asked for some visual information. As the committee knows,

in 1998, the Congress asked our center to become the 911 for the Internet on these kinds of issues. We have created a Cyber TipLine that has handled 385,000 reports of child sexual exploitation; 350,000 of those reports are on child pornography alone.

A graphic titled "NCMEC Statistics" with the logo for the National Center for Missing & Exploited Children. The logo features three stylized figures of children. The statistics are listed in a white font on a dark background. To the right of the text is a close-up, high-angle photograph of a computer keyboard, showing keys like F10, F11, F12, Backspace, Enter, and Shift.

**NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN**

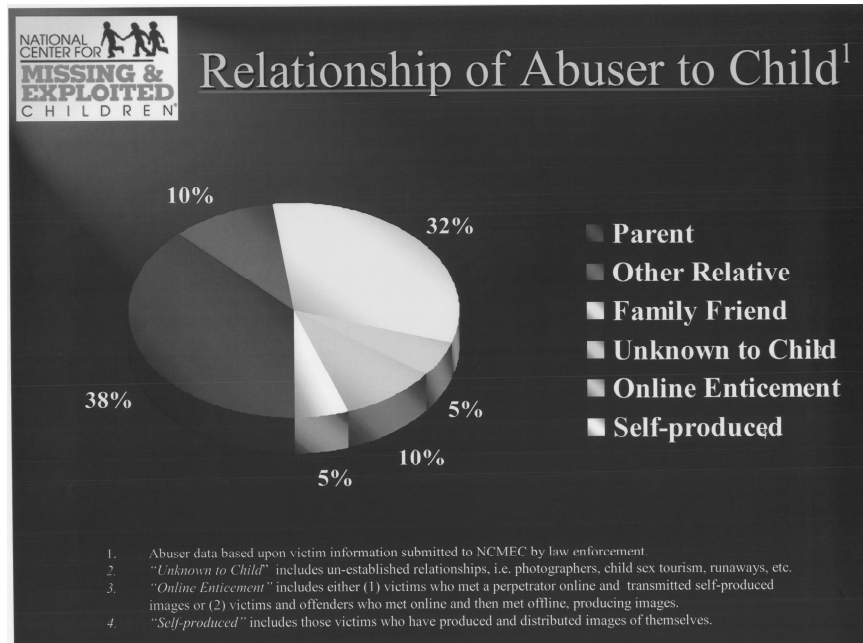
## NCMEC Statistics

- 660+ Identified Children
- 5,000+ Requests for Victim Identification
- 3.7+ Million Images/Videos Processed thru CRIS
- 10,000+ *Child Pornography Evidence Guides* distributed to LE in the past year

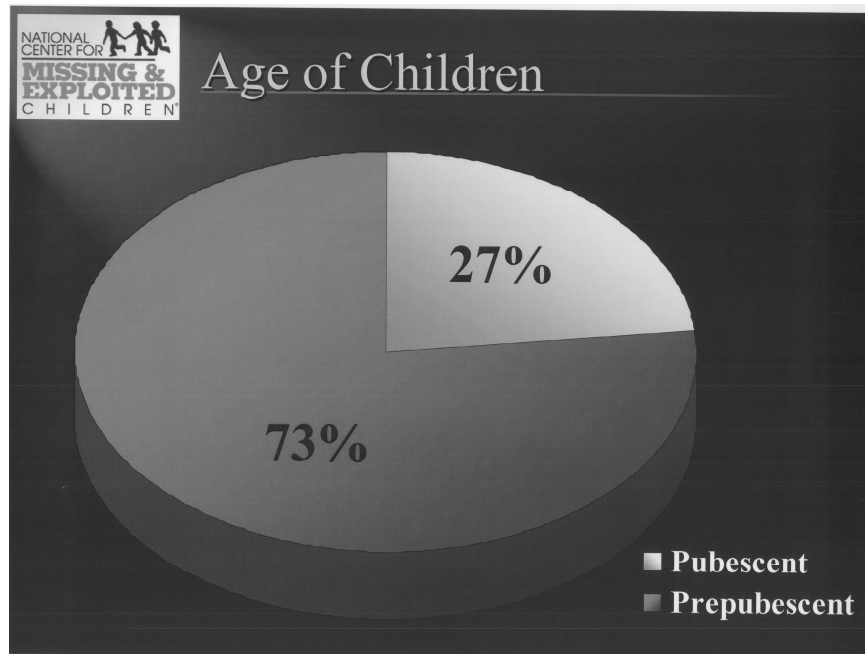
MR. WHITFIELD. Excuse me, Mr. Allen, what was the year that you started this?

MR. ALLEN. In 1998. But just to give you an idea, the first year of the Cyber TipLine we handled 4,800 reports. In 2004, we handled 112,000 reports. So this is a growing phenomenon.

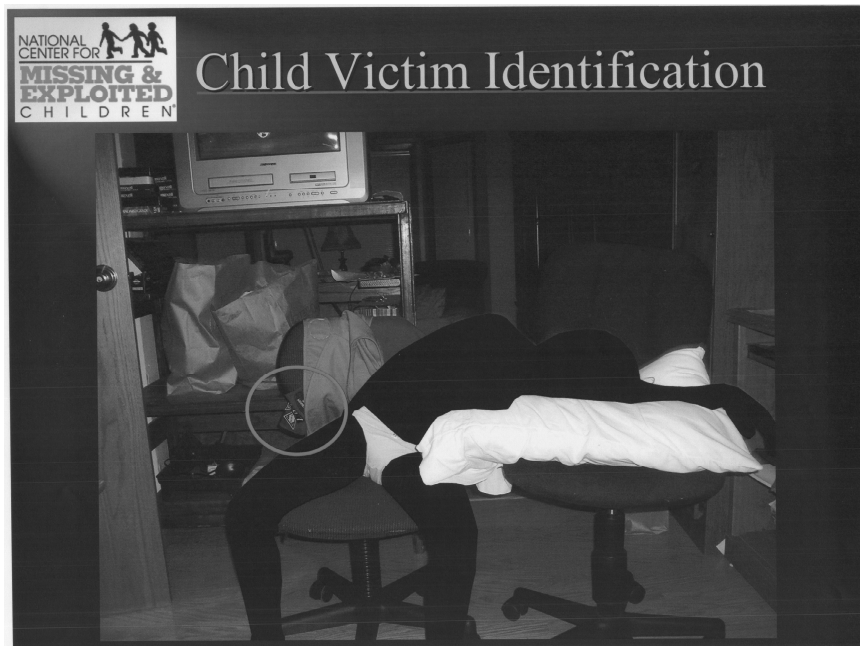
One of the key issues we are trying to address is who these children are. In the aftermath of the Ashcroft Decision by the Supreme Court 3 years ago, increasingly defendants are now arguing these are not real kids. These are virtual images. So judges and prosecutors are asking that we try to figure out who these children are. We have been able to identify working with Federal law enforcement in the United States and law enforcement around the world, 660 children have been identified but we have reviewed 3.7 million images so this is a huge and growing phenomenon.



One of the other points I would like to make to the committee is that overwhelmingly the perpetrators of these offenses are not strangers to the children. Almost half of the offenders have been members of the child's family. Another 32 percent have been family friends and associates. The phenomenon that we talked about in Justin's panel that preceded this, the sort of self-produced images, that covers 5 percent of the reports we have received but is a growing share of the problem with the advent of the webcam and other technology.



The age of the children who we are identifying in these images, 73 percent of the victims had been pre-pubescent. And of the offenders that we have identified, 39 percent of the offenders have had images of children younger than 6 years old, 19 percent younger than 3 years old.



Now a couple of quick examples. I talked about the importance and in each one of these cases obviously we have eliminated any possibility of identifying who the children are. In the recent case, ICE agents made a child pornography arrest involving an offender but there were six young girls in these images who we were not able to identify rapidly. What our center is trying to do is to place these children somewhere on planet Earth so we can identify the appropriate law enforcement agency. In this case, there was some evidence in the background, a television set with an advertisement that enabled us to narrow, identifying the company that produced this cup to narrow the focus to several Midwestern States; a grocery bag on a shelf that similarly helped us hone in on where these children were; an envelope on a desk that enabled us to reduce the focus to one city. And then in one of the images, it is very difficult to see but there is, the child had had--she was drugged and had her Brownie or Girl Scout uniform removed. Through enhancing this image, we were able to identify the last two digits of the scout troop. And through the other information and in localizing the information, we were able to identify the six children and the offender who is currently being prosecuted in that State. This is an ongoing challenge.

**Membership Information for Illegal Site**

**Join page**


**IMPORTANT!**  
Specify your REAL e-mail address to receive your login information!  
Your inquiry will be processed and you will receive information to your e-mail.  
If you use anonymous proxy server your transaction may be declared as a fraud.

\*E-mail:  
\*Password:  
\*First Name:  
\*Last Name:  
\*Billing Address:  
\*City:  
\*State/Province:  
\*Billing Zip:  
\*Country:  
\*Phone Number:  
\*Credit Card number: \*CVV:  
\*Bank name:  
\*Exp. Month: \*Exp. Year:  
\*Select membership option:  
79.99 (per day/month/ship)

**SUBMIT**

I want to give you just a quick example of the kinds of sites that are out there. And we are currently working with law enforcement not only

State and Federal but around the world to identify these sites and then use every legal means to shut them down. This is one example. This is-- obviously we have removed images from the sites--but this is an active child pornography website. As you can see, you are encouraged to join. This is a fee-based commercial site, \$150 a month and you are offered the opportunity to provide credit card information or other method of payment information. What is happening in so many of these cases is that the individuals are purchasing access to this illegal content, using credit cards and other methods of payment information and we are working very hard to end that. Credit card information--it is hard to see from here, it is on the bottom of the screen.



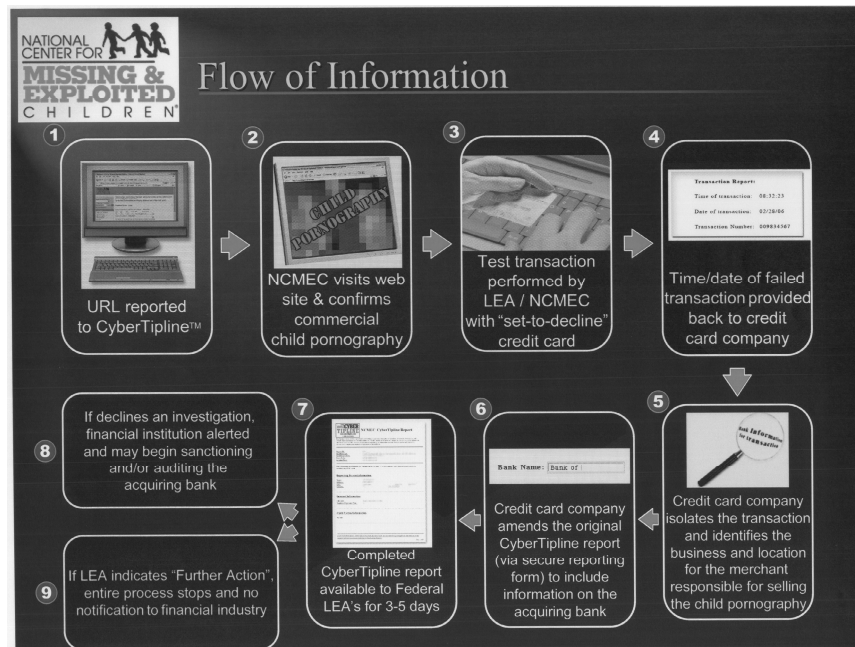
## List of Financial Coalition Companies

<p><u>MEMBERS</u></p> <ul style="list-style-type: none"> <li>• America Online</li> <li>• American Express Company</li> <li>• Bank of America</li> <li>• Chase</li> <li>• Citigroup</li> <li>• Discover Financial Services LLC</li> <li>• e-gold</li> <li>• First Data Corporation</li> <li>• First National Bank of Omaha</li> <li>• MasterCard</li> <li>• Microsoft</li> <li>• North American Bancard</li> <li>• PayPal</li> <li>• First PREMIER Bank/ PREMIER Bankcard</li> <li>• Standard Chartered Bank</li> <li>• Visa</li> <li>• Wells Fargo</li> <li>• Yahoo! Inc</li> </ul>	<p><u>COLLABORATORS</u></p> <ul style="list-style-type: none"> <li>• Child Focus</li> <li>• European Federation for Missing and Sexually Exploited Children</li> <li>• International Association of Internet Hotlines (INHOPE)</li> <li>• U.S. Office of the Comptroller of the Currency</li> <li>• DLA Piper Rudnick Gray Cary</li> </ul>
<p><u>SUPPORTERS</u></p> <ul style="list-style-type: none"> <li>• Cybrinth</li> <li>• G2</li> <li>• Potomac Counsel LLC</li> <li>• The Fairfax Group</li> <li>• Omnitech, Inc.</li> <li>• The Smith-Free Group</li> <li>• Yoran Associates</li> </ul>	

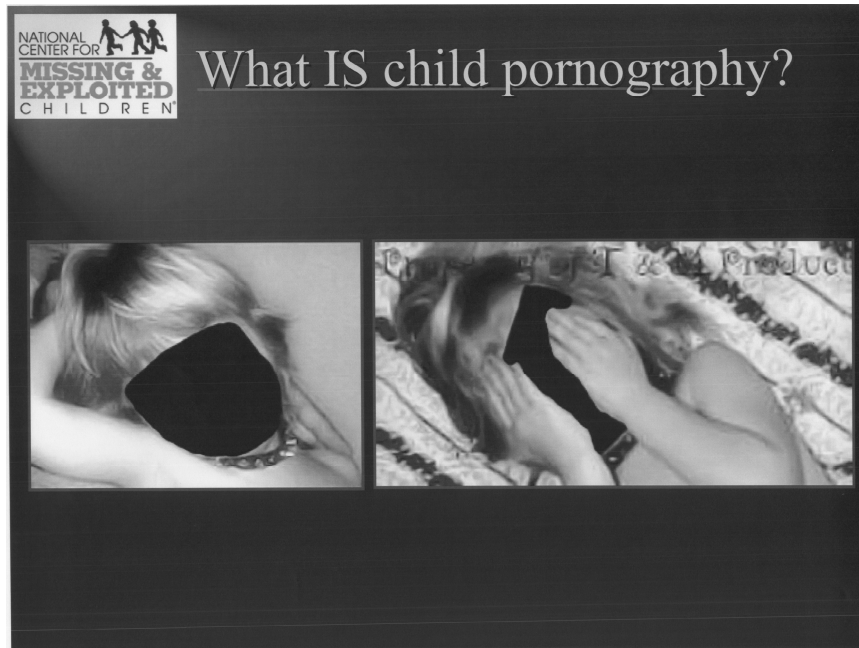
One of the steps we have tried to take, I know in the earlier panel you talked about the difficulty of prosecution and law enforcement simply because the magnitude of the challenge is so great. What we have tried to do is to create a financial coalition. We brought together credit card industry leaders, banking leaders, Internet industry leaders with the premise that you cannot possibly prosecute everybody. And at a minimum, what we can do is following the money, stop the payments under existing terms of service agreements under existing law, and shut these sites down. If we take away the profitability, it is going to be very difficult for them to sustain themselves. And the process that we have developed just to show you quickly, we are going to use our Cyber



TipLine to identify the reports, aggressively identify these sites. Once that is done, our analysts will visit the sites and confirm that it is illegal child pornography. Then what we will do is work with Federal law enforcement to perform test transactions.



What the financial industry has told us is that credit card companies do not often know what the purchase is for. If we can identify the merchant bank for them in a timely way, they can use their legal leverage to stop the payments and use their licensure provisions to put the pressure on the banks to terminate these relationships. Once we have done that, the companies will provide us the details of that transaction, the credit card company will isolate the transaction and the location of the merchant. The credit card company will amend the information in the database and one of two things will happen. We are going to provide it to law enforcement for 3 days so that law enforcement can make a determination of whether it wants to initiate a criminal investigation. That will always be the first priority. But if it does not act within those 3 days, then we would provide that information to the appropriate financial institution, issue a cease and desist letter, and ask them to take administrative action to shut down the businesses.



The last thing, Mr. Chairman, that I want to do is show you a highly edited photograph. We hear from people every day that well, child pornography, isn't that just adult pornography? Aren't these 20-year-olds in pigtails dressed to look like they are 15? This is a real image that flowed through our Cyber TipLine. The child was identified. The predator was identified, has been arrested, and prosecuted. The child is getting help. This little girl was 5 years old. As you will notice in the image, she had a dog collar around her neck. And in the second photo, the child was covering her face with her hands because she did not understand what was going on and was so traumatized and terrified by what was happening she would rather have been dead. This is an insidious problem, it is a growing problem, and America needs to wake up to it and do more.

Thank you, Mr. Chairman.

[The prepared statement of Ernie Allen follows:]

PREPARED STATEMENT OF ERNIE ALLEN, PRESIDENT AND CHIEF EXECUTIVE OFFICER,  
NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

Mr. Chairman and distinguished members of the Committee, I welcome this opportunity to appear before you to discuss how the Internet is used to commit crimes against children. Chairman Whitfield, you are a tireless advocate for child protection and I commend you and your colleagues for your leadership and initiative. The National Center for Missing & Exploited Children ("NCMEC") joins you in your concern for the

safety of the most vulnerable members of our society and thanks you for bringing attention to this serious problem facing America's communities.

Let me first provide you with some background information about the National Center for Missing & Exploited Children (NCMEC). NCMEC is a not-for-profit corporation, mandated by Congress and working in partnership with the U.S. Department of Justice as the national resource center and clearinghouse on missing and exploited children. NCMEC is a true public-private partnership, funded in part by Congress and in part by the private sector. Our federal funding supports specific operational functions mandated by Congress, including a national 24-hour toll-free hotline; a distribution system for missing-child photos; a system of case management and technical assistance to law enforcement and families; training programs for federal, state and local law enforcement; and our programs designed to help stop the sexual exploitation of children.

These programs include the CyberTipline, the "9-1-1 for the Internet," which serves as the national clearinghouse for investigative leads and tips regarding crimes against children on the Internet. The Internet has become a primary tool to victimize children today, due to its widespread use and the relative anonymity that it offers child predators. Our CyberTipline is operated in partnership with the Federal Bureau of Investigation ("FBI"), the Department of Homeland Security's Bureau of Immigration and Customs Enforcement ("ICE"), the U.S. Postal Inspection Service, the U.S. Secret Service, the U.S. Department of Justice's Child Exploitation and Obscenity Section and the Internet Crimes Against Children Task Forces, as well as state and local law enforcement. Leads are received in seven categories of crimes:

- possession, manufacture and distribution of child pornography;
- online enticement of children for sexual acts;
- child prostitution;
- child-sex tourism;
- child sexual molestation (not in the family);
- unsolicited obscene material sent to a child; and
- misleading domain names.

This last category was added as a result of enactment of the PROTECT Act in 2003.

These leads are reviewed by NCMEC analysts, who visit the reported sites, examine and evaluate the content, use search tools to try to identify perpetrators, and provide all lead information to the appropriate law enforcement agency. The FBI, ICE and Postal Inspection Service have "real time" access to the leads, and all three agencies assign agents and analysts to work directly out of NCMEC and review the reports. The results: in the 8 years since the CyberTipline began operation, NCMEC has received and processed more than 385,000 leads, resulting in hundreds of arrests and successful prosecutions.

However, despite our progress the victimization of children continues and there is evidence that it is increasing. The number of reports of online enticement of children to the CyberTipline increased 400 percent since 1998. Our records show a significant and steady increase in these reports over the years. This upward trend is very disturbing and shows the seriousness of this issue. But this is not the only evidence.

According to a recent study, one in five youth ages 10 to 17 who used the Internet regularly received a sexual solicitation over the Internet within the previous year. However, less than 10% of sexual solicitations were reported to authorities.<sup>1</sup>

These numbers are powerful testimony to the fact that children are at risk and that we must do more.

---

<sup>1</sup> Finkelhor, David, Mitchell, Kimberly J. and Wolak, Janis, *Online Victimization: A Report on the Nation's Youth*, National Center for Missing & Exploited Children, 2000.

Over the years as technology has evolved so, too, have the methods for victimizing children. The Internet has provided a veil of apparent anonymity, enabling predators to seek out children, win their confidence and then victimize them.

As technology evolves, so does the creativity of the predator. Today, we are hearing a great deal about new innovations, including the use of webcams, social networking websites and Internet access on cell phones.

These innovations are popular and are utilized by millions of Americans. Yet, as with every other new program or service, there are those who would use them inappropriately and for unlawful purposes.

For example, there has been great attention to the social networking websites. While they are marketed to and primarily utilized by young adults, kids are attracted as well, and there have been instances in which offenders have taken advantage of the images and information displayed to target kids.

Some of the social networking sites link defined communities of registered users, such as students attending a particular college or high school. Others are open to anyone over a certain age. These websites permit registered users to create an online profile, including photographs, with categories of interest such as music and sports, as well as an online journal. They are highly personalized and often extremely detailed. Children consider this to be an easy way to connect with friends, find new friends and share their thoughts and feelings.

However, child predators consider these sites to be an easy way to find child victims. They can use the information posted by children to pretend to be someone with shared interests, then develop a 'cyber-relationship' that can lead to that child being victimized. The number of reports involving online journals received by our CyberTipline has increased. In recent years, many kids were using their email profiles and chat rooms in a similar fashion to share their hobbies and interests and make "friends". However, those forums didn't have nearly the same implications as the social networking sites given the enormous universe of users. This recent phenomenon reinforces the importance of education messages where we engage teens to be a part of their own online safety.

Today, NCMEC is working with leaders in many industries who are involved in the burgeoning field of social networking in order to explore improvements, new approaches and better ways to attack the problems. Further, we are also working on plans to bring together key business, law enforcement, child advocacy, governmental and other interests and leaders to explore ways to more effectively address these new issues and challenges.

Webcams offer the exciting ability to see the person you're communicating with over the Internet. While this has many benefits, such as allowing divorced parents to have "online visitation" with their children in distant states, it, too, can be used to exploit children. Many children are victimized inadvertently, by appearing on their webcams without clothes as a joke, or on a dare from friends, unaware that these images may end up in a global commercial child pornography enterprise. Other children are victims of blackmail, threatened with disclosure to friends and family if his or her 'performance' before the webcam doesn't become more sexually explicit. Too much technology and too much privacy, at a sexually curious age, can lead to disastrous consequences.

The teenage years are a time of personal exploration. This is only natural. However, the new form of social interaction is over the Internet, exposing children to, literally, a world of potential danger.

Finally, let me briefly report to you on the exploding problem of child pornography via the Internet. Child pornography has become a global crisis. A recent report by McKinsey Worldwide estimated that today commercial child pornography is a \$20 billion industry worldwide, fueled by the Internet. Its victims are becoming younger. According to NCMEC data, 19% of identified offenders had images of children younger than 3 years old; 39% had images of children younger than 6 years old; and 83% had

images of children younger than 12 years old. There is also strong evidence of increasing involvement by organized crime and extremist groups. Children have become a commodity in this insidious crime.

We are particularly concerned about the linkages between child pornography and the financial system. In a recent case investigators identified 70,000 customers paying \$29.95 per month and using their credit cards to access graphic images of small children being sexually assaulted.

That is just not acceptable. As a result we have convened a Financial Coalition Against Child Pornography. At this point it includes as members 18 major financial and Internet companies, including MasterCard, Visa, American Express, Bank of America, Citibank, Microsoft, America Online, Yahoo and many others. We are bringing new financial institutions into this Coalition every day.

Our goal: To eradicate commercial child pornography by 2008.

How are we going to do that? We are going to follow the money. First, we will aggressively seek to identify illegal child pornography sites with method of payment information attached. Then we will work with the credit card industry to identify the merchant bank and stop the payment. Then we will shut down the sites.

In each case we will work hand-in-hand with federal, state, local or international law enforcement, and the first priority will be criminal prosecution. However, our fundamental premise is that it is impossible to arrest and prosecute everybody. Thus, our goal is twofold:

- (1) To increase the risk; and
- (2) To eliminate the profitability.

We have created working groups of industry leaders explore the best techniques for detection and eradication.

In addition, these companies have asked NCMEC to serve as the global clearinghouse for this effort, sharing information and working together on this effort in a truly collaborative way.

We need to do a better job as a nation of identifying and addressing the greatest risks to our children today.

NCMEC urges lawmakers, law enforcement and the public to take a serious look at the dangers threatening our children today, and to move decisively to minimize the risks posed by those who exploit new technology and target our children.

Now is the time to act.

Thank you.

MR. WHITFIELD. Well, Mr. Allen, thank you, and once again we appreciate your being here and the great work that you are doing in this important area.

I know you had showed us the images of this little 5-year-old girl prior to the hearing today and it is unbelievable that someone would exploit a child in that way. And I believe that you are telling me that the person who was indicted, convicted, and sent to prison in this case actually had a site that was generating in the neighborhood of \$2 million a month in revenue. Is that correct?

MR. ALLEN. Well it was a different site but that is right. I mean one of the things that really awakened us to this problem, we thought the child pornography problem had been virtually eradicated because the Supreme Court of the United States in 1982 said it is not protected speech.

MR. WHITFIELD. Right.

MR. ALLEN. It is child abuse.

MR. WHITFIELD. Right.

MR. ALLEN. But what awakened us was one lead we received that led to an investigation of Federal law enforcement and local law enforcement of a mom and pop website. They decided they were not making enough money doing what they were doing so they set up a child pornography website. When that was shut down by local law enforcement, these people had 70,000 customers paying \$29.95 a month and using their credit cards to purchase access to graphic images of young children being sexually assaulted.

MR. WHITFIELD. Unbelievable. And they were both convicted. Is that correct?

MR. ALLEN. They were both convicted. The husband is doing 60 years in prison and the wife is doing 20. They were making \$2 million a month net.

MR. WHITFIELD. Okay.

MR. ALLEN. And I think, Mr. Chairman, one of the most frightening aspects of this problem is that it has reached beyond pure pedophilia and organized criminals and other entrepreneurs now suddenly recognize that children are a commodity.

MR. WHITFIELD. Right.

MR. ALLEN. And this is a way with relatively low risk and high profitability to make a lot of money.

MR. WHITFIELD. Yeah. Well you are the real experts in your organization in this field and I assuming that you would consider the \$20 billion figure we hear per year on this type of activity is probably a conservative figure.

MR. ALLEN. I do not think there is any question about that and I sincerely believe that we really do not know how big the figure is.

MR. WHITFIELD. Right. Well tell us a little bit about Cyber TipLine. How would children and parents actually find this Cyber TipLine?

MR. ALLEN. Well Mr. Chairman, we are non-profit. We are not Proctor and Gamble. We cannot advertise in the media but what we try to do is use free media and promote it in every way possible. We for example, a number of Internet service providers provide links on their sites, companies like AOL, Microsoft, Yahoo!, AT&T, Cox Communications. And we try to promote it in every way we can. The goal is if people encounter this kind of content, we want them to report it. They can be anonymous but we really need to find out about these sites.

MR. WHITFIELD. All right. You may have heard Chairman Barton today talking about the fact that we are getting ready to mark up a telecommunications bill that is going to change the way the telecom

business does business. Would you have any thoughts or suggestions on using that bill as a vehicle of some small steps that we might take to make it easier to put these websites out of business or to prosecute?

MR. ALLEN. Well, Mr. Chairman, I think there are a couple of things. One is I believe it is imperative that these companies report suspected content like this. As you know, the Congress in 1998 also passed legislation called the Protection of Children from Sexual Predators Act that mandates electronic service providers to report child pornography on their systems to law enforcement through the National Center for Missing and Exploited Children. Now today, 215 ISPs including the major ISPs, are doing that. In addition, we are in discussions with the wireless industry and two of the major wireless companies, Verizon and Sprint Nextel, are currently reporting voluntarily. But there are still thousands of ISPs who are not reporting. This is an issue that is moving into the wireless world. And I think a requirement that these companies when they encounter this kind of content report it, is imperative. Identification is the first step to eradication.

MR. WHITFIELD. All right. Well that is a good suggestion and I know our committee does look forward to continue working with you to explore additional options as we consider legislation on this in the near future.

You had mentioned the Department of Justice. Do you find yourself working closely with the Department of Justice and specifically the Child Exploitation and Obscenity Section?

MR. ALLEN. We do. We work very closely with Federal law enforcement generally and our Cyber TipLine. The FBI's Innocent Images national initiative is connected online to all the leads we receive. CEOS is connected online. The Homeland Security's Immigration and Customs Enforcement plus the FBI, ICE, and the United States Postal Inspection Service all assign agents, inspectors, and analysts to work out of our center in Alexandria. So we are not law enforcement. We are a non-profit mandated by Congress working in partnership with the Department of Justice. What we are trying to do is build the cases for the appropriate law enforcement agencies. We also work very closely with the Justice Department-funded Internet Crimes Against Children Task Forces, 46 of them around the country who are making hundreds of arrests and prosecution. So we are working with every agency that has some role in this issue.

MR. WHITFIELD. Now I know that the Department of Justice provides some funding for you through their--

MR. ALLEN. Yes, sir.

MR. WHITFIELD. --Congressional appropriation process but--and I am not even going to ask you to comment but if you heard all the testimony today, you know that we have some real concerns about the effectiveness and the enthusiasm with which the Child Exploitation and Obscenity Section appeared not to operate in the Justin Berry case and that is something that we are going to look at more closely.

You testified in your opening that the goal was to eradicate child pornography as a commercial enterprise by 2008. Do you think that is a reachable goal?

MR. ALLEN. I have been accused of being naive in the creation of that goal but yes, sir, I do. I think this is a challenge of mobilizing these financial companies with law enforcement. I firmly believe that the vast majority of this commercial enterprise is accounted for by relatively few organizations and people. And I believe that it is like taking, tracking down terrorist financing, and anything else. I think you follow the money. You use the kinds of tools and resources you have and you shut it off. I think that that is not going to eradicate child pornography, but I think if we can get it back to where it was and, in fact, I and the FBI and others testified before Congress a decade ago that if there were no pedophiles there would be no child pornography. I am skeptical that all 70,000 of those people accessing that one website in Texas were pedophiles. So something else is going on here.

MR. WHITFIELD. Yeah.

MR. ALLEN. There was research in 2002 by ETPAD International and the Bangkok Post that estimated that there were 100,000 child pornography websites. That was 2002. But frankly, I think this is an issue where law enforcement has come relatively recently to this process. Once again, law enforcement has not been at the forefront of getting and being able to utilize the new technology.

MR. WHITFIELD. Right.

MR. ALLEN. And instant images is only 10 years old. And so I think that is realistic. I think we can do that.

MR. WHITFIELD. And did you also tell me that there is now developing a tourism business in which pedophiles go on trips to foreign countries and young children are brought to their rooms. Is that correct?

MR. ALLEN. Yes, sir. It is a global enterprise. And this Congress had the wisdom in the Protect Act in 2003 for the first time to provide legislation that enables the prosecution of U.S. citizens who go abroad for that purpose and there have been many charges brought just in the couple of years since then.

MR. WHITFIELD. Well, Mr. Allen, my time has expired. I recognize the gentleman from Michigan, Mr. Stupak.



MR. STUPAK. Mr. Allen, I appreciate your enthusiasm in trying to get it wrapped up by '08 but how is that possible when you get your ISPs you say there are 250 and reporting more, but there are thousands more out there plus wireless providers. How are you going to get the rest of them if you got 250 right now?

MR. ALLEN. Well I think two responses to that, Mr. Stupak. One is we need not just to wait for people to report it, we need to aggressively go out and find it and we are trying to do that. And secondly--

MR. STUPAK. Who is we?

MR. ALLEN. Well Federal law enforcement and the National Center. We have been using spidering technology to go out and proactively search out illegal sites and we are going to continue to do that. Secondly, I believe that the key to this is the financial industry. And the good news is to this point we have been able to encourage and persuade 18 major companies to join in a financial coalition against child pornography including MasterCard, Visa, American Express, Discover.

MR. STUPAK. How many of these 18, did you ever check them against Justin Berry's list to see how many of the 18 were on his list of 1,500 names and transactions?

MR. ALLEN. Well now these and I am talking about, I mean, when you spiral the web and look for active child pornography websites, the major sites that you find or the major methods of payment that you find today are the third party payment sites like Egold which is a part of this coalition and the credit card companies. Now a lot of those are bogus. But MasterCard, Visa, American Express have all said to us we do not want to make any money on this.

MR. STUPAK. But what are they doing?

MR. ALLEN. Well they told us the same thing.

MR. STUPAK. Yeah.

MR. ALLEN. They have agreed to participate in this process in which--

MR. STUPAK. What does that mean, participate in this process? What can they really do?

MR. ALLEN. Well what they are going to do is take the information that we generate, they are going to share it within this network of companies. They are going to, once we have identified with them the merchant bank and law enforcement has said we are not going to investigate or prosecute on this one, they are going to take steps under their agreements. I mean credit card companies are just associations of banks to hold the banks responsible because when a bank operates an illegal account and submits payment, it is not only a violation of the law, it is a violation of their--

MR. STUPAK. Has any of that been done yet?

MR. ALLEN. Just begun. We just started this 2 weeks ago. Hold us accountable, we are going to do that.

MR. STUPAK. Well what about this meova.net, the third party that we heard so much about in the last panel?

MR. ALLEN. We have no contact with them.

MR. STUPAK. Okay.

MR. ALLEN. But we welcome everybody's involvement and welcome the committee's help in bringing other financial institutions into this process.

MR. STUPAK. But isn't that the name that in Justin Berry's case, why these were paid was this meova group and not the big credit card companies? So how do you get them to participate?

MR. ALLEN. Well we do it one at a time. We basically leverage the relationships we are building with the credit card companies and the banks and we--I mean I am not suggesting Mr. Stupak that there is a quick, easy solution to this.

MR. STUPAK. No, there is not and that is what I am trying to drive at.

MR. ALLEN. Yeah.

MR. STUPAK. How do we get it done? Even if we put something in legislation tomorrow, I am not too sure it is going to either. I think we have to have a more comprehensive approach.

Two years ago, you testified before this committee about the use of peer-to-peer clipboards by child pornographers and pedophiles as a way to share files without being identified. This is often the system that child pornographers and the customers use to share files and individuals from all the world can use these networks. Could you describe how this works and whether there have been any advances? Have you been in control of these networks, these file sharing networks?

MR. ALLEN. Well the way it works is that this it basically does not require an ISP, this basically linked the files shared through networks like Kazaa and other mechanism. What is happening is there has been aggressive effort by Federal law enforcement and the Internet Crimes Against Children Task Forces to make cases. The case that the Attorney General and ICE announced a couple of weeks ago was in essence a peer-to-peer network, child pornography on demand. You know, it remains a challenge because it is harder to identify. It is harder to capture that image at the moment that it is distributed than it is if it is distributed through an ISP.

MR. STUPAK. Well part of my concern is the music company shut down Napster for illegal file sharing of copyrighted material. Why can't law enforcement be more aggressive in shutting down these sites?

MR. ALLEN. Well frankly, I think the largest challenge is again, I think law enforcement is overwhelmed by the magnitude of the problem. We would welcome, I mean, I do not speak for the FBI or Homeland Security or anybody else, but I think this is a problem that is going to require more resources, more personnel. Innocent Images needs to get bigger. The Cyber Crime Center at ICE needs to get bigger.

MR. STUPAK. Throughout your testimony today and even the earlier the testimony, everyone talked about the Federal law enforcement, Justice, things like this, Department of Justice. Can you or do you work with State and local law enforcement?

MR. ALLEN. Yes, sir, we do actively. And I think a very important point that needs to be made is that Federal law enforcement cannot possibly do all of this. What we have emphasized very strongly is building State and local capacity because in every one of these cases, just like Justin in Bakersfield, there was a local victim. The only thing that is different about this is the medium that is being used to transmit the image.

MR. STUPAK. Have you had any access to the information that Mr. Berry provided Justice? Have they worked with you at all, Justice like I-

-

MR. ALLEN. I do not think we have seen that information.

MR. STUPAK. You also testified that a 1999 law that requires Internet service providers to report child pornography on their sites or face substantial fines and that was back in 1999 that law was passed. Five years later in 2004, the reporting mechanism had not yet been formalized. Has any been formalized? I mean, why should it take 5 years? If we knew it was a problem in '99 and we passed a law, it is 5 years. Has it been formalized or has it not? What has happened? Has anybody been fined or anything ever happened with that?

MR. ALLEN. No, sir it has not been formalized. What we have been advised by the Justice Department is that there was a flaw in the statute that in essence it is a civil statute with a criminal penalty and so we have met with many. The good news is that the majority ISPs are complying. We have developed our own system with them. We work with the U.S. ISP Association but anything this committee can do to make every electronic service provider in America have to report, I think it is a good thing. One of the real challenges quickly, Mr. Stupak is that a lot of these companies are saying to us that absent some safe harbor provision, their concern is that when they transmit these images to us they in fact may be violating the law. So I know the Justice Department is taking another look at that. We welcome whatever resolution can happen.

MR. STUPAK. Well I know Mr. Chairman, and I think members of this committee should be--we passed the law in '99 and this is the first

we have heard that there is a problem with it. I would think after 7 years someone would step forward and say hey, we cannot do what you intended, to go after this Internet pornography especially with children, because there is a flaw in the law. So thank you for that, we will note it for those questions on Thursday.

Since controlling peer-to-peer networks seems so difficult, do you think the new financial coalition, the one you have listed here against this child pornography to follow the many, will eradicate child pornography? What percentage of the child pornography is shared without payment? I think we have had a lot of that where you had to produce a payment, plus you had produced pictures, nude pictures, or fill in the blanks or I call them trading cards if you will pornography. Is that here today?

MR. ALLEN. In our judgment, we think that the largest share of child pornography is distributed and shared without payment. Even though the commercial side of this problem is a billion dollar problem, we think the non-commercial side is larger.

MR. STUPAK. I think you mentioned it earlier, but if you could take a moment and expand upon it. I think you said law enforcement lacks the resources. What area do they lack the resources? I thought you indicated they could come to your shop and do some work there but what are the resources that are lacking? Is it just training in what is going on? Is it the empire or what is it?

MR. ALLEN. Well there has been an aggressive effort to train. We have been training unit commanders and investigators in computer facilitated crimes against children for some time. Ten years ago, I was aware of one specialized unit in a local police department; the San Jose Police Department had a kind of an early cyber crimes unit. The good news today is that most major police departments now have specialized units. The good news today is that there are 46 Internet Crimes Against Children Task Forces funded by Congress around the country that are State and local with Federal involvement. But I just think the sheer scale of this problem requires greater investment, more people, more technology, more advanced technology, because it continues to evolve.

MR. STUPAK. Let me ask you one more clarification. I had asked you earlier if your center has been provided any of the names or the information on the Justin Berry case. It is my understanding that the FBI has an agreement to provide all the images to your center.

MR. ALLEN. That is right.

MR. STUPAK. So if your center--have you received those images, and if not and that means CEOS has not given you the images, then the FBI--you have not seen them yet, have you?

MR. ALLEN. Candidly not to my knowledge, no.

MR. STUPAK. So you cannot give me comparisons then either without the images.

MR. ALLEN. That is true. Now I will confirm that. I do not know that absolutely, but to the best of my recollection, I do not believe we have received those images.

MR. STUPAK. Any reason why not? Not names but just images so you could do you work?

MR. ALLEN. Not to my knowledge.

MR. STUPAK. Okay. Thank you.

Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you, Mr. Stupak.

Mr. Allen, let me just ask one concluding question here. Around the world, do most countries have laws against child pornography and child molestation?

MR. ALLEN. The answer unfortunately, Mr. Chairman is no. Through our international center, we just did an analysis, we have done a report that we are releasing on Thursday of the 184 member nations of Interpol. Ninety-five of those countries have no law on child pornography at all. About 135 or 140 including some of those that do have some law do not criminalize the possession of child pornography. The good news is we reviewed this law based on five categories of statute. The good news is five countries including the United States have enacted laws in each one of those five areas.

MR. WHITFIELD. Okay.

MR. ALLEN. And another 22 have enacted laws in all areas except ISP reporting.

MR. WHITFIELD. Okay.

MR. ALLEN. But there is a lot of work that needs to be done around the world as well.

MR. WHITFIELD. Mr. Allen, I thank you very much.

Ms. Blackburn, did you have any questions for Mr. Allen?

MRS. BLACKBURN. Mr. Chairman, thank you.

I do have a couple. I do not know if--and I apologize I have got constituents that were in and I had to jump out--and I think you have maybe answered these but let me just go back. In your very opening statement, you said something about looking at how much of the industry is in the U.S. and how much is offshore and that was one of the questions that I had posed earlier to Mr. Eichenwald.

MR. ALLEN. Right.

MRS. BLACKBURN. And the follow-up I have for you on that would be, are you all doing the research so that we can begin to quantify this and kind of get our arms around it?

MR. ALLEN. We are trying, but it is very difficult to do because there is no real database to measure. It is all sort of estimated. The other thing that is clearly happening is, for example, there was a case in January of 2005 in which the business, the server, was Delarosa. The financial support for the child pornography system was in the Caribbean, was offshore. But the vast majority of the customers were Americans and the vast majority of the victims, the child victims were Americans.

MRS. BLACKBURN. You know, Mr. Allen, to me listening to all of this testimony today, it seems that the business of the child pornography which is just so sickening when you hear about this that it is labeled in some ways to identity theft, the pirating, the different types of theft or subversive type activity that we see over the Internet and there seems to be some common things that are developing and running through these businesses.

MR. ALLEN. Well Congresswoman, we have heard from a number of experts that there are five basic factors in play for the reason why this has become not just an insidious crime but big business. One is that children are plentiful and easily accessed. Secondly that the production of the material has become very inexpensive. You do not need massive studios anymore. Thirdly, that there is enormous consumer market for the content. Fourth, therefore it is incredibly lucrative, incredibly profitable. And five, at least comparatively there is virtually no risk, particularly compared to drugs and guns and tobacco and other kinds of commodities. So what our focus has been strategically working with law enforcement agencies around the world is we have got to dramatically increase the risk and we have got to dramatically reduce the profitability.

MRS. BLACKBURN. Because at this time it is the lowest risk, highest profit area of the what we would call subversive or--

MR. ALLEN. Right. And that is why I wanted to add one other thought to the Chairman's question earlier about is the goal of eradicating commercial child pornography by 2008 realistic. Well our basic premise is if you can eliminate the use of the credit card, we can take the credit card out of this process. If you can eliminate the use of the third party payment mechanism and we are working with the Egold's and PayPal's and those kind of companies, it is going to become more and more difficult to sustain the enterprise. The payment mechanism is going to have become a lot more sophisticated and farther reaching. Kurt talked this morning about the six steps removed. We just have to make it ten steps and then 14 steps. If you have to pay cash, access to a child pornography website, the profitability compared to the investment drops dramatically. And I think at that point, these are entrepreneurs. These are organized criminals. They are going to look for some other way to make money.

MRS. BLACKBURN. Well I thank you. I thank you very much for your patience with us today. I thank you for the work that you all are doing and I thank you for being accessible to us and allowing us to have some time to visit with you on the issue.

MR. ALLEN. Thank you very much.

MRS. BLACKBURN. I yield back.

MR. WHITFIELD. Thank you, Mrs. Blackburn.

And Mr. Allen, thank you so much for being with us today. We look forward to continuing working with you on this issue and thank you for the great job that you do at the center.

MR. ALLEN. Thank you, sir.

MR. WHITFIELD. I would call the fifth panel of witnesses, please. We have Ms. Parry Aftab who is the Executive Director of WiredSafety from Irvington-on-Hudson, New York. We have Shannon Sullivan who is a Teen Angel with WiredSafety from Irvington-on-Hudson, New York. We have Ms. Teri Schroeder who is President and Program Director of i-SAFE America from Carlsbad, California. And then we have Moni Sallam who is a mentor at i-SAFE America from Carlsbad, California. I want to welcome all of you today. We genuinely appreciate your patience. We similarly look forward to your testimony because we know that you are doing some great work to assist our young people and others as we try to eradicate this problem. And as you know, this is an oversight investigation hearing and we normally do take testimony, in fact, we always take testimony under oath. Do any of you have any difficulty in testifying under oath today? And do any of you have legal counsel with you today?

[Witnesses sworn]

MR. WHITFIELD. Thank you. You are now sworn in and Ms. Aftab, we will ask you to give your opening statement first so you are recognized for five minutes.

**TESTIMONY OF PARRY AFTAB, EXECUTIVE DIRECTOR,  
WIRESAFETY; TERI L. SCHROEDER,  
PRESIDENT/PROGRAM DIRECTOR, I-SAFE AMERICA;  
SHANNON SULLIVAN, TEEN ANGEL, WIRESAFETY;  
AND MONI SALLAM, I-MENTOR, I-SAFE AMERICA**

MS. AFTAB. Thank you very much, Mr. Chairman.

My name is Parry Aftab. I am an Internet privacy and security lawyer or at least I used to be. A number of years ago, I used to represent corporations in cyberspace protecting them until one day someone sent me an email telling me shut down the website, to put the people in jail.

I know a great deal about child pornography and I testified before this House.

MR. WHITFIELD. Maybe you could just turn off the sound on your computer, Teri, it might make it easier. Thank you.

MS. AFTAB. I have testified before the House of Commons and the House of Lords, Parliament. I advised the Singapore Government. I do this all over the world so I knew a lot about child pornography. But when I went to this site, up came 150 names of images, just names. I clicked on one of them and up came a picture of a little three and half year old being raped. She had her eyes closed in the way that those of who are parents remember our children. Mommy, you cannot see me, can you? And we all pretend that our children are invisible. No, where did you go? Oh, my goodness, you did, where you, you are gone, you are invisible. And then giggle and we tickle our children and we laugh about it. This little girl was being graphically raped and had her eyes closed hoping that she too would be invisible. She was violated not only by the sexual molestation but by the fact that they expected her to pose for the cameras.

I cried for an hour, I vomited for two, and I realized that the reputation I had earned over the years as one of the first Internet lawyers in the world could be used to do perhaps greater good. The companies I represented I thought would follow me and the law enforcement that I had advised would as well. And we created the world's largest Internet safety and help group. It is called WiredSafety. We have 11,000 volunteers in 76 countries around the world. Not one of us is paid a dime. We have no offices, we operate from our homes and offices and cell phones. If you dial the telephone number on our websites, my cell phone will ring. I sold my house, a very expensive one in New Jersey, and emptied my bank accounts and this is what we do.

It started out in the early days where we were dealing with a child's sexual exploitation. We also do a tremendous amount of work in identity theft. We protect everybody of all ages in cyberspace and on wireless devices and interactive cell phones and gaming devices, on anything that can go wrong, from cyber terrorism to ID theft to fraud but my heart is with the children.

For years, I looked for this little girl. I never found her but instead we found many others. We have and this has never been a public statement of ours before, we have been working very closely with the National Crime Service in the UK for the last 7 years. Together, we infiltrated some of the leading sex trafficking groups in the world and hundreds of people have gone to jail because of our work. The person who did that with the National Crime Service is another one of my



unpaid volunteers. I have been doing this for a long time. It is what I am supposed to be doing.

A number of years ago, I met a young woman. Her name was Kitty Tarbucks. Kitty was 13 from Connecticut when she met someone online she thought was Mark. She thought he was 23. She was a little bit heavy. She was a member of the swim team. She was not as popular because she was brighter than a lot of the other kids in the room. She met him online. She thought what the heck, he was in California, she was in Connecticut, she is never going to meet him in real life. So she chatted with him and she talked on the phone with him and she shared pictures with him and became friends. She talked about politics. And he thought she was wonderful and pretty and bright and smart. Six months into the relationship, she shared that she was going to a swim meet in Dallas, Texas. He said, you know what, I will come out and I will meet you. I will fly out from California to your swim meet and he did. She made arrangement with her roommate that she was going to walk down the hall to meet him in real life. She really wanted to and she will admit that to this day. She found what room he was in and he was waiting for her. She walked down the hall, pushed the button the elevator and went upstairs. She knocked on the door and it was answered. Her first thought was oh, my gosh, he was an adult. And he has got the ugliest white shoes I have ever seen in my life. He opened the door, she walked in and sat down on the sofa. He shut the door behind her. He sat down and he said, you know, Kitty, it took so long to get the luggage in the airport and she said yes. And the food at this hotel is not very good is it? And she said no. I love your watch, he said, and starting touching it. And your hair is so beautiful and ran his fingers through it. I have been thinking about doing this for a long time he said. He reached out, kissed her, started to grope her, and began to molest her. Luckily, her roommate had told her mom who was a chaperone on the trip and her mom and the police and security were at the door pounding until he opened. They whisked him away and Kitty sat there in tears while she tried to reassemble her clothing. The police came to her a few minutes later and they said you talked to this man for 6 months? We talked to him for 5 minutes, he is a 41-year-old investment banker and his name is Frank Cusovich, not Mark. What are you thinking?

Years later she put him in jail for about two and a half years under the Communications Decency Act, a section that was actually maintained as constitutional, and she wrote a book that was later renamed *A Girl's Life Online* about her story.

But we do this all over the world. And I was working with a young family in the UK and little Georgiana was 13 and she had met Johnny who was 16 from about 200 miles away. And they were talking on the

phone. Her parents knew and he said he wanted to meet her and she said great, my mom will bring me and he said no, you bring your mom, I am not coming. So she said to her mom, I do not know what to do, I have to lie to one of you, I am going to lie to him. She said to her mom but when you drop me off, pull the car up about a half a block. You will be able to see me but I do not want him to know you are there and if everything is okay, disappear, come back later, we are going to the movies. She stood there alone in front of the movie theater when a 46-year-old approached. She wondered why Johnny had sent his dad. He said, Georgie, I am Johnny. Her first thought was oh my gosh, he is an adult and he has got the ugliest brown shoes I have ever seen in my life.

Now I am a lawyer so I hear this, I talk to a lot of kid victims. I immediately think about that I am from New Jersey. We have this very ugly shoe store that sells only very ugly shoes in New Jersey. And I said what you need to do is stake out places like this because obviously the Internet sexual predators wear ugly shoes. And the child psychologists who donate their time with us and the forensic psychologist turned and they said, describe my shoes, Parry. Okay, no, no, look at me and describe my shoes. Well how can I describe your shoes if I am looking you in the eye and they said exactly.

When our children fall in love with a person they meet online who they think is now a perfect soul mate for them and they meet them in real life and find out who they are, they all become experts in men's shoes. They walk through it. They got through with the molestation. They do things they ordinarily would not have done because they are embarrassed. They just think they led him on because of something else.

Well if you went to Myspace about a month ago and you clicked on safety tips, you would have learned all about us. For the last year and a half we have been working on the inside with Myspace and with Facebook, and with Febo, and all of the others. We have done a great deal of work in cyber stalking, cyber bullying, and sexual predators and we deal with these issues and provide this information to these sites.

One of the problems we are finding on social networking is that there are some benefits like we never thought there were. It would have been much easier if I could find social networking and say, you now, that it is terrible, let us shut them down. But we are finding kids who are raising money for charities and expressing themselves and writing music so a kid from Connecticut or California can write the words to it. So we now have to do the hard thing. We have to find a way of making them safer, so we worked with Myspace in the west in developing safety tips and links to my volunteers to help with these issues.

Not too long ago, I was in L.A. having lunch with a girlfriend and who walked in but Nick Lachey. If you do not have any young kids at

home, he is the one who is getting divorced from Jessica Simpson. He is on the cover of Teen People and everything else. So my girlfriend was there and she said look that is Nick Lachey and I said I will be right back. And she said, we are from California, we do not approach celebrities. I said I am from New York, we do not admit they are celebrities. And I walked up to his table, I handed him my card, and I said Internet sexual predators Nick, are using your name to lure kids. If they find out, the kids have posted something that they are fan of Nick's, the predator becomes a close personal friend of his. I am a close personal friend of Nick Lachey's and if you send me a picture, I will get it to him. He really likes that picture. Do you have a sexier one, something in a bikini? Anything else? He turned white as a ghost. He said would any money--I should have said yes, but we run a charity that is all volunteers. I should have said, yes, but I said no, just give me a public service announcement. Two weeks later he had Googled me. He got Tom Patters who owns Polaroid and everything else to write a \$2 million check to create a safer social networking site for teens called YFly. When kids are bothered by people posing as a teen they can click report the creep.

I then reached out trying to find spokespeople. I used to represent a lot of them in the olden days and so many of them now are getting arrested on drunk driving and everything else, I was standing on a stage in Singapore and who popped through a screen behind me but Spiderman. And as part of our exhibits today, you will see the first of a series of Internet safety comics written by Marvel for us using all 4,000 of their characters that they donated to us on a worldwide license.

We do a lot of this work and it is going to take all of us. There is far too much backbiting and knifing of MGAs in the back. Unfortunately, there are enough children being hurt, there is enough work to go around and each of us has our own specialties. What I suggest we do is look at some of the models that we have used around the world. UNESCO named me to head up their efforts on these things for the United States. And we do not have in this country a national task force that is put together with the leading experts in the world on Internet safety. Instead, I am on a home office task force in the UK and I advise the EU. We need one here and that is easy and that is cheap. You get good at doing that when you run a non-profit that is unfunded.

In addition, there are lots of questions about the statistics. Ernie, who I respect incredibly well, cannot give you the statistics on how many kids have been victimized in what way because they do not exist. Because on a crime reporting form there is no check, or no box you can check, saying that the Internet was involved in some crime. That is an easy fix to help us start tracking growth. We need to know that if we are

going to address it to see if we are making a difference. We need to get a lot of players together and work together. And one of the things I learned a number of years ago is if we are going to reach the kids, we have to do it in their own language in their own ways. So I founded a group that is called Teenangels and it is part of our group. And they train for a very long time. It usually takes about a year to train a Teen Angel. They are trained by law enforcement, AOL, and Disney, and Oracle, and everybody else I know and the FTC and they learn what everybody needs to know about privacy policies, predators, piracy, illegal inappropriate use, and responsible technologies. And when they are done, they go out and create their own programs and they are now advising all of those companies. They have got a new cell phone that Disney launches tomorrow that is a little safer because parents can control who can text message or call their kids. And that came out of some of the thinking of the Teenangels. And Disney and AOL and the CTIA when you look at the Telecommunications Act that you are reviewing, the CTIA has turned to my Teenangels and to us for advise on how they can use our skills and things we know to make things safer.

So I would like to thank you so much for giving us the time today. And I would like to introduce one of my very special Teenangels who in addition to Nick Lachey and with Teen People that is out on the stands right now was selected by Teen People as one of the top 20 mover and shaker teens in the country. Shannon is 14 and here to talk about her experiences as a Teen Angel.

[The prepared statement of Parry Aftab follows:]

PREPARED STATEMENT OF PARRY AFTAB, EXECUTIVE DIRECTOR, WIRESAFETY

#### **SUMMARY**

Our children are online. They do their homework, entertain themselves, communicate with each other and us, research things, buy and compare prices online. They need the Internet for their education, their careers and for their future. Of all the risks our children face online, only one is certain. If we deny our children access to these technologies, we have guarantees that they are hurt. All other risks are avoidable through a combination of awareness, supervision and parental control and other technologies. More and more children being lured and stalked by online predators who gather information about them from chatrooms, instant messaging, e-mails, websites and the like and use this information to become close to them.

With our children walking around with Internet access in their backpacks and pocketbooks, we can no longer rely on parents watching whatever they do from a central location computer. Our children need to learn to use the "filter between their ears" and "ThinkB4TheyClick." This requires that we get them involved in framing solutions and educating each other. It also requires that we find new ways of building good cyber-citizenship and helping the kids and parents spot risks in new technologies and protect themselves online.

But we also need to recognize that in most cases our children are putting themselves in harm's way. They are intentionally sharing risky information online in profiles, blogs

and on websites. They post their cell numbers on their public away messages when using IM technologies. And even when they are careful about protecting their own privacy, their close friends may expose personal information about them by posting photos and information on their profiles. They are also, in greater and greater numbers meeting people offline that they met online. Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47-year old child molester instead. This has to stop.

Smart kids are sharing sexual images online with people they don't know, or e-mailing them to others they have a crush on and hope to entice. And with the newer video-chats and technologies, the predators have moved to luring our kids into posing and engaging in sexually explicit activities.

Yet, the actual statistics are lacking. Everything we know is largely anecdotal. In 1999, the FBI's Innocent Images (charged with investigating crimes against children online) opened 1500 new cases of suspects who were attempting to lure a child into an offline meeting for the purposes of sex. Based upon my estimates, about the same number of cases were opened by state and local law enforcement agencies that year. The same year, approximately 25 million minors used the Internet in the U.S., Now, with more than 75 million young Internet users in the U.S. we don't know if the number of instances have increased, decreased or remain flat, given the growth. The crime reporting forms don't collect information about the use of the Internet in child sexual exploitation crimes, or any other crimes. That has to change.

We also need to recognize the real risks and what is hype. Notwithstanding media reports to the contrary, to my knowledge, law enforcement is not aware of anyone who is using the information children provide online to seek them out offline, by hiding behind a bush or grabbing them on their way home from school. They currently agree to meetings (even if they don't admit it to the police when things go wrong.) But it's only a matter of time before this happens, since universal access to the Internet means that even violent sexual offenders who are online can use it for their own horrible purposes.

#### **OPENING STATEMENT**

Thank you for inviting me to testify here today about ways we can keep our young people safer online. This is a very important topic and one to which I have devoted my life over the last ten years. My name is Parry Aftab. I am an Internet privacy and security lawyer and run the world's largest Internet safety and help group, WiredSafety.org. We are an all-volunteer group and a charity formed in the United States. We have approximately 11,000 volunteer from 76 countries around the world, all devoted to helping create a safer interactive technology experience for users of all ages.

#### ***SNAPSHOT OF U.S. MINORS ONLINE AND HOW PREDATORS REACH THEM***

It is estimated that approximately 75 million minors in the United States access the Internet either from home, schools, community centers and libraries or from some newer Internet-capable device. This is up more than ten-fold since 1996, when only 6 million U.S. minors were online. Now our children are using cell phones with Internet and text-capability, interactive gaming devices (such as X-Box Live and Sony Playstation Network) with voice over Internet and live chat features, handheld devices with Bluetooth and other remote-communication technology (such as PSP gaming devices and mobile phones) and social networking profiles (such as MySpace, Facebook, Bebo, YFly and others) where they can advertise their favorite things, where they live and pictures of themselves and their friends to anyone who wants to see them.

Ten years ago, when I first wrote my safety tips telling parents to put the computer in a central location, that made sense. It was a central point, where parents could get

involved and supervise their children's interactive communications and surfing activities. Now, where they take their communication technologies with them in their pockets, backpacks, and purses, it is not longer as relevant as it once was. Now, instead of expecting parents to watch everything their children are doing online from the comfort of their familyrooms, or kitchen counter, we have to do more. Now, we have to teach our children to use the "filter between their ears" and exercise good judgment and care when using any interactive device. While teaching parents how to supervise their children online was a challenge (I have written the leading books, worldwide, for parents on Internet safety), teaching children to "ThinkB4uClick" is much harder.

When I was growing up (in the days before electricity and indoor plumbing, when we had to walk up hill, both ways!, in blizzards to get to school ), parents used to blame us for not behaving. We were disciplinary problems. Now pediatric neuro-psychologists tell us that preteens and young teens are hardwired, through immature brain development, to be unable to control their impulses at this age. Either way, we recognize that preteens and teens take risks, don't appreciate the consequences of their actions and act before they think. When their audience was their school friends, family and neighbors, the risks were containable. When they act out where 700 million Internet users can see, it takes on a much deeper significance.

#### ***Putting Their Heads into the Lion's Mouth***

Now, I will share something very controversial. While educators and child psychologists understand this, most parents will be shocked at the suggestion that their preteens and teens are in control of their safety online and putting themselves at risk, often intentionally. But unless we accept this, and direct our attentions at solutions aimed at this reality, we are all wasting our time. We will focus on the much smaller segments of preteens and teens who are being victimized through not fault of their own - those who are targeted at random. All others need to change their online behaviors. And that's where we need to devote all our attentions.

For this to happen, you need to understand the truth. For years we have told parents and minors not to share too much personal information online. "You can be tracked down in real life," we told them. But, notwithstanding anything to the contrary reported in the media and by some local law enforcement officers, to my knowledge, to this date, no preteen or teen has been sexually-exploited by someone who tracked them down from information they posted online. In each and every case, to my knowledge, to teens and preteens have gone willingly to meet their molester. They may have thought they were meeting someone other than the 46 year old who is posing as a teen, but they knew they didn't know this person in real life. They are willingly agreeing to meet strangers offline.

What does this mean? It means we can do something about this. It means we can educate teens and preteens about the realities of meeting people in real life they only know in cyberspace. It means we can create solutions. It means that this is, at least for the time being, 100% preventable. It means that what we do today will have an immediate impact on the safety of our youth. It means we have to join together and work on things that are effective and abandon those that are not.

But we have to act quickly. When I testified before the U.S. House Of Representatives, Committee On Commerce, Subcommittee On Telecommunications, Trade, And Consumer Protection on October 11, 2000, I cautioned:

Law enforcement is not aware of anyone who is using the information children provide online to seek them out offline, by hiding behind a bush or grabbing them on their way home from school. But it's only a matter of time before this happens, since universal access to the Internet means that even violent sexual offenders who are online can use it for their own horrible purposes. (See Testimony of Parry Aftab, Esq. U.S. House Of Representatives, Committee On Commerce, Subcommittee On Telecommunications, Trade, And Consumer Protection on October 11, 2000.)

Luckily, while our young people are sharing much more information online than ever before, to my knowledge, predators aren't using it to hunt down our children offline. They are like vampires. They need to be invited in. Sadly, our teens and preteens are too often doing just that. They are inviting them to offline meetings, phone calls and videochats. But, as an expert in cyberrisk management, I can tell you that this is good news. Because we have a single point of risk - our children, preteens and teens. If we stop their risky and unsafe behaviors, and teach them when to reach out for help, we can manage this risk. We can keep our children safe.

Our children are mainly at risk because of their own actions. Some are intentional. Others are inadvertent. They may willingly engage in communications with people they don't know in real life "RL," agree to meet them offline or send them sexually-provocative images or perform sex acts on webcams they share with people they encounter online. They cyberbully each other by advertising their victims for sexual services, posting real or manufactured sexually explicit images of them online or by passing online rumors about their sexual preferences or activities.

**Preteens and Teens at Risk:** Most of the high risk preteens and teens fall into three categories: those who are naive and looking for love and affection (typically the "loners" and "shy" preteens and teens), those who already engage in other high risk activities, such as drug and alcohol abuse, driving too fast or doing risky things for the thrill of it (often the student leaders, athletes, cheerleaders and very competitive teens, the risk takers and thrill seekers looking to let off steam or impress their peers) and those who don't realize that what they do online is real, the ones who are looking to appear older, cooler, more fun and more popular (most of the teens and especially preteens fall into this category at least once). Sadly, most of our preteens and teens fit one of these categories. Sadder still is the fact that in recent years we have learned that most preteens and teens are potential victims.

**Naive, loners and socially-shy preteens and teens:** Some believe that they are communicating with a cute 14 year old boy, who they later discover isn't cute, isn't fourteen and isn't a boy. Most of the reported cases fall into this category, and until the death of Christina Long four years ago this May, experts all believed that *all* victims fell into this category. They are conned, and easy to spot online. Predators can seek them out, and find their vulnerabilities. They are groomed with care, and often fall in love with their molesters. Sadly, when the molestation finally occurs, not only are their bodies broken, their hearts and trust are too.

They need to understand how the predators work online. Too often they tell me that they can "tell" how old someone is online. They can't. No one can. Many predators spend years cultivating the right tone and language to look like a fellow teen online.

These preteens and teens are sitting ducks. While they may have learned not to fall for the "help me find my puppy" ploy offline, they need to learn how that same ploy (appeal for assistance) works online. They need to know how to spot the risks and the predators, when online everyone can look like a cute 14 year old boy. They need to learn that romance shouldn't occur only in cyberspace, and that parents can get involved to help them meet their soul-mate, assuming they really are. So, if they aren't, and turn out to be a 46 year old child molester, they can come home safely and help put that molester behind bars where they deserve.

**Risk-takers, Thrill-seeking preteens and teens:** Some preteens and teens (mainly teens) are looking for the thrills and challenge of engaging in a relationship (or at least prolonged communication) with an adult. They "play games" with the adult, and are intentionally extra sexually-provocative. They think they are smart enough to do this without getting hurt. They see this as a game, without realizing the consequences of their actions. And crossing the sexual line isn't as frightening online as it would be in real life. The problem is that the consequences are not as apparent, the realities not as immediate.

They take risks. And they think they can handle them. (They don't often understand the consequences, though.) They often willingly engage in sexual communications with men they know are adults. That's part of the thrill. They are also often willing to engage in sexual activities with the adult, but don't realize what that can mean when things go very wrong. We rarely hear about these kinds of victims, because they never report it when things go wrong. They feel as though they "asked for it," or are to blame. When we hear of these cases, it's because they are killed or kidnapped. (Christina Long was in this category. She was the first confirmed murder victim of an Internet sexual predator in the U.S. and died four years ago this May.)

Friends are the answer here. If we can get friends too help watch out for each other, it is less likely that they will meet adults in real life, or if they do, got alone. Also, finding cool spokespeople, like Nick Lachey, to explain that it isn't cool to be stupid and campaigns such as our "Don't Be Stupid" help. So do real life stories from victims themselves about how they got caught and advice from the trenches. Kateisplace.org has sections specifically directed at this type of victim. And Teen People is an important partner of ours in spreading the word.

**Not really a drunken slut, just playing one online:** We've all been reading about this new trend in the news (often with me as the expert). Good, respectful, otherwise well-mannered preteens and teens acting out in cyberspace. In profiles, blogs, on social networking sites and their away messages on IM, on their websites and interactive gaming bios, they act out. They pose in their bras, or worse. They simulate sexual activities (and in some cases post images of actual sexual activities). They pretend to be someone or something other than what they really are. And this alter-ego may be a sexually promiscuous teen "up for anything."

They don't think it is cool to tell others they were home coloring with their five year old niece last weekend. Instead they claim to have snuck out after everyone was asleep to get drunk at a wild party. To them it isn't real. They lie. They pose. They do thing online they would never dream of doing in RL. They aren't really drunken sluts - they are just playing one online. (Shannon, one of our award-winning Teenangels, will share insight into why teens and preteens are doing this, during her testimony today.)

### ***The Anatomy of a Cyberpredator:***

There have been many cases recently where pedophiles and other adults have lured children into offline meetings and molested them. Luckily, there are even more cases when such attempts to lure a child have brought about the attention of law-enforcement groups. I debated whether I should discuss any of these cases, because I did not want to sensationalize them. But if explaining the methods used by offenders might make parents more aware, and their children safer, it's worth it.

Cyberpredators, just like their offline counterparts, usually aren't the scary, hairy monsters in trench coats we imagine standing on a dark street corner. Many are the kind of person you would be inviting to your home as a guest, and often have. They are pediatricians, teachers, lawyers, clergy, vice cops, welfare workers, journalists, Boy Scout leaders, baseball coaches, scientists, etc. They are almost always men. (Sometimes women are accomplices, but rarely are women the molesters.) They are often articulate and well-educated. They come in all shapes, sizes, and colors, and they can be very rich or out of work. But they have one thing in common: they want your child.

Most of us are sickened at the thought of an adult having sexual relations with a child, but to be able to protect our children, we must get into the mind of the predator. First of all, predators often don't see themselves as predators. They see themselves as loving partners with the children they molest. To them this isn't rape, it's a seduction. And, as with any seduction, it's a slow and painstaking process. (Predators have been known to wait more than two years, collecting data on a particular child, before striking.) That's what makes them hard to detect. They don't appear to your child to be dangerous.



An FBI agent who shared a panel with me recently said it best: “Before the Internet, these people had to get physically close to your children. They had to lurk near schoolyards, or playgrounds. Kids would see them. Adults would see them. It was a dangerous situation to be in for them, because everyone would notice an adult male lurking around children. They often had to take jobs and volunteer positions that allowed them to work with children in a position of trust in order to reach their victims. Now, however, the personal risks the pedophiles had to expose themselves to in order to be around children are gone. Now they can be ‘one of the kids’ and hang out with your kids online without exposing themselves. As long as they don’t say or do something in the public room that makes them stand out, they can stay there forever, taking notes.”

And, many of them do. They have been known to create large databases on children. They track the children’s likes and dislikes. They track information such as whose parents are divorced, who doesn’t like their father’s new girlfriend or their mother’s boyfriend, or who likes computer games or a particular rock group. Kids often share personal information about their lives in chatrooms or on profiles. This is one reason why they shouldn’t. The more the predator knows about your child, the more easily they can “groom” them or appear to be their soulmate.

Some cyberpredators (known as “travelers” to law enforcement) seek out the good kids, the smart ones, the ones who are not street-smart and are from sheltered suburban or rural families. Many of our children match that profile perfectly. Others, however, target (or are targeted by) popular, super achiever, risk preferring teens. It took the death of a young teen from Connecticut, Christina Long, before we realized that many of the incidents involved teens who did not fit the loner profile. What we learned was that these kids never report any attacks or exploitation. The only time we hear of these cases is when the teen is kidnapped or killed.

So who is a typical victim of an Internet sexual predator? Anyone between 11-1/2 and 15. All are vulnerable.

### ***It Doesn’t Take Torture for Them to Spill Their Guts***

Here’s a mock chatroom discussion that my law-enforcement friends and I agree is pretty realistic. Imagine a predatorial pedophile sitting and taking notes on this child, and using this information to lure them later. Would your child fall for this? Most, unfortunately, would. This one is more typical of a boy victim and predator communication than a girl victim communication.

Child: I hate my mom! I know it’s her fault that my parents are getting divorced.

Predator: I know. My parents are getting divorced, too.

Child: We never have any money anymore, either. Every time I need something, she says the same thing: “We can’t afford it.” When my parents were together, I could buy things. Now I can’t.

Predator: Me too. I hate that!

Child: I waited for six months for the new computer game to come out. My mom promised to buy it for me when it came out. She promised! Now it’s out. Can I buy it? Nope. “We don’t have enough money!” I hate my mom!

Predator: Oh! I’m so sorry! I got it! I have this really kewl uncle who buys me things all the time. He’s really rich.

Child: You’re soooooo lucky. I wish I had a rich and kewl uncle.

Predator: Hey! I got an idea! I’ll ask my uncle if he’ll buy you one too....I told you he’s really kewl. I bet he’d say yes.

Child: Really!? Thanks!!

Predator: BRB [cybertalk for “be right back”]... I’ll go and call him.

---

Predator: Guess what? He said okay. He’s gonna buy you the game!

Child: Wow, really? Thanks. I can't believe it!!!  
 Predator: Where do you live?  
 Child: I live in NJ. What about you?  
 Predator: I live in New York. So does my uncle. New Jersey isn't far.  
 Child: Great!  
 Predator: Is there a mall near you? We can meet there.  
 Child: Okay. I live near the GSP Mall.  
 Predator: I've heard of that. No prob. What about Saturday?  
 Child: Kewl.  
 Predator: We can go to McDonald's too if you want. We'll meet you there at noon.  
 Child: Okay. Where?  
 Predator: In front of the computer game store. Oh! My uncle's name is George. He's really kewl.  
 Child: Great... thanks, I really appreciate it. You're so lucky to have a rich and kewl uncle.

Saturday arrives, and the child goes to the mall and meets an adult outside the computer game store. He identifies himself as "Uncle George" and explains that his nephew is already at the McDonald's waiting for them. The child is uncomfortable, but the uncle walks into the store and buys the \$100 game. He comes out and hands it to the child, who is immediately neutralized and delighted. Stranger-danger warnings are not applicable. This isn't a stranger—he's "Uncle George," and if any proof was needed, the computer game is it. He gets into Uncle George's car without hesitation to meet his friend at McDonald's. The rest is reported on the 6 o'clock news.

It's disgusting. It makes us sick to our stomachs, but it happens. Not very often, but often enough that you need to be forewarned. (Several thousand cyberpredator cases are opened each year by law enforcement agents in the United States.) But no matter how often it happens, even once is too often. Knowing how they operate and the tricks of the trade will help us teach our child how to avoid being victimized. Each case differs, but the predators tend to use the same general tactics. Aside from the "bait and switch" scam discussed above, they often attempt to seduce a child. They want the child to "want" them.

#### ***The Script—How They Operate Online***

They begin by striking up a conversation with the child, trying to create a relationship of trust and friendship. They often masquerade as another child or teenager, typically of the opposite sex, unless the child has indicated homosexual interests. (The child may or may not know the "seducer's" real age by the time they meet face-to-face.) Phone calls usually start at this point. Sometimes gifts are sent to the child as well, which may include a Polaroid camera and film. Once they have broken down barriers of caution, they begin introducing sexual topics gradually, often with the use of child pornography to give the child the impression that other children are regularly involved in sexual activities.

Then they begin to approach the child's own sexuality and curiosity, by asking questions and giving them "assignments," like wearing special underwear, sending sexually suggestive photos of themselves to the pedophile, or performing certain sexual acts. These assignments eventually broaden to the exchange of sexually explicit photographs (using the Polaroid, cell phone camera or digital camera) or videos of the child. Finally, the pedophile attempts to arrange a face-to-face meeting. (He may also have divulged his true age or an age closer to his actual age at this point.)

***Why It Works***

All the lectures we have given our children from the time they are very young about not talking to strangers aren't applicable online, where everyone is a stranger. A large part of the fun online is talking to people you've never met. In addition, our children's stranger-danger defenses are not triggered when other kids are involved. The warnings apply only to adult strangers, not to other children.

If any of us walked up to a child in a playground and tried to strike up a conversation, they would ignore us and probably run away. But if an unknown eleven-year-old came up to another eleven-year-old in the same playground, they'd be playing in ten seconds flat! That's how the pedophiles get in under our kids' stranger-danger radar—they pretend to be other kids. And children often believe what they read and hear. They "know" things about the predator because they believe what he told them. They also believe what they read about him in his "staged" profile, which supports what he told them. So it's not just true, it's confirmed.

There are many stages at which the pedophile can be thwarted by an observant parent. In addition, children with healthy friendships and a strong, open, and trusting relationship with their parents are less likely to fall victim to pedophiles online. Pedophiles typically prey on a child's loneliness. They feed the child's complaints about her home life—creating an "us-versus-them" atmosphere. "Your mom is so mean to you! I don't know why she won't let you \_\_\_\_." (Fill in the blank with whatever we try and limit: makeup, malls, concerts, etc.)

This atmosphere does two things: It creates a distance between the child and her parents, at the same time bringing the child into a special secret alliance with the pedophile. (You should know that boys are almost as often the victims of Internet sexual exploitation as girls are, but they report it less frequently.)

I have followed many cases over the last few years. In my role as WiredSafety executive director, I've also been responsible for reporting several of these to law enforcement and for helping many families through the pain of prosecution. Sometimes we just help the families survive what the molestation has done to them. (The child isn't the only victim—entire families are torn apart in the aftermath of a molestation.) Parents feel guilty for not having protected their child, siblings don't know how to treat their fellow sibling—the pain can continue for a lifetime, and even more. And, in addition to being hurt physically, the young victim's heart is broken by the betrayal of trust.

***Anatomy of a Real and Early Case***

One case I reviewed many years ago involved a New Jersey teenager and an Ohio adult predator. It was one of the earliest reported cases of cyber-predatorial conduct, discovered in 1996. Luckily, the liaison was discovered before the girl met the man face-to-face. But it had gone on for a year and a half before being discovered by the girl's mother. As you read the details, think about what could have been done to discover the situation earlier and how you can use these precautions to protect your children.

Paul Brown, Jr., an Ohio resident, was forty-six years old. He was also unemployed, weighed over four hundred pounds, and lived in a basement. He had accounts with several ISPs. Mary (a hypothetical name for the young girl involved) was twelve when her mother, a schoolteacher, bought her a computer, reportedly because Mary was having problems making friends. When she got online, Mary posted a message on an online service, in the spring of 1995, looking for a pen pal. In her message she described herself as a teenage girl. Paul Brown, Jr., responded to the message, using his real name (something they often do, surprisingly) but identifying himself as a fifteen-year-old boy.

Brown and Mary maintained an e-mail and telephone relationship for several months. As the relationship became more involved, they began writing letters, and Mary sent Brown a photograph. He told her that he was living at home with his mother and was hoping to find a girlfriend. In early August, Brown asked Mary for a "favor." "If I sent

you a roll of film, could you get one of your friends to take pictures of you in different outfits and maybe hairstyles? Makeup if you use any, and different poses. Some sexy, if possible. Please. Baby for me. Thanx. You're the best. Love Ya."

Mary complied. For the next eight months, they continued to converse and correspond, and Mary sent additional photos. Brown encouraged her with juvenile antics, such as using stickers in his letters to her saying things like "Getting better all the time!" In May 1996, Brown sent Mary a special love note. "Saying I love you... seems to be an understatement. At the age of 14 you have captured my heart and made it sing... I love everything about you..."

Shortly thereafter, Brown confessed to being in his twenties. He also suggested that Mary videotape herself in sexually provocative poses. She did. After Brown had reviewed her videotape, he returned it to her with instructions to redo the tape and include views of her genitalia and breasts. He later admitted to being divorced and in his thirties. He reportedly also sent her small gifts from time to time.

A few months later, in response to Brown's promise to pass copies of the tape to four members of a rock band Mary admired, she sent additional videotapes to Brown. (Brown told Mary that he knew the band members very well.) Each tape sent to Brown was designated for a different member of the band and contained sexually explicit conduct. Brown apparently had also sent her his size 48 underwear. When her mother discovered the underwear, the authorities were notified. Tracing Brown through phone records, special agents of the FBI in Cleveland seized the videotapes and photos of Mary and of more than ten other teenage girls from across the country.

Mary was fourteen when this was all discovered. Brown pled guilty to enticing a minor to produce sexually explicit photos and videos and was sentenced to a little less than five years in prison (the maximum penalty for a first offense). In a written statement to Brown following all of this, Mary said, "I trusted you. I thought you were my friend."

There are several things that stand out in this case. One, interstate phone calls were made by Mary. Parents should always be reviewing long-distance bills for suspicious calls. Two, Mary was lonely. These kinds of children are often the most vulnerable; a parent should be involved in their online friendships, and monitor their online lives. And, three, as hard as it is to know what our kids are doing when we're not around, especially if you are a single parent, a year and a half is a long time for a relationship to be going on undiscovered. You should spend time learning who your children's friends are, online and off. But Monday-morning quarterbacking is always easier than playing the game in real time. We may look at the situation and say that could never happen to one of our kids. However, there but for the grace of God go all of us...

Knowing your child is lonely and has problems making friends is the first sign that the child may fall prey to a pedophile or cyber-predator. Predators can spot lonely children. They can also spot kids who are new online and may not yet know all the rules. Most teens, when surveyed, admit to having been propositioned online. But what may be obvious to a cyberstreet-smart kid may not be so obvious to a child not yet familiar with cyberspace. Pedophiles befriend these kids and patiently build trust and a relationship—looking toward the day when they can meet face-to-face.

Encourage your children to make online friends, but learning about their online friends is an important way to avoid these secret relationships. Education is important in avoiding this danger, too. (Had Mary been forewarned about how pedophiles operate online, she may have been more attentive to how old Brown sounded on the phone, and been more aware of his classic tactics.) So is control over incoming and outgoing information when younger children are involved, using technology blockers, monitors, and filters. These kinds of situations can be avoided if you plan ahead, educate and communicate with your children, and keep your eyes open.

***Getting in Under Your Radar:***

Even when parents are watching, bad things can happen.

I included the Paul Brown case in my first book, *A Parents' Guide to the Internet*. (He was sentenced in 1997, when I wrote the book.) I included it because it was a good example of how cyberpredators typically operate, and suggested that if the mother had been a bit more attentive, it might have been discovered earlier. I was right about how cyberpredators operate. I was wrong about how being attentive might have avoided the sexual exploitation. It takes more. It takes both an attentive parent and a teenager who has been taught how these pedophiles operate online.

In November 1998, I met a mother who did everything right. She was attentive and inquisitive about her daughter's online relationships. She asked the right questions. She had a good relationship with her daughter, and yet Charles Hatch, a child molester from Utah, got in under everyone's radar and sexually exploited her thirteen-year-old daughter.

Jennifer (not her real name) was eleven and a half when she first met "Charlie" online. She thought he was a few years older, and was intrigued about befriending a slightly older teenage boy. Jennifer was an honors student and had already been taking advanced college courses while still in middle school. She lived in a loving and warm household with her mother and father. She also had siblings and half siblings from her father's previous marriage. They were all close.

Jennifer's mother, Sharry (also not her real name), talked to Jennifer about her online friend, Charlie. She insisted on talking to Charlie himself, by phone, once he and Jennifer had started calling each other. He passed the phone call test, and Sharry was convinced that he really was the teenage boy he professed to be. Either he had manipulated his voice to sound younger or he had a younger person make the call. Charlie even called and spoke to Jennifer's brothers, talking about when he would be their brother-in-law someday, after he and Jennifer were married. He pleaded with Jennifer to come and visit him in Utah. Sharry invited him to visit them instead. But Charlie always had a reason he couldn't come.

As things progressed, Sharry insisted on talking to Charlie's mother. He first avoided it by saying she was sick, later that her sickness had become cancer, and that eventually she died from the cancer. The family fell for this, hook, line, and sinker. Most caring families would. Although the "relationship" progressed for almost two years, it remained relatively tame. Charlie was romantic rather than predatorial, and he sent her expensive gifts, including a Polaroid camera. (Remember the Polaroid camera Paul Brown sent?)

Jennifer was inexperienced with boys and dating, and Charlie seemed to know not to push her too fast. But about a year and a half after they met online, Charlie sent her sexually explicit photos of himself from the neck down. She became very uncomfortable and pulled back. But several tragedies occurred around the same time, which made Jennifer easier prey. Her father was hospitalized with a serious illness, and her sixteen-year-old half brother died of a brain hemorrhage.

Charlie, like all good predators, knew when to strike. He told Jennifer that she owed him sexually explicit photos of herself, since he had sent those of himself. When she refused, he told her that she would be left alone, since her family was dying or would die—and he threatened to leave her. Reluctantly, after fighting against it as hard as she could, she acquiesced and sent him sexually explicit photos of herself.

When Sharry was cleaning Jennifer's room, she discovered a letter in which Charlie had set forth the sexual poses he wanted Jennifer to photograph. Sharry sent him a letter, confronting him. She said that he didn't sound like a teenager in the letter. She told him that if he ever contacted her daughter again, she would inform the police. He never replied, and Jennifer was not permitted to use the Internet for months.

One day, just when Jennifer and Sharry thought that the whole episode was past them, the phone rang. It was a detective from Utah, who informed Sharry that Jennifer's

photos had been discovered in Hatch's day planner by a coworker. He wasn't sixteen—he was thirty-six. He was a former teacher who had been dismissed by the school after having been accused by a student of sexual abuse. (The school hadn't taken any other action.) He was currently employed by the welfare office in Utah, and was married with children and step-children.

Six months later, Charles Hatch was convicted of sexual exploitation in a Utah federal court. He began his six-and-a-half year sentence in early June 1999. As a condition of his plea, he will not be permitted to use the Internet. This mother has become a dear friend of mine, after seeking WiredSafety's help in getting through this. She was the first parent to speak out publicly about her child being targeted by a sexual predator online.

Unfortunately, the predators are willing to try many different ploys until one finally works.

### ***Using Celebrity's Names***

I was having lunch in Los Angeles with one of my girlfriends when Nick Lachey walked into the restaurant. She pointed him out to me and I immediately grabbed my business card and approached his table (to the utter embarrassment of my friend). I introduced myself and told him I needed his help. I explained that predators were using his name and the name of other celebrities to lure kids into meetings and unsafe activities. They find teens who post their favorite celebrities on their profiles, websites or other online communications. Then they create a profile claiming to be a close personal friend of that celebrity. They offer to forward a pic of the teen to the celebrity, and seek sexier and sexier pics as time goes on, ultimately ending with an offer to introduce the teen to their favorite celebrity in real life. Years ago, Justin Timberlake was the most popular of these celebrity lures. Nick is now. He listened intently and turned white when he realized people were using his name to hurt his young fans. He offered his help.

When I left his table, he has agreed to do a public service announcement to help teens understand that if anyone claims to be a close personal friend of a celebrity, they aren't. Or won't be for long. I was very excited, but not as excited as I was two weeks later when someone from Nick's office called asking me to help them create a safer teen-only social networking site called YFly.com. I agreed and YFly.com became a reality with the financial assistance of Tom Petters (and the Petters Group), and the creativity and energy of its founders, Drew Levin and Daniel Perkins. I joined the team to set up a safer network and create the most advanced educational and awareness content online, just for teen users. The young users can click on "Report the Creep" if they suspect someone is an adult posing as a teen.

It's a beginning. Finding safer technologies and services is part of the solution. So is awareness using teenspeak.

Shannon, one of our Teenangels is 14 years old. She was selected by Teen People as one of the twenty teens who will make a difference. She has gone from one better...she is already making a difference. It is with pride that I introduce Shannon Sullivan, one of my Teenangels.

### **Common Internet Sexual Predator Ploys...How it works online**

WiredSafety has done a substantial amount of research on how predators operate offline and online. Working with missing children organizations internationally, Internet providers, law enforcement and victims and their families, we have developed a substantial knowledge base about how teens and preteens are lured into offline meetings and online sexual exploitation. From the young victims of sexual predators and online sexual exploitation, we have learned the typical [ploys and how they unfold. By handling online one-to-one help for victims of cybercrime and cyberabuse, we have learned what

parents and teens need and how to get them assistance quickly. WiredSafety has stood on the front line against Internet criminals and abusers since 1995.

There are certain tactics that sexual predators use offline to prey on children offline, whether they are strangers or someone known to the child. Interestingly, these same ploys are often used online, by Internet sexual predators, with some “virtual” modifications. Only a few ploys, which are aided by the anonymity of cyberspace, are unique to cyberpredators. Until our recent work, no one has pulled together a list of common predator ploys used by offline sexual predators and compared them with the ploys used by online sexual predators. Our researchers are developing additional materials and studies to expand what we have already learned.

This new research is crucial to keeping our teens and preteens safer. Protecting young people from Internet sexual exploitation is much easier if the young people are aware of the kinds of tricks and ploys used by the predators. If they are alert to possible “ploys” they are less likely to be caught off-guard. Many of these ploys are used over and over again by perpetrators and taught to others within their child molester communities. They include: asking you child for assistance (this is the help me find my puppy ploy, when used offline), the love and affection, confidence and trust ploy (where the child is groomed to fall in love with their online soul mate), the curiosity ploy, the fear tactic, the games and fun, the fun and job offers and the modeling, talent scout or beauty contest ploys.

“Don’t talk to strangers” is probably the most common warning parents give their children in an attempt to prevent abduction or exploitation. Unfortunately, these warnings don’t work in cyberspace, where one of its greatest benefits (and the most fun for teens) is being able to communicate with strangers. In addition, unlike the perception of a “stranger” as the raincoat clad, dirty, bearded man who lurks on street corners or in playground, Internet “strangers” quickly become Internet “friends” and the stranger danger radar is no longer working. The kids, tweens and teens are no longer treating them with care, and have let them into their inner-circle. That’s where the real dangers begin. These child molesters can get in under your and our children’s stranger danger radar.

Sometimes this happens because they believe their net friend is another young person. And a “stranger” is never another young person. Unlike the offline counterpart ploys, a 47 year old can easily masquerade as a 13 year old online. Or someone can be three or four different people at the same time online, engaging in conversations with themselves in a public setting, allowing young by-standers to think they are trustworthy, or famous or otherwise worth talking to. Online our children are in the dark, literally.

With the number of young sexual predator victims growing, and the amount of contact information young people are sharing online in blogs, profiles and away messages putting them at greater risk, awareness and prevention in these areas is crucial. Partnerships with Internet service providers, media and entertainment companies and learning from and sharing what we know with each other is what needs to be done. And, it is worth the effort. Our children are entitled to sleep more safely at night, and enjoy the wonders of the Internet...without fear of being preyed upon or hurt.

### **Parents are the Beginning**

From the time I published my first book for parents on Internet safety in 1997 (*A Parents Guide to the Internet*) we have been educating parents on how they can stay ahead (or at least on par :-)) with their children and teens online. Our quick guide - Parenting Online, is available online without charge and has been copied and distributed by hundreds of groups and schools around the United States. It includes a parent/child contract, a quick guide to parental control technologies and our very popular "Common Sense to Cybersense." (A copy of this guide is attached as part of the Parenting Online Guide.)

Now, many parents want something quick. They are happy that expert groups such as WiredSafety.org understand all the issues and that they can turn to us. But they are being pulled in so many directions just by virtue of their parenthood, that they want "Just the Facts...Madam." Our new programs, called Internet Safety 1-2-3 make it easy for parents to spot the risks by age, and also by technology. Our new automated Family Internet Safety Plan works using this new approach (patent pending) to help parents understand what works for them and what things they need to do to keep their family safer, given the technologies they use, the ages of their children and their value system. (A quick example of the kinds of things covered is attached as an Appendix 3 in our "Cheatsheet on Risks by Age".)

Our children are worth it, and so is the Internet. Too often blamed for everything from the Black Plague to the sinking of the Titanic, the Internet is a wonderful tool for learning, communication and entertainment. It levels the playing field between the haves and the have-nots. All children look alike online. No one is classified by their race, ethnic origin, religion, accent or physical ability. Online they are all just children. And like it or not, the Internet is here to stay.

We're all in this together. Let's work together to make the Internet fun, safe, private and educational for children. And let's work together to make sure that the children's Internet industry, which has so much to offer our children, flourishes!

For the children.

I remain willing to help, and provide input and expertise in any way this Subcommittee can use my help and expertise.

I wish to thank the Subcommittee, its chairman and all its members for inviting me to present this testimony on such an important subject.

Parry Aftab, Esq.



**APPENDIXES:****Appendix 1: WiredSafety's Guide to MySpace.com**

This was posted on MySpace.com as a public service from June 2005 to help parents understand how to keep their children safer on the site.



(a 501c-3 corporation)



## WiredSafety's Guide to MySpace.com

Hi! My name is Parry Aftab.



I am an Internet privacy and security lawyer and founded and run the world's largest online safety and help group, [WiredSafety.org](http://WiredSafety.org). You may have seen us on TV or read about us in magazines or newspapers on Internet safety issues for every member of the family. We specialize in helping protect kids and teens online. We also have extensive information for adults on Internet safety, privacy and how to avoid becoming the victim of identity theft, cybercrime or cyberabuse. And are the leading resource for parents on Internet safety.

We are posting this information and our guides and other materials available to help MySpace users as a public service. We are not employed by or legally affiliated with MySpace. We are an independent charity devoted to helping everyone stay safer online. And MySpace is serious about trying to help their users be safer online. That's why we have agreed to make our materials available at MySpace and provide special help for MySpace users and parents of MySpace users.

It's a challenge protecting privacy and personal information while building a blog or profile page no matter how old you are. But there are some tricks and tips [WiredSafety.org](http://WiredSafety.org) has pulled together over the years that might help you stay safer while letting you express yourself on MySpace.com. To learn how to protect yourself better online, read our MySpace.com Safety Guide and other safety tips at [WiredSafety.org](http://WiredSafety.org).

**For Parents:** Recently, I have been receiving a large number of inquiries from schools, parents, regulators and the media about social-networking websites. I decided that it was important to address parent concerns and answer their questions. Where better to do that than on the most popular of all social-networking sites, MySpace.com?

MySpace.com and other similar sites are designed to allow people to share their creativity, pictures, and information with others. It also allows them to network with others online.

Sometimes people do this to find romance. Sometimes they do it to find friends with similar interests. While this may be okay for adults, it is not okay for kids.

MySpace.com recognizes this, and prohibits anyone less than 14 years of age from using their website. There are special rules and settings for teens between the ages of 14 and 16 too. These rules and settings are designed to help these younger teens better protect their privacy and be safer on our site. You can learn more about these settings at [WiredSafety.org](http://WiredSafety.org) and at MySpace.

Unfortunately, while MySpace has set rules to keep preteens and younger teens off the site, they can't prevent kids from lying about their age and pretending to be 14 years of age or older. To address this, MySpace.com has developed methods designed to help identify preteen members by reviewing certain content of member profiles. It doesn't review their photos to determine if the person appears to be younger than their stated age, but can scan the profiles looking for certain words and statements that can often give away the young person's real age. It's not perfect, but it does help spot many underage members. Thousands have been removed from the site for having misstated their age. And I expect that thousands more will have their profiles deleted in the months to come.

MySpace.com really does try to keep them off their site. Many other similar sites do not. That's why we agreed to post our safety information there. They care and are working hard to keep the site as safe as possible. That matters to us at [WiredSafety.org](http://WiredSafety.org). If your teens are going to lie about their age and post a profile somewhere online, I would prefer it's at a site that cares about their users and is willing to work with an online safety group, rather than one that doesn't care or seem to care at all.

But no matter how much they may care about the safety of their users, some parents are shocked about what their teens are posting online and the things they admit to have done offline. And a shocked parent (or a frightened one) is often an angry one. Before you do anything else, take a breath. Think about how your parents would have reacted if they had been able to record everything we said and did with our friends, when we thought they weren't around. I would still be grounded, trust me!

Then, take another breath. Make a cup of coffee or tea and prepare to handle a tough parental choice. (I know, all are tough ones these days, but this one is especially challenging.)

Have you seen their page yet? If not do you know how to find it? You should start by asking your teen to show it to you. If they refuse, or you want to see it before you confront them, you can search for it easily. You can learn how at [WiredSafety.org](http://WiredSafety.org).

If you discover that your child is posing as someone older and using their site, you have two choices. You can have the site taken down, or you can supervise what they are posting and doing at MySpace.com. It's important to all parties that you help maintain your child's safety while online. Unfortunately, while we at [WiredSafety.org](http://WiredSafety.org) can help you keep yourself and your family safer online, we can't do your job for you. We need your help.

For parents, the procedures for deletion of an underage MySpace account fall into the following two primary categories. No matter which one applies in your case, you should take advantage of this opportunity to review their page first. You might be surprised (hopefully pleasantly).

If they haven't posted anything to put them at risk, and aren't communicating with strangers, ask them why they want a page at MySpace.com. You might be surprised at what they tell you. While parents freak out (understandably) at the provocative images and wild language used by many on MySpace (even though they violate the site terms of service rules), most of the teens don't see them or pay attention to them.

Believe it or not, they are there to show off their creativity and self-expression and to communicate with their offline friends. As long as they are old enough to understand the rules and adhere to them (no one under 13 is old enough for this, even with parental approval in my humble opinion), and as long as you keep an eye on what they are doing, posting and how they are communicating with others, it's YOUR choice as to whether they keep their site up or not. (Make sure that you don't become the self-appointed MySpace.com police, reporting other people's kids for posting underage until you speak with their parents first!)

If you find that they are saying and posting inappropriate things or those comments don't seem to conform to their otherwise good offline behavior, don't panic yet. Think about how our parents would have reacted if they could have seen or heard everything we said to our friends when no adult was around. I guarantee that they would have been almost as shocked as many parents are about what their kids are posting online. Also, remember that many of the things your kids are saying are being said to impress their audience and are often not true. (Lucky!)

The important difference between what we used to say or do and their posting online, however, is that when we acted out or boasted about acting out, we didn't do it to an audience of millions of people (including our parents, principals and everyone else). So, while you shouldn't panic, you should take quick action if your kids are posting personal information in a public forum, such as MySpace.com, or communicating with strangers online. Either have them remove the personal information and use a photo software program to alter their pictures (to a pixilated, cartoon or sketched form that can't be misused by others or used to identify your child offline) or have them take down their profile page entirely. (Note that if you overreact they will just rebuild another one tomorrow at MySpace or another site.)

You can learn more about how to help them surf and communicate safely at [WiredSafety.org](http://WiredSafety.org), [WiredKids.org](http://WiredKids.org) or [Teenangels.org](http://Teenangels.org). If you fear that they are communicating with strangers, or even thinking about meeting them offline report it right away to the authorities or to the [cybertipline.com](http://cybertipline.com). We are building a new page just for kids on sexual predators - [Katiesplace.org](http://Katiesplace.org). Victims of Internet sexual predators are helping us explain the real risks in terms the kids can understand. This is up, and growing (it will always be under construction, we hope, improving as we add more and more features and content.) Then you can send them to [KatiesPlace.org](http://KatiesPlace.org) to learn how Internet predators operate. It may help scare them safe. If you fear that they are being cyberbullied, check out our [Stopcyberbullying.org](http://Stopcyberbullying.org) page, or reach out to [WiredSafety.org](http://WiredSafety.org)'s cyberbullying help line.

With that being said, here's how you can have their page taken down from MySpace.com:

#### **Taking Down Your Child's Profile Page:**

There are two ways to have their pages taken down, or everything on them deleted. You can do it the easy way (with your child's cooperation) or the hard way (without their cooperation). Even if they are cooperative, though, their friend may have set up their account using a fake e-mail address, or they may have used a fake e-mail address, or they

could have forgotten their password or their friend never gave it to them. These may require you use the Alternate Account Closure Process, below.

**If your child has their password and is cooperative, and used a real e-mail address when setting up their account:**

First try asking your child to take it down themselves. They have a password for their page that can be used to remove anything (or everything) from their page. Tell them to use it to wipe their page clean of any content or contact information. Then you can move forward to remove the entire profile or not. Since the page will be entirely blank, it won't make any difference if it remains up.

If you want to go through the bother to take down the empty profile page, this is how you do it:

- Logon to MySpace
- Click "Account Settings"
- On the "Change Account Settings" page, click on "-Cancel Account-"
- Click on the "Cancel My Account" button in the confirmation box.
- Include remarks if desired; then click on the second "Cancel My Account" button to complete the request process.
- A cancellation message will be sent to the email address of record. Replying to this email **is required** in order to complete the automated account closure process.

Note: If your child lied about their e-mail address when setting up the account (see, they do know something about protecting their privacy ☺), this won't work. The e-mail with the automated process link has to be received and replied to. So, even if your child is cooperative, you'll need to follow the instructions to remove a page if the e-mail address used to set up the account is not operational. It may not be worth it if you followed my advice and removed everything on their page anyway.

Note that many ISPs and e-mail providers block MySpace communications, thinking they are spam. So, when they send the instructions, they might not get through. If that happens, you should use the method set out below that we helped MySpace create.

**Alternative Account Closure Process:**

**If your child is cooperative and had their password, but used a fake e-mail address or someone else's e-mail address when setting up the account; or**

**If your child claims not to know their password or lied about the e-mail address when setting up the account, or is uncooperative**

Unfortunately, in addition to lying about their age, many kids will use a bogus e-mail address when applying for membership, or may profess to have (or really have) forgotten their passwords. Often friends set up profile pages for their close friends and use a fake e-mail address or never turn over the password. These circumstances can make it virtually impossible to use the process outlined above.

MySpace recognizes this reality and has established special account cancellation procedures to deal with these contingencies. (These are unfortunately required as many teens cyberbully and harass each other, notifying MySpace.com to delete a profile while posing as the parent of their victim.) When a parent wishes to close an underage account and either the child is uncooperative, or a technical difficulty precludes the use of the general account closure method, the following procedures can be used.

If they know their password but don't have a real e-mail address or can't remember it, have them remove everything from their account, leaving a blank page, except for typing in "remove this profile" somewhere on the page. Then notify MySpace.com's customer service staff giving them the exact url of your child's profile (what appears in the window of your web browser when you are viewing their page (cut and exactly copy it into the e-mail). Ask them to remove the profile and let them know it is blank and has a posted instruction to remove it. This let's the customer service staff know that it is an authorized removal. As long as you have given them the right url and the message appears on the profile, the profile page will be removed as quickly as possible.

If your child does not have their password, or claims not to have it, it's a bit more complicated. First contact MySpace.com's customer service staff at [customercare@myspace.com](mailto:customercare@myspace.com). This request HAS TO include your child's URL address in the form. It is the address that appears in your browser window when you access their profile page. It starts with "www.myspace.com/" and will include numbers that identify their own profile page. (For example, an address could be [www.myspace.com/123456](http://www.myspace.com/123456).) This information can also be located on the left-hand side of the Welcome page that is displayed following your child's initial logon.

When MySpace.com's help staff receives your e-mail, assuming your child's profile is included in the email, the site will review the account for any definite indications that the account owner is underage. If definite proof IS found, the child's profile WILL be removed and an email will be sent to the email address on the account explaining WHY the account was deleted.

If the child's URL is NOT indicated in the cancellation request, the parent is emailed with a request for the information.

While all parents should work WITH the child in removing the account through normal cancellation procedures discussed above, if the child does not have their password or claims not to have their password, the parent must submit an affidavit stating that they are the custodial parent or legal guardian of the child, the birthdate of the child, that they want their child's profile removed and that their child does not have the password to remove their profile information or has used a fake e-mail address and therefore cannot use the normal account closure procedure, and providing offline contact information. E-mail [customercare@myspace.com](mailto:customercare@myspace.com) for an address to mail it. The MySpace.com personnel will then contact the parent or legal guardian by phone number in order to confirm the custodial parental or legal guardian status of the requestor. Upon successful verification, the minor's account will be removed while on the phone with the parent or legal guardian.

If schools need help with one of their students, there are special e-mail addresses set up just for school administrators. And with our help, MySpace has adopted the most liberal law enforcement policy online. If their users is at risk, they want law enforcement to have the information and access they need to protect them. They have hired a law enforcement liaison to help law enforcement agencies and have published a law enforcement

investigators guide, which we helped write.

While MySpace.com is doing its best to keep your children from using their website and lying about their age, it's up to parents to do their job too. Parents need to talk with their children about not sharing personal information online. Personal information includes pictures, names and addresses, schools they attend, cell and phone numbers and many other less obvious things, such as the name of their school team, ethnic background and even a mall near your house. (You can learn more about how to talk to your kids and what you should be asking at [WiredKids.org](http://WiredKids.org) or [WiredSafety.org](http://WiredSafety.org).)

We are developing a special program just for parents concerned about their kids using social-networking and online dating sites. It will teach you what you need to know about finding out if your child has a profile on one of these sites, how to review them and remove them, if you want to. It will also help if your child is being cyberbullied by other members from these sites, or is cyberbullying others.

The best way to find out if your child has a profile on this or another similar site is to ask them. If you're not sure that your child is being honest with you, you can search MySpace.com using their e-mail address, or by searching for their school. (You click on "search" and enter their email address or full name in the appropriate search box.) If you find that your child has a profile on the website, you should review it. It's amazing how much you can learn about your child by reading their profiles. Does it contain personal information, such as their full name, address or phone numbers? Has your child posted photos? Are they photos of themselves or someone else? Are they sharing poems they write or provocative comments about themselves or others?

Ultimately, protecting your child is your job. We will be building a few tutorials at [WiredSafety.org](http://WiredSafety.org) and at [MySpace.com](http://MySpace.com) to help parents and their children understand how to be careful when communicating publicly online.

Ask them why they created the profile. You might learn that they wanted to share their thoughts with others, make new friends or even allow others in their school to get to know them better. But not all of their motives are as noble or safe. Some may be interested in meeting new romantic interests or role-playing inappropriately online. And when a young preteen lies about their age posing as a seventeen year old at the site, that can be a serious problem. Others in their late teens might approach your child thinking they were older. That's bad for everyone.

If you discover that your child is posting provocative comments or inappropriate images online, it's time for the tough talk. The one about stranger dangers and how that cute eighteen year old boy they meet online may not be cute, may not be eighteen and may not be a boy. (Parents of young boys need to understand that their children are equally at risk. About one-third of the cases of Internet sexual exploitation are men exploiting boys.) Our children need to realize that there are real risks relating to meeting strangers offline, including murder. The first confirmed murder victim by an Internet sexual predator was thirteen when she died, three years ago May 2005. The risks are real, not matter how smart, sophisticated or tech savvy your kids are. We recommend the book, *A Girl's Life Online*, by Katie Tarbox. We are also developing a few videos for teens teaching them about standard plays used by Internet sexual predators to lure a young boy or girl into an offline meeting or sexual exploitation situations online.

It's not easy raising children anymore. It is even harder when the parent is expected to be

expert in Internet, cell phone and interactive game risks. The good thing is that you're not facing these challenges alone. We're here to help.

Just remember that while your kids may know more than you do about technology, you know more about life. And you are allowed to set the rules and enforce them. You're still the parent! There is software you can install that will record what your kids say and post online. There is even one that will e-mail you reports at work. The ones I like best are made by Spectorsoft, and can be found at [software4parents.com](http://software4parents.com) or [spectorsoft.com](http://spectorsoft.com). But don't use them just to spy on your kids. Treat them like a security video camera in the corner of a bank. No one views the tapes unless and until there is a break-in. Do the same here. Check the program reports if something goes wrong. It will collect whatever you need for evidence and to help your child if something goes wrong.

Also, check your parental control programs. Many, such as AOL's and MSN's, can block access to social-networking websites or other sites you think are inappropriate for your younger child. There are many other products you can purchase to block sites as well. (Check out [software4parents.com](http://software4parents.com) to learn about and purchase some of these.) Just remember that the best filter is the one between your children's ears.

If your child is being bullied by another MySpace.com user online, check the terms of service first. If the bullying violates MySpace.com's terms of service, report it to TOS and the offending comments and/or profile will be removed. If something serious occurs and you need to reach out to law enforcement, let them know that MySpace.com has created a special procedure for law enforcement inquiries, especially when the safety and well-being of its site users is involved. They should contact [abuse@myspace.com](mailto:abuse@myspace.com). Cyberbullying is a growing problem. You can learn more about it, as well as how to prevent and handle cyberbullying incidents, at WiredSafety's [StopCyberbullying.org](http://StopCyberbullying.org) and [InternetSuperheroes.org](http://InternetSuperheroes.org). [WiredSafety.org](http://WiredSafety.org) also has a reportline link for victims of cyberbullying, their schools and parents where specially-trained volunteers assist victims of cyberstalking, harassment and cyberbullying without charge.

If schools are looking for a presentation or program to address their students' posting inappropriate profiles or using these websites while underage or other parent concerns, they should visit [WiredSafety.org](http://WiredSafety.org), [WiredKids.org](http://WiredKids.org) or [Teenangels.org](http://Teenangels.org). Schools may find many of their students using a particular website. Working together with schools and parents, we may be able to keep our kids off of website that are inappropriate for young children and teach them to make good choices online and offline.

If you have other questions, contact me at [askparry@wiredsafety.org](mailto:askparry@wiredsafety.org).

Stay safe.

Parry Aftab, Esq.  
Executive Director,  
[WiredSafety.org](http://WiredSafety.org) ([wiredsafety.org](http://wiredsafety.org))  
The world's largest Internet safety and help group

**Learn more about [WiredSafety.org](http://WiredSafety.org)!**

## **Appendix 2: Parry Aftab Bio and CV**

### **Contact Info:**

Dr. Parry Aftab  
 Parry@Aftab.com  
 www.aftab.com  
 +1-201-463-8663

### **Introduction:**

Parry Aftab was one of the first lawyers to practice Internet law. Known for her ability to think outside the box, she quickly became a leader in the emerging area of Internet law and policy. She now devotes most of her time to issues impacting children and families online. Dr. Aftab is the award-winning "Privacy Lawyer" columnist for Information Week magazine. She is a frequent expert resource for and quoted by most leading media outlets, online and offline, around the world. Dr. Aftab is a sought-after public speaker and the author of several books. When Internet policy and consumers and families online are involved, hers is the first name mentioned.

### **About Parry:**

Parry Aftab resides in the NY metropolitan area. She started out on Wall Street in 1984, as a corporate takeover lawyer. Along the way, she completed her undergraduate degree in less than 2 years, as Valedictorian, with her two children in tow. She is a member of *Phi Beta Kappa* and an NYU Law School graduate with a *juris doctorate* degree. Her work with children online began following a CNN appearance on Internet censorship in 1997. She founded and runs the world's largest Internet safety group and works closely with law enforcement, the Internet industry and governmental agencies around the world. Dr. Aftab has received many awards for her work.

### **Areas of Expertise:**

Parry Aftab is a legal expert in all aspects of best practices and cybercrime and abuse. She has advised the Internet industry on consumer and children's issues since 1994 and is called the "Kids Internet Lawyer." Dr. Aftab expanded her focus to privacy and security law and the application of sound practices to new interactive technologies. Her expertise now extends to interactive gaming, mobile and wireless technologies, as well as the Internet. Unlike many experts, Dr. Aftab's talents include her ability to factor in societal, values and legal differences around the world. This enables a truly globally sensitive approach to a global medium.

### **Additional Information:**

Her first book, *A Parents' Guide to the Internet...and how to protect your children in cyberspace*, was released in December 1997. It was a guide for the "technology challenged" parents providing practical solutions to parents' concerns about Internet safety. Her second book, *The Parent's Guide to Protecting Your Children in Cyberspace*, was published by McGraw-Hill and released in 2000 in the United States. It was subsequently adapted for the UK, Singapore and the US Spanish-speaking market. Her third book on Internet safety was written expressly for families in China. It was released in November 2004, in Chinese. Her latest book is a shorter and updated version of her second book, written exclusively for Spain and Spanish-speaking South and Central American families. Her second book, even out-of-date and out-of-print, it is still considered the leading resource for parents on Internet safety for their children. Ms. Aftab reacquired the rights to that book and will be making sections of it available without charge at WiredSafety's website.

Although her vocation was Internet security and privacy law, her avocation is children online – helping them become good cybercitizens and keeping them safe, private and secure online. She is dedicated to helping curb Internet-related crimes against children and assisting law enforcement in bringing the child predators to justice. Everyone who encounters Ms. Aftab is impressed with her passion and energy when children's Internet issues are involved. She has devoted all of her money and time to these issues, since stumbling on an Internet image of a 3-1/2 year old girl being raped online. Ms. Aftab defines that moment graphically as "a branding iron being applied to your brain. It leaves a permanent and painful memory. It stays with you forever."



While her passion is for protecting children from Internet sexual exploitation, she is also devoted to empowering them through access to the wonders of the Internet. She hopes to help all children become better informed and responsible cybercitizens, controlling the technologies instead of being controlled by them. Her programs are designed to teach them safe, private and responsible technology use, which includes teaching them good netiquette and respect for each other and the rights of others, including intellectual property rights of the music, movie, gaming and software industries.

Her newest project, Peers2Peers (peers2peers.org) is designed to teach children and teens to understand and respect intellectual property rights, whether to music, software, games, movies or trademarks. Understanding that the fastest way to stop wholesale piracy (especially of motion pictures) is to teach the children to pay for what they download, Ms. Aftab has combined forces with some of the key players in the IP markets, including major artists, Marvel Comics, multimedia lawyers, software manufacturers, game designers and members of the motion picture industry to help teach kids that everyone has a stake in protecting the legal rights of others. The Peers2Peers program includes classroom lesson plans and curricula, videos and public service announcements as well as a competition where youth volunteers can design their own public service awareness campaigns.

Ms. Aftab was among the first in the world to devote her talents to keeping children safe online. She has helped design programs for parents and children in a wide range of Internet-related issues since 1997, including the P.I.E. Program (Parent Internet Education) for the Baltimore County School system. This was the first of its kind, in educating parents and families about safe and fun online use. She is also an expert on filtering and blocking products. And now provides best practices guidance (in her role as head of the charity) to most of the social networking sites online, around the world.

Her work has been recognized by leading technology influencers, such as Family PC Magazine, when she was awarded Internet Pioneer of the Year in 2001. And child protection agencies have recognized her as well, when Child Abuse Prevention Services presented her with their 20<sup>th</sup> anniversary Community Leadership Award in 2005. (Past recipients of this award include Senator Clinton, Linda Fairstein, Judy Collins, Dr. Joyce Brothers and the "God Squad.")

Parry Aftab also provides parent Internet education and online safety content for such diverse sites as Nickelodeon, Children's Television Workshop, Disney, Microsoft, AOL, AT&T and MSNBC. She is a regular keynote speaker, and resource on camera for the media on diverse cybercrime, safety, privacy and cyberlaw issues. Recently she became The Privacy Lawyer columnist for Information Week Magazine where she writes on a range of topics that affect technology, policy and privacy. Her expertise is especially in demand on children's Internet issues, because no one knows more about children online than Parry Aftab.

While she is devoted to protecting children online, Ms. Aftab seeks to empower children and their parents, not the censors. Her common sense approach to technology risks and solutions works as well anywhere in the world as it does in the United States. But what really makes her special is her ability to tap into the caring and creativity of young people to craft solutions that are written in their language and designed for their needs.

She is a frequent and respected resource for news programming and print journalists around the world. Her expertise has been featured nationally and internationally in online and print publications, including Readers Digest, Playboy, TV Guide Magazine, Cosmopolitan, People Magazine, Redbook, Biography, USA Today, Information Week, Working Women, Teen People, U.S. News & World Report, Family Circle, Newsweek, Ladies Home Journal, Smart Money Magazine, PC Magazine, Good Housekeeping, Better Homes & Gardens, Family PC Magazine, Yahoo! Internet Life, Information Week, CIO Magazine, The Wall Street Journal, The New York Times, The LA Times, most regional newspapers in the United States, The London Times Magazine, The Strait Times (Singapore), The South China Morning Post Sunday Magazine (Hong Kong), and more. As a result of her work online with children, Ms. Aftab was selected as a charter member of Children Television Workshop's Advisory Board, as well as appointed to The

National Urban League's Technology Advisory Committee. In 2003 she was elected to TRUSTe's Board of Directors. She served on the advisory board for the Ad Council for two terms.

Parry Aftab has spoken to many governmental agencies and groups worldwide, conducted briefings for the U.S. Senate, been a key speaker at the White House Summit on Online Content, the sole Internet-related expert speaking at the 2002 White House summit on Missing and Exploited Children and testified before leading legislative committees and The House of Lords, all with the same message: The Internet is a wonderful resource for families, and once parents understand the online risks, they can use common sense (and perhaps some filtering tools) to help their children enjoy cyberspace safely.

As one of the first lawyers in the world to specialize in Internet legal issues, Parry Aftab is admitted to practice law in New York and New Jersey. She attended law school at NYU School of Law where she received her J.D. degree. She received her B.A. degree as *Valedictorian* of Hunter College (having completed her full undergraduate degree in less than two years), where she was inducted into *Phi Beta Kappa*.

She resides in the New York metropolitan area and is a mother of two. Ms. Aftab can be reached at [Parry@Aftab.com](mailto:Parry@Aftab.com).

**Parry Aftab****Professional Curriculum Vitae**

Phone: 201-463-8663  
[parry@aftab.com](mailto:parry@aftab.com)

---

Internet privacy and security lawyer, licensed to practice law in NY and NJ,  
 The Privacy Lawyer columnist, author, consultant and public speaker

AREAS OF EXPERTISE: Worldwide Cybercrime Protection and Prevention/Identity Theft/ Privacy, Data Collection and Security / Workplace Risk Management and Security/ Consumer Protection, Advertising and the Internet / E-Commerce/ Cyberstalking and Harassment/ Child Exploitation and Child Pornography, Children Online, Online Marketing, Cyber-workplace issues, Privacy training and coaching

---

CURRENT POSITIONS      President/CEO - Aftab Cyber-Consulting  
 Executive Director, WiredSafety.org (a 501c-3 corporation)  
 The Privacy Lawyer columnist for Information Week

---

EDUCATION                      City University of New York      B.A., 1981  
 Hunter College                      Valedictorian  
 (Completed 4 yr degree in 2 yrs) *Phi Beta Kappa* (Nu Chapter)

New York University                      J.D., 1984  
 School of Law

SELECT HONORS                      Community Leadership Award, 2005  
    *Awarded by Child Abuse Prevention Services*

American Society of Business Publication Editors Award "Gold" *Original Web Commentary*  
*Informationweek.com for Parry Aftab's*  
*"Patriotism, Compliance and Confidentiality" article*

Activist of the Year Award, 2002  
    *Awarded by Media Ecology Association*

Internet Pioneer of the Year, 2001  
    *Awarded by Family PC Magazine*

Home Office, U.K.  
    *Child Protection, Criminal Laws and Law Enforcement Task Forces*

ORGANIZATIONS                      TRUSTe  
    *Member- Board of Directors (Elected December 2002)*

Ad Council  
    *Advisory Committee member (1999 - 2003)*

Children's Television Workshop Online (Sesame Workshop)  
    *Advisory Board (appointed 1998)*

UNESCO  
    *President, U.S. National Action Committee, Innocence in Danger (appointed 1999)*

**Appendix 3: From Parry's Upcoming Book, Internet Safety 1-2-3:**

**Internet Safety 1-2-3: The Quick Guide**

While you can take the time to do your own inventory on risks, not everyone will. This will give you a quick guide on the risks that most children and teens face at certain ages. Read the description of their activities, not just the age ranges. How they are using the technologies and which they are using are more important than their age in determining the risks they face. This can be very helpful when you want to know where to start. Reviewing these will help you know what to look for, especially when you want some quick help. Remember the 3Cs and look for "content" issues, "commercial" issues and "contact" issues. In the early years, though, no matter how you feel about commercialism, most of the quality and fun content and online activities come from the big entertainment companies and trusted family brands, such as Disney, Children's Television Workshop, Nickelodeon and Scholastic.

**Under 8 years of age:**

The children are lap-surfing and just beginning to use the Internet. Some are pre-readers, and others are new writers and slower readers. That means they can easily make a mistake when typing in their favorite website name or searching for their favorite topics in a search engine. Most are not using interactive communication technologies (e-mail, instant messaging, etc.) without parental screening and supervision. They may or may not be allowed to access the Web without their parents standing over their shoulder. These children play lots of games, online and offline, but most of the ones they play are not interactive (meaning, they don't usually involve them playing against other people). They spend most of their time on favorite sites that usually involve their favorite offline and television characters and brands, such as Disney, Children's Television Workshop, Nickelodeon and Cartoon Network.

Children under eight years of age are very concerned about doing something to break the computer (downloading viruses and spyware applications). It's a good age to get them started with secure surfing and using an anti-virus program if downloading anything or accepting any attachments. It's also a good time to get them to start using spyware and pop-up blockers (perhaps by using a customized toolbar, such as Google's or Yahoo's). They are not yet involved with stranger communication or the risks of meeting people offline.

They need to learn good netiquette and how to respect others online. (I have written an entire chapter on this called "Ms. Parry's Guide to Netiquette." Pay special attention to this chapter.) They also need to learn how to find new sites without risking full-sized search engines. Being able to communicate with large numbers of friends and have them be able to reach you are less of a problem at this age. The most restrictive parental control technologies work well here. They don't need millions of websites to do their homework at this age. It's less about opening up their access and more about limiting it.

Some children of this age are using mobile phones and handheld gaming devices with networking capability, but most aren't. Prepaid calling cards for their mobile phones are a good decision, to keep them from running up high phone bills. Text-messaging shouldn't be permitted at this age. And the most restrictive settings for all networked handheld technologies is your best bet, if you buy them at all.

And if you are allowing them to play video games, check the ratings and choose one that is appropriate in violence, language and sexual content for your child. Check and make sure that they can't install new video games on their mobile phones without your approval. Keep them from using any interactive game devices, such as X-Box Live or Sony PlayStation Network, or other voice chat games or devices.

Less is more when you are dealing with children of this age. They still believe that their parents are in charge, know everything and are there to protect them. (It's a magical age...Enjoy it, it won't last! ©) Also, are you using babysitters? Remember what I suggested about password protection and turning off the Internet when you are not home.

- Use filtering or parental control technologies. Block everything that isn't pre-approved, rather than just filtering out the "bad" sites.
- Think about whether they really need e-mail or IM, and if you determine they do, block all

communications from anyone other than pre-approved senders.

- Make sure that the buddy list is no longer than the age of the child, and that you know (in real life) everyone on it.
- Bookmark their favorite websites so they won't mistype them and end up at a "bad" site.
- Use kid-sized search engines: Yahoo!igans and Ask Jeeves for Kids.
- Limit their online time to no more than ½ hour a day, unless they have a special project for school.
- Check with their teachers and librarians for suggested websites and for recommendations for good resources online.
- Don't let them use interactive games, such as X-Box Live or Sony PlayStation Network yet. You should use our safe gaming award winning Disney's Toontown.com instead.
- Sit down with them as often as possible and find out where they go online, what they like and ask or answer any questions they may have.
- Don't allow them to set up websites, profiles, blogs or away messages or use other public posts without your direct supervision.
- Control their passwords.
- Look for safe site lists you can trust. Check out WiredKids.org approved safe sites list and the other safe sites listed in my "Green Light" section.

#### **From 8 to 10 years of age:**

They are beginning to use instant messaging, e-mail and other interactive communication tools. They are also surfing more and spending more time online. They need to learn more about what information they can and can't share with others online, how to choose their passwords and with whom they can be shared. (Parents tend to worry most at this age, as their children do from surfing to communication tools.)

They may be engaged in interactive gaming (playing against strangers, sometimes with voice chat), spending more time playing video games (including more violent and adult-themed games) and be more likely to use adult-sized search engines to find the sites they are looking for. Because of their visiting gaming related websites, like code and cheat sites (to improve their game play), they are prime targets for spyware. And as they learn to flex their cyber-muscles, they are often cyberbullied or cyberbullying others and frequently hacking into, and sending malicious codes to, each other.

Fortunately, they are still too young to be engaged in face-to-face meetings with adults offline, and generally not looking for sexually-explicit content online. They are more interested in finding gory and shocking websites, where baby seals are being clubbed to death.

They often begin to use lewd and inappropriate language at this age too, even if they would never dream of doing this offline. Boys and girls are very different in how they use the technology at this age, as well. Boys tend to be less involved with interactive communications, even with their friends, and girls tend to surf less, spending more of their time chatting or IMing their offline friends. The people they talk with online are still the ones they know in real life. And more have mobile phones, but still need to have prepaid calling plans and restrictions on who can call them and who they can call.

Children begin to register at websites and fill out online forms at this age. Parents need to talk with them about what they can and can't do and which sites to trust. And their homework may require more websites than they can get with the most restrictive parental control settings or with some of the child-sized search engines.

Most of the children in this age group aren't downloading music or other copyrighted media online yet, unless they have older siblings. And they are still willing to tell their parents what they are doing online and when things go wrong online. Parents are still the "good guys" and are an important influence on their online activities. This may be your last chance to have an affect on their online activities. Don't waste it.

- Raise the bar on filtering or parental control technologies if you find they are complaining or are locked out of school-recommended sites. Or make sure that you use a product that will send you an e-mail at work to let you unblock a particular site. (MSN has this feature.)
- If you add IM or e-mail, make sure only pre-approved senders can send your child an IM or e-mail. Consider using a free web-based service with parental controls and spam blockers. That way, whatever they access online won't pollute their real e-mail address, or yours.
- Use a pop-up blocker or toolbar (like Google's or Yahoo's), an antivirus program and a spyware

blocker and remover (this begins the age of dangerous downloads).

- Keep using the Yahoo!igans! and Ask Jeeves for Kids search engines.
- Make sure that they understand what information can and can't be shared online with anyone.
- Practice chatting online with them so they know how to handle strangers they encounter online.
- Make sure that they know not to cyberbully someone or say or do anything online that they wouldn't do offline.
- Make sure they know how to use the "notify" or "warning" buttons, or consider using a monitoring software to be able to review what they are saying and doing.
- Watch for hacking, password and identity theft at this age. This is when they start stealing each others' passwords and locking them out of their own accounts.
- Also watch for their corrupting your files on your computer with spyware, etc. Back everything up!
- Limit online time (aside from special school projects) to under an hour a day (including all IM and text-messaging time).

**Between 10 and 12 years of age:**

Cyberbullying is very common at this age. So are filling out forms, signing up for newsletters and registering for contests and giveaways online. More of the children at this age have mobile phones, which should still have a prepaid calling plan and restrictions on who can call them and who they can call. Many have text-messaging on their mobile phones, and if you don't use a prepaid plan, you may find yourself with very high mobile phone bills for their text-messaging use alone.

Some preteens are setting up profiles on social networking websites at this age, usually hiding them from their parents. They are more interested in communicating with their friends from school on these sites, and self-expression and being creative by creating "pink, pink, pink" profiles (how one of my Teenangels described her site). They are still usually chatting and IMing only people they know offline.

But some are starting to feel more confident and are willing to respond to a stranger's message or to engage in communications with a friend of a friend. (A sexual predator will often befriend one preteen to get to their friends.) And some of the younger Internet sexual predator victims engage in meeting strangers offline at this age. They usually think they are meeting a cute fourteen-year-old, but know it's someone they don't know in real life. A much higher portion of victims at this age are female than male.

Some of the boys may begin to seek out sexually-explicit content online. Many of the boys and girls are using lewd language and pretending to be more sophisticated than they are. "Cybersex" or ask the kids call it "cybering" usually begins at this age too. It is when they type sexual things online with someone else (similar to having "phone sex"). Sometimes they don't appreciate the seriousness of what they are doing, but do it anyway. Sharing their personal information and communicating with strangers are the most important issues they face at this age. Keeping them grounded at this age will payoff in the future. They are already starting to keep online secrets from their parents and don't share their passwords as readily. Some try and avoid their parents' supervision and use chat lingo to avoid their parents understanding their communication. They pretend a great deal at this age. Pretending to be older, more popular, richer, a better athlete, etc. is commonplace. They are experimenting all the time.

As they are starting to grow up, they may be entitled to more privacy (when discussing young crushes and other private information). But balancing their privacy with supervision is something parents need to learn to do. They may want more privacy and freedom than they should have at this age. You'll have to decide that for yourself, based on your preteen. The more balanced their activities are (offline friends, sports, after school activities and hobbies) the safer they usually are online. But, trust needs to be earned on both sides.

School assignments may require more access to websites than the younger parental control settings would allow. And the more restrictive kid-sized search engines may not give them access to the sites they need, either. And, when they are upset and online, they are more likely to act out. So teaching them to Take5! and ThinkB4UClick are important lessons at this age. (You can learn more in the "Ms. Parry's Guide to Netiquette" chapter and the chapter on cyberbullying.)

They may start using peer-to-peer software to illegally download music at this age. Keep an eye out for their use of file-sharing software (like Kazaa or Limewire), since there is no good reason a child of this age should be using it at all. Consider buying them a music service subscription service, like Yahoo's or

Napster's, or giving them an account at iTunes.

- Raise the bar on parental controls and filtering programs to allow them to access websites they need for school, or use a parental control software that allows you to unblock sites from a remote location, by e-mail override.
- Start using full-sized search engines with filters applied (check their advanced settings) or use a toolbar (Google's comes preset with a medium filter).
- Cyberbullying is a serious problem at this age, watch for the signs...
- Teach them about personal information and predators. Without going into details, they are concerned about people showing up at their house. Make sure they remember this when online or on text-messaging devices.
- Watch for "away messages" for their IM programs. Kids often post their cell phone numbers there.
- Websites and profiles they build should be reviewed carefully, as should screen names.
- Make sure that you control the family account password and have their passwords too. Expect some push-back.
- Give them privacy as long as it is with people you trust.
- Block all but pre-approved senders. (Expect push-back here too.)
- Make sure they can't share pictures online, or set up profiles, blogs or webcams without your okay.
- Interactive games should still be limited to Toontown.com and other kid-approved sites. They are still too young for X-Box Live, without direct parental supervision or parental controls. (X-Box won one of our safe gaming awards for its parental controls.)
- Watch early media piracy, teach them not to steal online or offline.
- Google their name, screen names, address, and telephone numbers at least once a week and create alerts to warn you of any new postings. Many kids post nasty things about others at this age. (Read about how to Google someone in Step Three, Implementing and Enforcing Your Choices.)
- Change their passwords often and make sure that they aren't using a provocative screen name.
- Search regularly on your computer for images (of porn or of your kids), and any music, movie or media files you don't know about.
- Spyware is a serious problem at this age, since they often access game sites riddled with spyware and malicious code.
- Lock your private files with a password they don't know.
- Get them started in online safety education, check out [wiredkids.org](http://wiredkids.org) or [internetsuperheroes.org](http://internetsuperheroes.org). Check out starting a tweenangel chapter at your local school. (For more information visit [teenangels.org](http://teenangels.org).)
- Watch cell phone gaming, porn and spending capabilities, and think about limiting their cell phone usage in a way that shuts it down when they exceed it, instead of just charging you extra. (Check into filtering products for cell phone Internet access.)

**Between 13 and 15 years of age:**

The risk of Internet sexual predators and Internet sexual exploitation is highest at this age. They have the freedom to meet the Internet "friends" in the mall or in other public places and their being away from home (at the movies, etc.) isn't questioned as it would have been a few years ago. Their hormones are raging, and they are more sexually inquisitive at this age too. Our studies have shown that a surprisingly high percentage of girls at this age admit to engaging in cybersex (having graphic sexual communications online, typically with strangers they encounter.) In one of our studies 60% of the girls we polled between 13 and 16 years of age admitted to engaging in cybersex.

It gets tricky, as they need more privacy at this age than ever before, yet also need more supervision and guidance. Respect their privacy more and talk with them about their online experiences. If you use monitoring software, use it for emergencies - never accessing the reports until something goes wrong and you need to. Consider them the security video camera in the corner of the bank. No one reviews the tapes until there is a bank robbery. And then they are invaluable.

Their mobile devices are their lifeline at this point in their young lives. Text-messaging is crucial to their social life and if they are offline for a few hours, everything falls apart. © Maintaining balance is harder too. And no one website or collection of websites holds their loyalty. In fact, they surf much less than ever before, spending their online time posting on social networking profiles, building their own websites, setting up webcams and instant and text-messaging their friends. Perhaps social networking websites and

blog sites are more of a risk for teens in this age range than for anyone else. And, since they have a huge influence on money spent offline and have lots of their own money to spend (from holiday gifts, babysitting and other jobs), they are targeted by marketing schemes and ads of all kinds. Unfortunately, everything they had practiced until now on safe and secure technology use is often thrown out the window in their quest for new thrills and to be treated like young adults. They will sometimes at this age engage in sexual discussions and intentionally meet adults offline for sexual purposes. At least one study reflected that 1 in 4 girls and 1 in 7 boys in this age range were meeting strangers offline.

They are also listening, accessing and downloading music online and sometimes accessing movies and software through peer-to-peer websites, illegally. (Although most of the movie, software and gaming piracy occurs when they are in university, not middle or high school.)

Online gambling, eating disorders, bomb-building and other more dangerous websites hold their greatest appeal to kids in this age group. They experiment often and push the envelope, challenging your rules. Even if you remain consistent in your rules and use of parental control technologies, they are more likely to use handheld devices and their friend's Internet access to circumvent them.

Cyberbullying becomes cyber-sexual-harassment and more mean-spirited. Hacking, malicious code attacks and cyber-stalking become more common place when their tech skills improve and their access to higher powered technologies increase. Posing and password theft is a serious problem too. Sadly, the typical culprit is a close friend or former friend.

They are buying things online at this point, often bidding for things they collect on eBay and other auction websites. They may have their own e-commerce accounts and credit cards they are using online. That means that ID theft and financial credential theft are more prevalent at this age too. And scammers and con artists often target young teens, knowing that they may be less careful than they should be and may be conned into giving away your banking information.

- Filter sites that are inappropriate for young teens, instead of blocking all but approved sites. Some bad ones will get through, though. So talk about it beforehand.
- Give them more leeway on people they can accept IMs or e-mails from. But check and account for everyone, in real life, on their buddy list. No friends of friends.
- Make sure you filter or block image searches (a way around many filters).
- Block peer-to-peer technologies and get your kids an account with iTunes or another legal music download site, or even better, one of the new subscription services, like Yahoo!
- Teach them to guard their passwords. Password theft is a serious problem at this age.
- Teach them not to pirate or illegally download or share software, games, music or motion pictures.
- Have them Google themselves often, screen names, telephone and cell numbers, addresses, full names, nicknames, etc. (all in quotation marks to search the whole phrase).
- Try and limit their use of chatrooms to monitored chatrooms or themed chatrooms on safe topics.
- Limit their online use (including text-messaging) to under 1-1/2 hours a day (aside from a special school project).
- Keep them out of social network or online dating sites (like xanga.com, friendster.com or match.com).
- Talk to them about not meeting strangers offline, and agree to go with them or teach them large group safe meeting tips (see "Step 3- Implementing and Enforcing Your Choices")
- Get girls (and boys) a copy of Katie Tarbox's book "A Girl's Life Online" (formerly known as "Katie.com") to read. (Katie founded Katiesplace.org, a website for young victims of Internet sexual exploitation and their families and friends.)
- Try to keep the computer in a central location, if it has Internet access, and watch new interactive devices, like cell phones, text messaging devices and interactive gaming devices, like X-Box Live. Use parental controls if they come with them. (X-Box Live got an award from us for their safety devices and parental controls.) But note that even with parental controls, these games are risky for young teens when they chat with strangers.
- Consider setting up a teenangels.org chapter, or starting an online safety club at their school. (Visit Marvel comic-themed Internetsuperheroes.org for available free materials.)
- Pick your battles! Not all risks are created equal online. Let things like their use of inappropriate and even sometimes lewd language go, understanding it's how kids talk online, and focus on their sharing too much personal information or meeting strangers.



- Talk to them about protecting their friends' privacy too.

**For 16 years of age and over:**

All bets are off. If they have earned your trust, give it to them. If not, unplug the computer and take away their cell phones and interactive gaming devices. And pray often and hard. ☹ If you haven't taught them what they need to know by now, we're all in trouble.

- Focus on teaching them to be responsible cybercitizens and to use the filter between their ears.
- Emphasize the risks of sharing personal information and meeting strangers offline.
- Make sure they Google themselves often and report what they find. Have them set an alert on themselves as well.
- Teach them to use anti-virus programs, not believe everything they read online and to respect others. Check for adware or spyware often, use a firewall and teach them to come to you if anything goes wrong online. (Maybe they will.)
- And get their help in keeping their younger brothers and sisters safe online.
- Remind them that you're still around if they need your help.
- Pick your battles! Not all risks are created equal online. Let things like their use of inappropriate and even sometimes lewd language go, understanding it's how kids talk online, and focus on their sharing too much personal information or meeting strangers.

**Appendix 4: Parenting Online - WiredSafety.org's booklet for parents - printable online**



## Parenting Online

What do we do when our eight-year-old knows more than we do about cyberspace? How do we guide our children safely through this new world? How do we set the rules when we don't even understand the risks? The childproof locks, seatbelts and helmets we use to help keep them safe in everyday life won't protect them in cyberspace. There we need new and different gadgets and safety tips.

Welcome to the new world of parenting online! It's your newest challenge. But don't worry...it's not as hard as you think and it's well worth the effort.

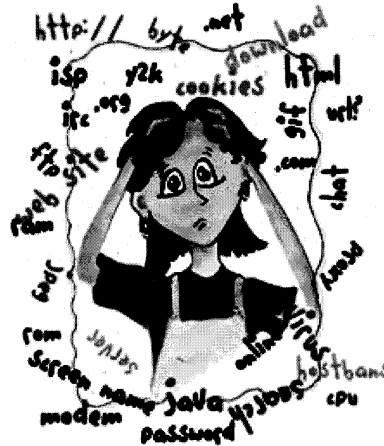
Parenthood is never easy and the ground rules are always changing. We go from playing the role of confidante, to co-conspirator, to police chief, to teacher, to playmate and back...all in the same day. We barely have the chance to catch our breath!

The things we do to make sure our children stay safe are constantly changing too. When they crawl, we learn how to keep things off the floor. Then, they pull themselves upright, we have to keep them safe from the new dangers at eye level. Training wheels have to be removed, and we have to watch while they pedal away (generally into the nearest tree). We watch their sugar intake, make sure they take their vitamins and keep small items out of their mouths.

That's our job, as parents. So the tried and true warnings, passed down from generation to generation, are repeated... "don't talk to strangers..." "come straight home from school..." "don't provoke fights..." "don't tell anyone personal information about yourself..." and "we need to meet your friends..." This is familiar territory after all. We know the dangers our kids face in the street or at the mall or in the school yard, because we faced them.

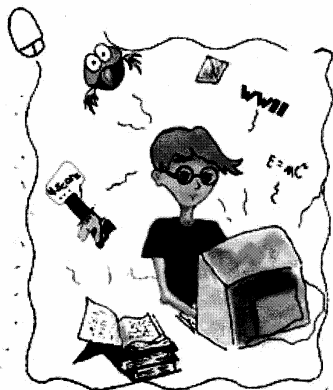
As in any large community, there are dangers our children encounter in cyberspace, too. But, since our children know more than we do about cyberspace, we worry about how we can teach them to avoid those dangers. Don't panic... those dangers can be managed using the same old warnings we've always used.

We just need to translate them into cyberspace terms...



### And there are wonders around every cyber-corner too...

The Internet is the largest collection of information in the world, always available without a charge and delivered to your home computer. Every question you might have can be answered online. When your child asks you how deep the ocean is or why the sky is blue, you can "ask the Internet," together.



You and your children can communicate with others too, worldwide and in every language, with the click of your mouse. Their artwork can be displayed, their news reporting published and their poems posted on the largest "refrigerator door" in the universe, where 700 million people can appreciate them.

You can research your family tree and build a family Web site. And, best of all...the most complicated homework assignment can be researched online (even last-minute on the Sunday night before it's due).

You can search online for just about anything and any information you want. The easiest way to do that is by using search engines. You can type your search into one of the search engines and often will find what you are seeking. Just as often, though, you will find sites that are trying to get your or your children's attention. Pornographers are the most frequent abusers of search engines, registering and coding their sites to trick people into visiting them, thinking they are Disney, Pokemon or even the White House.

Most of the search engines now have filtering options. By selecting one of these options, most inappropriate content is filtered out and the search results are typically kid-friendly. Two commercial search engines were

designed just for kids, though, and are wonderful places to begin your child's search online. Yahoo!igans!, Yahoo! kid-sized search engine hand-selects the sites, making sure nothing slips through. It is best for younger children, ten and under. Ask Jeeves for Kids is Ask Jeeves kid-sized search engine. Although not as scrubbed clean as Yahoo!igans! hand-selected sites, it contains many more sites which make it perfect for slightly older children. I recommend it for children ten and older.

In addition, most full-size search engines have a filtered option you can select. But remember that even if you use a search engine filter, if the kids search for images, they can find things you wish they hadn't. That's when using a filtering product that can block images too might come in handy.

In addition to kid-sized search engines, there are many wonderful family-friendly site lists. WiredKids has one of its own, where the sites are selected and reviewed by our specially-trained volunteers. You can even recommend your favorite sites to be added.

There are some entertaining sites that teach children online safety, as well. Although we prefer our WiredKids.org, StopCyberbullying.org and InternetSuperHeroes.org the best, (she says modestly...) another very special one we want to point out. Disney's Surfswellisland.com teaches online safety Disney-style. Mickey Mouse, Donald Duck, Minnie Mouse and Goofy all find themselves involved in tropical island cyber-challenges relating to viruses, privacy, netiquette (cyber-etiquette) and responsible surfing. Lesson plans, online safety worksheets and other wonderful resources are all available without charge at the site.

Looking for homework help? Check out Discovery.com, Nationalgeographic.org, PBSkids.org and The National Gallery of Art kids page [www.nga.gov/kids/kids.htm](http://www.nga.gov/kids/kids.htm). And ask your school librarian or the librarian at your public library for sites they recommend. Librarians and library media specialists are the guides to valuable and safe online resources for children. And if you need something you can't find, send me an email at "Ask Parry," ([askparry@wiredsafety.org](mailto:askparry@wiredsafety.org)) my Internet-syndicated online safety column. Drop by WiredKids.org or WiredSafety.org to find out how to submit a question.

## CyberSense ...translating common sense for cyberspace

- **Don't talk to or accept anything from strangers.** That's the first one we learn while growing up, and the first one we teach our children. The problem in cyberspace though is teaching "stranger danger." Online, it's hard to spot the strangers.

The people they chat with enter your home using your computer. Our kids feel safe with us seated nearby. Their "stranger" alerts aren't functioning in this setting. Unless they know them in real life, the person is a stranger no matter how long they have chatted online. Period. You need to remind them that these people are strangers, and that all of the standard stranger rules apply.

You also must teach them that anyone can masquerade as anyone else online. The "12-year-old" girl they have been talking to may prove to be forty-five year old man. It's easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace.

- **Come straight home after school.** Parents over the generations have always known that children can get into trouble when they wander around after school. Wandering aimlessly online isn't any different. Parents need to know their children are safe, and doing something productive, like homework. Allowing your children to spend unlimited time online, surfing aimlessly, is asking for trouble.

Make sure there's a reason they're online. If they are just surfing randomly, set a time limit. You want them to come home after they're done, to human interaction and family activities (and homework).

- **Don't provoke fights.** Trying to provoke someone in cyberspace is called "flaming." It often violates the "terms of service" of your online service provider and will certainly get a reaction from other people online.

Flaming matches can be heated, long and extended battles, moving from a chat room or discussion group to e-mail quickly. If your child feels that someone is flaming them, they should tell you and the sysop (system operator, pronounced sis-op) or moderator in charge right away and get offline or surf another area. They shouldn't try to defend themselves or get involved in retaliation. It's a battle they can never win.

- **Don't take candy from strangers.** While we don't take candy from people online, we do often accept attachments. And just like the offline candy that might be laced with drugs or poisons, a seemingly innocent attachment can destroy your computer files, pose as you and destroy your friends or spy on you without you even knowing it. Use a good anti-virus, update it often and try one of the new spyware blockers. You can get a list of the ones we recommend at [WiredSafety.org](http://WiredSafety.org). Practice safe computing!
- **Don't tell people personal things about yourself.** You never really know who you're talking to online. And even if you think you know who you are talking to, there could be strangers lurking and reading your posts without letting you know that they are there. Don't let your children put personal information on profiles. It's like writing your personal diary on a billboard.

With children especially, sharing personal information puts them at risk. Make sure your children understand what you consider personal information, and agree to keep it confidential online and everywhere else. Also teach them not to give away information at Web sites, in order to register or enter a contest, unless they ask your permission first. And, before you give your permission, make sure you have read the web site's privacy policy, and that they have agreed to treat your personal information, and your child's, responsibly.

- **We need to get to know your friends.** Get to know their online friends, just as you would get to know their friends in everyday life. Talk to your children about where they go online, and who they talk to.
- **R-E-S-P-E-C-T.** We all know the golden rule. We have a special one for cyberspace. Don't do anything online you wouldn't do offline. If you teach your child to respect others online and to follow the rules of netiquette they are less likely to be cyberbullied, become involved in online harassment or be hacked online. You can learn more about the ways to combat cyberbullying at our new website, [StopCyberbullying.org](http://StopCyberbullying.org) or at [WiredSafety.org](http://WiredSafety.org)'s cyberstalking and harassment section. Remember that it is just as likely that your child is a



cyberbully (sometimes by accident) as a victim of one. Let them know they can trust you not to make matters worse. You have to be the one they come to when bad things happen. Be worthy of that trust.

Remember that the new handheld and interactive gaming devices you buy have real risks to. Your children can send and receive text-messages from anyone on their cell phones or text-messaging devices and interactive games allow them to chat, on Internet phone, to anyone who wants to talk with them. The new Bluetooth devices let your child receive messages from anyone in a 300 foot range, and could be a problem if they play the new Bluetooth handheld games in a mall. Think about the features you are buying when you buy new devices for your children. Check into privacy and security settings. Our Teenangels ([teenangels.org](http://teenangels.org)) are working on new guides for parents and other teens on what to look for and think about before you buy a new interactive device. Look for them at your local retailer or on the [WiredSafety.org](http://WiredSafety.org) and [Teenangels.org](http://Teenangels.org) websites.

Don't just set up the computer in the corner of their bedroom, and leave them to surf alone. Take a look at their computer monitor every once in awhile, it keeps them honest. Sit at their side while they compute when you can. It will help you set rules that make sense for your child. It also gives you an unexpected benefit...you'll get a personal computing lesson from the most affordable computer expert you know!

And it's worth the effort. When our children surf the Internet, they are learning skills that they will need for their future. They become explorers in cyberspace, where they explore ideas and discover new information.

Also, because there is no race, gender or disability online, the Internet is the one place where our children can be judged by the quality of their ideas, rather than their physical attributes.

## What Tech Tools Are Out There?

### Blocking, filtering and monitoring...when you need a little help

There are many tools available to help parents control and monitor where their children surf online. Some even help regulate how much time a child spends playing computer games, or prevent their accessing the Internet during certain preset times.

I've listed the type of protections that are available. But, most of the popular brands now offer all of these features, so you don't have to choose. Recently, given parents' concerns about strangers communicating with their children online, monitoring software has gained in popularity. Although it might have its place in protecting a troubled child, it feels more like "spyware" than child protection. But it's ultimately your choice as a parent. The newest trend is to use products supplied by your ISP called parental controls. AOL's parental controls were the first of these to be developed and used. MSN 8.0 launched the first set of parental controls for MSN. To read more about the various products and services we have reviewed, visit [WiredKids.org](http://WiredKids.org) and [WiredSafety.org](http://WiredSafety.org).

#### Blocking Software

Blocking software is software that uses a "bad site" list. It blocks access to sites on that list. They may also have a "good site" list, which prevents your child from accessing any site not on that list. Some of the software companies allow you to customize the lists, by adding or removing sites from the lists. I recommend you only consider software that allows you to customize the list, and lets you know which sites are on the lists.

#### Filtering

Filtering software uses certain keywords to block sites or sections of sites on-the-fly. Since there is no way any product can keep up with all the sites online, this can help block all the sites which haven't yet been reviewed. The software blocks sites containing these keywords, alone or in context with other keywords.

Some companies allow you to select certain types of sites to block, such as those relating to sex, drugs or hate. This feature engages special lists of keywords that match that category. As with the "bad site" lists, the lists of keywords used by the filtering software should be customizable by the parent, and every parent should be able to see which terms are filtered.

#### Outgoing Filtering

No...this doesn't mean your software had a sparkling personality :-)) (that's cyberspace talk for "grin" and means you're supposed to smile at my brilliant humor, and if you want to learn more about this stuff...you need to read my Ms. Parry's Guide to Correct Online Behavior). It means that your child won't be able to share certain personal information with others online. Information such as your child's name, address or telephone number can be programmed into the software, and every time they try to send it to someone online, it merely shows up as "XXXs." Even with kids who know and follow your rules, this is a terrific feature, since sometimes, even the most well-intentioned kids forget the rules.

#### Monitoring and Tracking

Some software allows parents to track where their children go online, how much time they spend online, how much time they spend on the computer (such as when they are playing games) and even allows parents to control what times of day their children can use the computer. This is particularly helpful when both parents are working outside of the home, or with working single-parents, who want to make sure their children aren't spending all of their time on the computer. Many parents who don't like the thought of filtering or blocking, especially with older children and teens, find monitoring and tracking satisfy their safety concerns. They can know, for sure, whether their children are following their rules.

We particularly recommend using a monitoring software and then forgetting it's installed. Think of it as the security video camera in the corner of the bank. No one views the tapes until the bank is robbed. If something bad happens, you can play back the monitoring log and see exactly what occurred, and who said what, and in dire situations, where your child went to meet an adult offline. We particularly like Spectorsoft.com, because their products can monitor all instant messaging platforms, which is key to keeping your children safe online.

Parents have to remember, though, that these tools are not cyber-babysitters. They are just another safety tool, like a seat belt or child safety caps. They are not a substitute for good parenting. You have to teach your children to be aware and careful in cyberspace. Even if you use every technology protection available, unless your children know what to expect and how to react when they run into something undesirable online, they are at risk. Arming them well means teaching them well.

### **Your Online Safety “Cheatsheet”**

Some Basic Rules for You to Remember as a Parent . . .

- Make sure your child doesn't spend all of her time on the computer. People, not computers, should be their best friends and companions.
- Keep the computer in a family room, kitchen or living room, not in your child's bedroom. Remember that this tip isn't very helpful when your children have handheld and mobile Internet and text-messaging devices. You can't make them keep their cell phones in a central location. So make sure that the “filter between their ears” is working at all times.
- Learn enough about computers so you can enjoy them together with your kids.
- Teach them never to meet an online friend offline unless you are with them.
- Watch your children when they're online and see where they go.
- Make sure that your children feel comfortable coming to you with questions and don't over react if things go wrong.
- Keep kids out of chat rooms or IRC unless they are monitored.
- Encourage discussions between you and your child about what they enjoy online.
- Discuss these rules, get your children to agree to adhere to them, and post them near the computer as a reminder.
- Find out what e-mail and instant messaging accounts they have and (while agreeing not to spy on them) ask them for their passwords for those accounts.
- “Google” your children (and yourself) often and set alerts for your child's contact information. The alerts will e-mail you when any of the searched terms are spotted online. It's an early warning system for cyberbullying posts, and can help you spot ways in which your child's personal information may be exposed to strangers online. To learn how to “Google” them, visit [InternetSuperHeroes.org](http://InternetSuperHeroes.org).
- Teach them what information they can share with others online and what they can't (like telephone numbers, address, their full name, cell numbers and school).
- Check your children's profiles, blogs and any social-networking posts. Social-networking websites include [myspace.com](http://myspace.com), [facebook.com](http://facebook.com) and [xanga.com](http://xanga.com). (We work closely with MySpace and Facebook to help keep their users safer.) Social networks, generally, shouldn't be used by preteens and should be only carefully used by teens. [Yfly.com](http://Yfly.com) is a new teen-only social network that is designed from top to bottom to keep teens safer and teach them about more responsible behaviors.
- For those of you with preteens and young teens, read the Safer Social Networking guide at [WiredSafety.org](http://WiredSafety.org).
- Get to know their “online friends” just as you get to know all of their other friends.
- Warn them that people may not be what they seem to be and that people they chat with are not their friends, they are just people they chat with.
- If they insist on meeting their online friend in real life, consider going with them. When they think they have found their soul mate, it is unlikely that your telling them “no” will make a difference. Offering to go with them keeps them safe.
- Look into the new safer cell phones and cell phone features that give you greater control over what your children can access from their phone and how can contact them.

## PARENTING ONLINE

### MY AGREEMENT ABOUT USING THE INTERNET



Once you understand enough about cyberspace and how your children surf the Internet, you can set your own rules. These are the basic rules, even though you may want to add some of your own.

Some kids like setting the rules out clearly in an agreement. Here's one you can use, and post near your computer to help them remember how to surf safely. (Note that while the tips may work for teens, the contract is designed for preteens and younger.)

I want to use our computer and the Internet. I know that there are certain rules about what I should do online. I agree to follow these rules and my parents agree to help me follow these rules:

1. I will not give my name, address, telephone number, school, or my parents' names, address, or telephone number, to anyone I meet online.
2. I understand that some people online pretend to be someone else. Sometimes they pretend to be kids, when they're really grown ups. I will tell my parents about people I meet online. I will also tell my parents before I answer any e-mails I get from or send e-mails to new people I meet online.
3. I will not buy or order anything online without asking my parents or give out any credit card information.
4. I will not fill out any form online that asks me for any information about myself or my family without asking my parents first.
5. I will not get into arguments or fights online. If someone tries to start an argument or fight with me, I won't answer him or her and will tell my parents.
6. If I see something I do not like or that I know my parents don't want me to see, I will click on the "back" button or log off.
7. If I see people doing things or saying things to other kids online I know they're not supposed to do or say, I'll tell my parents.
8. I won't keep online secrets from my parents.
9. If someone sends me any pictures or any e-mails using bad language, I will tell my parents.
10. If someone asks me to do something I am not supposed to do, I will tell my parents.
11. I will not call anyone I met online, in person, unless my parents say it's okay.
12. I will never meet in person anyone I met online, unless my parents say it's okay.
13. I will never send anything to anyone I met online, unless my parents say it's okay.
14. If anyone I met online sends me anything, I will tell my parents.
15. I will not use something I found online and pretend it's mine.
16. I won't say bad things about people online, and I will practice good netiquette.
17. I won't use bad language online.
18. I know that my parents want to make sure I'm safe online, and I will listen to them when they ask me not to do something.
19. I will help teach my parents more about computers and the Internet.
20. I will practice safe computing, and check for viruses whenever I borrow a disk from someone or download something from the Internet.
21. I won't post my cell number on my away message, and will check with someone before posting something personal about me on my blog or on a networking site.
22. I will Stop, Block and Tell! If I am harassed online or cyberbullied.
23. I will Take 5! before reacting to something that upsets me or makes me angry online.
24. I will practice responsible "think4Uclick" rules. (I know I can find out more about these things at [InterentSuperHeroes.org](http://InterentSuperHeroes.org) and [StopCyberbullying.org](http://StopCyberbullying.org).)
25. I will learn how to be a good cybercitizen and control the technology, instead of being controlled by it.

\_\_\_\_\_  
I promise to follow these rules. (signed by the child)

\_\_\_\_\_  
I promise to help my child follow these rules and not to over react if my child tells me about bad things in cyberspace (signed by parent).



**From Parry:**

I am asked questions about kids online safety at least a hundred times a day. Is the Internet a dangerous place? Are there predators out there looking to set up a meeting with my child? How can we find good and reliable content online? How can I supervise my child's surfing when I can't even turn on the computer?

These any other question like these fill my inbox daily. (If you have a question of your own, visit [WiredKids.org](http://WiredKids.org) or [WiredSafety.org](http://WiredSafety.org) and click on "Ask Parry." Here is the one simple answer:

The single greatest risk our children face in connection with the Internet is being denied access. We have solutions for every other risk.

That bears repeating, over and over, especially when we hear about Internet sexual predators, hate, sex and violence online. But our children need the Internet for their education, careers and their future.

Happily, most of the risks are easily confined. In each and every case when children encounter Internet sexual predators offline, they go willing to the meeting. They may think the person is a cute fourteen year old girl or boy, but they know they are meeting someone they don't know in real life. That means we can prevent 100% of these crimes. Merely teach our children not to

meet Internet strangers offline. If they are set on meeting that person anyway, go with them. That way, if the person turns out to be a cute fourteen year old, you are the hero. And if they aren't, you're an even *bigger* hero.

Our [WiredKids](http://WiredKids.org), [WiredTeens](http://WiredTeens.org) and [Teenangels](http://Teenangels.org) programs, in addition to being fun and educational sites, are also volunteer programs where children and teens are taught online safety and privacy and responsible surfing. They then use these skills to help other children and teens learn to surf safely, as well. Talk to your children about what they do online (and offline also), and let them know you are there to help if things go wrong. You will note that in our safe surfing agreement parents have to promise only one thing...not to overreact if their children come to them for help. Earn their trust, and be worthy of it. Register your children at [WiredKids.org](http://WiredKids.org), our children's online safety site, and we will make sure they learn what they need to know about enjoying the Internet safely and privately. It's not about technology at all...it's about communication and good parenting.

Remember, we're all in this together!

Parry

Parry Aftab, Esq.

Executive Director

[WiredSafety.org](http://WiredSafety.org) and its family of sites and programs, including [Teenangels.org](http://Teenangels.org), [WiredKids.org](http://WiredKids.org) and [CyberLawEnforcement.org](http://CyberLawEnforcement.org)

[WiredSafety.org](http://WiredSafety.org) is a 501c-3 non-profit organizations formed under the laws of the State of New York. (Its legal name is "Wired Kids, Inc.") This publication is copyrighted to Parry Aftab, Esq. All rights reserved. For permission to duplicate this publication, contact [parry@aftab.com](mailto:parry@aftab.com).

### **Appendix 5: More about WiredSafety.org**

WiredSafety, is a 501(c) (3) charity and the largest and oldest online safety, education, and help group in the world. Begun as a group of volunteers rating websites in 1995, it now provides one-to-one help, up-to-date information, and education to cyberspace users of all ages on anything that can go wrong online. These services are offered through a world-wide system of volunteers, who make up their various teams and divisions, and administer their specialized sites and programs. With the exception of our Teenangels, outreach and speaking programs, all work and help is provided online and without charge. All within WiredSafety.org are unpaid volunteers, including its founder and Executive Director, cyberlawyer Parry Aftab.

WiredSafety's work falls into four major areas:

- **Help** for online victims of cybercrime and harassment
- **Assistance** for law enforcement worldwide on preventing and investigating cybercrimes
- **Education** for children, parents, communities, law enforcement, and educators
- **Information and Awareness** on all aspects of online safety, privacy, responsible use and security

WiredSafety's audience and the key stakeholders include:

- Parents, grandparents and caregivers;
- Kids, preteens, teens and college students;
- Members of the Internet and interactive technology industries;
- Law enforcement, the judicial community and regulatory agencies; and
- Schools and educational institutions

Together with their wiredcops.org program, specially-trained volunteers assist with cases of child pornography, child molesters, and cyberstalkers. WiredSafety also offers a wide variety of educational and help services to the Internet community at large. Companies such as Disney, Yahoo!, Oracle, MySpace, Facebook, Microsoft and AOL turn to Parry Aftab and WiredSafety.org for guidance and help. Other volunteers find and review family-friendly Web sites, filtering software products, and Internet services. Some of the outreach team volunteers run programs, summit and also speak at local community groups and schools around the world teaching Internet safety, privacy and responsible use.

And its work is not limited to the Internet alone. WiredSafety focuses on all aspects of interactive technology use and abuse. Its expertise includes cell phone safety and security, interactive gaming, social networking (mobile and online) and text-messaging products, as well as any new interactive technologies as they are developed. Its long years of working with Internet users and handling cybercrimes and abuse have created a flexible and knowledgeable volunteer force. If you can view content, communicate with others or spend money or buy things using the technology, WiredSafety can help.

Its help also involves one-to-one assistance for cases of cyberabuse. WiredSafety's cyberhelp line gives netizens access to free help when they need it online. Its special team of help volunteers are assigned to cases and work one-to-one online to help resolve your problems and get you help when you need it. WiredSafety handles more cases of cyberstalking than any other organization in the work, helping

thousands each month through its site and reportline. Cyberbullying cases can be reported to the reportline as well.

The new focus on cyber-wellness and cyberethics fits perfectly within WiredSafety's mission and expertise. As we raise a new generation of cybercitizens, they need to understand the norms and rules of operating online. They must also recognize that they must be held accountable for what they do in cyberspace and that what they post online has ramifications beyond the momentary click. Marvel joined forces with WiredSafety to provide superhero assistance in educating our children and families on safer online practices. The first Internet safety comic, Internet Super Heroes meet the Internet Villains, teaches how Internet predators can infiltrate anyone's computer and wreck havoc on their lives by stealing their identity and posing as them online. Published under our exclusive license with Marvel, and sponsored by Microsoft, this comic will help teach the 250,000 readers how to be smart and safer online.

WiredSafety is proud of its reputation as the one-stop-shop for all cyberspace safety, privacy, security, and help needs. It is even prouder of the fact that all this can be accomplished without large government funding or money wasted on administration costs. Its volunteer workforce has been estimated at providing more than \$3 million in unpaid services every year. It has operated since 1995 with a total funded budget of under \$150,000 a year.

WiredSafety is headed by Parry Aftab (also a volunteer), a mom, international cyberspace privacy and security lawyer and children's advocate. Parry is the author of the first book written for parents about Internet safety - The Parents Guide to the Internet (considered the bible of online safety and published in 1997) as well as The Parent's Guide to Protecting Your Children in Cyberspace (McGraw-Hill, 2000), which has been adapted and translated around the world. Her most recent books have been especially written and adapted for and published in England, China, Spain and Singapore. Her new book, Internet Safety 1-2-3 will be released this year in the United States. It was released in December 2005 in Spain.

WiredSafety volunteers range in age from 18 to 80. WiredKids range from seven to twelve, and the Teenangels from 13 to 18. These programs run in conjunction with WiredKids.org, one of WiredSafety's division. WiredSafety backgrounds include everything from TV personalities, teachers, stay-at-home moms, retired persons, law enforcement officers, and students to PhD's and writers.

For law enforcement officers, WiredSafety provides information and resources to help educate and guide officers on Internet safety issues and crime prevention and reporting of cybercrimes. It also has a special website just for law enforcement officers, Cyberlawenforcement.org and WiredCops.org.

It is also the only organization that uses expert trained teens and preteens to help develop safer technologies, by advising members of the Internet industry and governmental agencies around the world. These expert Teenangels (and now their younger version, Tweenangels from 9 - 12 years of age) deliver the message of safe, private, and responsible technology use to their peers. These youth-based programs were formed in 1999 to provide special perspectives and insight into how young people are using the new technologies and how to better prepare them to handle the risks they encounter. Teenangels have been recognized and honored by Congress, John Walsh and recently, Teen People Magazine, among others. Recently, at the request of leading law enforcement agencies, WiredSafety has begun using its young volunteers to provide information that will assist undercover law enforcement officers in being more believable when posing as young teens.

Originally formed to provide help and protection for Internet users of all ages, WiredSafety's work has become more and more focused on children, tweens, and teens in recent years. WiredSafety is dedicated to protecting children in cyberspace from cybercrimes and abuse, including from each other. This involves protecting them from cyberbullying, hacking, sexual harassment and identity (ID) theft. It also includes protecting children everywhere from Internet-related sexual exploitation, including assisting law enforcement in the investigation and prevention of trafficking of children, child pornography, and organized child molester groups.

WiredSafety's experience is particularly effective in assisting law enforcement agencies in improving their undercover skills.

MR. WHITFIELD. Thank you, Ms. Aftab. And we want to hear from Ms. Sullivan in just 1 minute but right now I want to recognize Mrs. Schroeder for her 5 minute opening statement.

MS. SCHROEDER. Thank you very much. I wanted to thank you, Chairman, for inviting me here to testify today.

And what I would like to do is talk about what i-SAFE has been doing for the past 6 years. We have been in Congressional Appropriations for the past 6 years. We are in all 50 States and we are in 15 countries. Predatory acts against our children are the most heinous acts that we have ever seen. We have heard it today from Justin and we have seen it time and time again with many, many children. And we look at this in terms of, and we ask ourselves how can this be, you know, in terms of families, we are here to protect children.

Our Nation now is being faced with a new technological challenge which is these kids know a lot more about technology than parents. They know a lot more about technology than their teachers. This is their world. In my day, when I would come home from school, I would pick up the telephone and we would be talking to one another. Today, what the kids do is they go home, they fire up their laptops, and they get on the buddy list and that is their friends. And we have heard testimony today in terms of how do you define a friend, how somebody tries to make a friend online, and how that is all done under the guise of anonymity.

If you would look at the screen that I have here on the Internet landscape and as you see here, 90 percent of the kids and this is an assessment that we did with over 200,000 students in the schools and they have Internet access. If you look at the fact that 25 percent of those kids and we really do believe that this is a low number, they spend at least 5 hours a week online. If you look at also too the way the Internet is is that the kids like to be by themselves. We heard this with Justin in his room. This is where he was comfortable in terms of he needed to talk to people. And as you can see here with the statistics that we have with them, the numbers are quite high when you start looking at the fact of in fifth grade 40 percent. That is small. In fifth grade, we are still chaperoning our kids but yet they feel so comfortable on the Internet in

terms of being alone. Also here, if you look at the statistics that we have and there is no right or wrong answer from these kids. I mean they--we did pre, post, and delayed assessments, but 33 percent of them said that they feel freer in cyberspace. And I actually have had the opportunity to do site visits in these schools and some of the questions that we asked them is why do you feel freer in cyberspace. And it is just one of those that they feel that they know these people. We heard from Justin and how he was enticed and he did things that in real life you would think that is something that nobody would ever do.

But also, too what we looked at was the fact that the students and we went ahead and did a survey of 30,000 students with 30,000 parents and we asked them, do you tell your parents what you are doing online? And what was interesting after this survey was the fact that the kids said no but the parents said yes. And actually this was published by the Justice Department when we were through with it, and what we found out with the conclusion of this that this is the digital divide. We went ahead and asked the kids in terms of would your parents approve of what you did on the Internet? Many of the kids said no and the parents said that well of course I would, I trust my kids in terms of what they do on the Internet. We look at the risky online behavior of students. As kids grow older, they take risks and that is inherent within them. That is how they learn to be able to do things in terms of they take risks riding bikes, they take risks in everything that they do in life and one would hope as they grow and they become much more mature, that those risks are much more calculated and they do not become risks but more so it is one model of appropriate behavior.

We went ahead and in the school districts we asked the students in terms of how many of them gave out personal information and what we found out from these kids was the fact that many of them said well I do not tell people my name. And one of the activities in the classroom is the fact that they will have to go and actually tell what is their screen name and they had discussed is that identifiable information? How much of your screen name does that say about you? And what we found out was the fact if you look here, there is a very high percentage of kids that what they do is they will put a screen name down and then describe maybe their age, their location, what they like, what they do.

We found out, too that after education, NIJ gave a \$3 million grant to an entity in Virginia to study us for 2 years. We were selected on an efficacy study and we presented that study to you in November. And what they told me when they presented it was is that they saw that this is probably the fastest crime prevention in terms of preventativeness that really made a difference. And one of the questions I asked was why? Why did they see that of all the crime prevention that they had ever

looked at before? And you know it was a real easy answer, which is this is their world. This is their cyberspace. They know all about it. And after the curriculum, what we found out here was that 84 percent of the students they were a lot more careful in terms of the information that they gave out. They also were a lot more careful in terms of what they were sharing information because now they are a lot more knowledgeable about I understand now in terms of what that information can do and where it can go. Also in actual property. Many of the students did not understand what is that? Isn't everything free out there? They did not really grab the concept of this is actually stealing.

We look at the fact of meeting face to face and you can see here many of the students there is not any student that you would talk to that said yes, I do want to meet a pedophile online. There is just, I mean, that is just not going to happen to them. And we have talked to millions of kids. But the fact is while they are looking at that saying that they are a lot more careful in terms of being a willing participant. When they start giving gifts, they start thinking this is not normal. One of the activities in the fourth grade class was the fact that the kids turn around and they have something and they are to give it to their best friend. And if it contains a value, let us just say \$50, you do not want to give that away. Well then why would you think that somebody that you do not know would send you money in the mail?

Up here is a chart and it is a map of the United States. This year, i-SAFE will have educated 1.8 million students. And those are audited figures. Those are classroom instructions that we get from the school. We have cooperative agreements with the schools. And so as you can see here that, those are pretty significant numbers in terms of the desktops, the numbers of kids that we actually touch their lives every single day.

And one of the big things that we have found is is that the peer-to-peer, you are hearing it, peer-to-peer from the kids and I have with me one of our I Mentors and he is from the State of Maryland. And what I wanted to actually show today and I have here in terms of we use Kentucky as a model. Kentucky was one of our original States that we actually implemented in and it was a State that just took off with a vengeance, particularly with those mentors. It was amazing to see what they did in their State, in that particular State. When you look at the model of Kentucky, we formed the partnership with the Department of Education, with law enforcement, with the Attorney Generals, with the parent organizations, with the school organizations. We did 120 man professional developments in that State, 88 parent programs. And as you can see in that State alone there are over 112,000 students that have received the curriculum.

Also looking in terms of the educators on a national perspective, we have done almost 2,000 professional developments nationwide and we do train the trainers so we form a strategic development, a partnership with the Department of Education and it's institutionalized within their school day.

And you do not want to forget the parents because the fact is that parents they are trying to catch up with what their kids are doing. I was on the last two Dateline segments with Chris Hansen on how to catch a predator. And the big one that was just on television a few months ago, I addressed the issue of parents. And it is not the fact that parents do not care, it is just that many parents and including myself grew up in the television age, so you cannot grab the concept of can that computer really do that? Or, you know, if the computer is upstairs in their bedroom, many parents today are thinking, I am really glad that my son or daughter is at home, it is 10:30 at night, but the question is who are they up there with?

MR. WHITFIELD. If you could summarize, Ms. Schroeder.

MS. SCHROEDER. Yes. What we have looked at today is the fact that kids are having two way communication. We did a project with VeriSign and we gave kids their first digital ID and it was called the i-STIK Project. Kentucky participated in that as well. So they see what kids are doing with social networking, they are in school, they are doing their homework online. And on this particular project what we did there are the kids actually had a digital ID, they went to a local area and right now what we are working with is YAHOO. We had Myspace contact as well regarding, because of the problem that they are having, Microsoft, and looking at the fact of being able to give these kids their own digital ID so it would authenticate them. So what happens is is that you are in a green space where there is other kids.

What I would like to do is just show you brief video on the mentor in Kentucky.

[Video]

Thank you very much.

[The prepared statement of Teri L. Schroeder follows:]

PREPARED STATEMENT OF TERI L. SCHROEDER, PRESIDENT/PROGRAM DIRECTOR, I-SAFE AMERICA, INC.

Thank you, Chairman Whitfield and Ranking Member Stupak for inviting me to testify before the House Subcommittee on Oversight and Investigations at the hearing entitled "Sexual Exploitation of Children over the Internet: What Parents, Kids and Congress Need to Know about Child Predators."

Predatory acts against our children are among the most heinous of crimes perpetrated within our society. Historically, communities as a collective take deliberate and specific actions to protect their children in an effort to prevent these heinous acts.

These protective actions include: education – teaching children to be wary of strangers, to recognize and avoid dangerous situations, to cry for help when they feel threatened.

Our nation is now faced with technological advancements that allow even the youngest of children to have access to the Internet. Students today explore the wonders of the world by transporting themselves through cyberspace. They can travel to the brightest most intellectual domains of the universe and conversely, they may travel to the darkest most detestable realms of the human imagination; and they travel this world alone. A universal paradigm shift has occurred in the methods and means available to child predators in pursuit of their prey; and as such a universal paradigm shift has occurred on the preventative tactics that we employ in our efforts to protect our nation's youth against these predators.

The content of my testimony today will address the ramifications of this universal shift as our nation's youth explore the wonders of the Internet. We truly are a global economy and as such our nation's youth are cyber citizens engaging in online activities. Those activities include socialization (two way communication whether that be through email, chat or instant messaging), games, shopping, entertainment and education.

I will be addressing the role of education and youth empowerment and the need to empower our nation's youth with the appropriate tools to minimize the number of predatory acts predicated against them. It is imperative that a proactive well-balanced approach be deployed to support the challenge of embracing the activities of our nation's youth online.

i-SAFE America is dedicated to: 1) implementing a standardized Internet safety education program throughout the nation that provides kids and teens with essential tools to reduce the risk of their being victimized while engaged in activities via the Internet; and 2) launching an Outreach Campaign that empowers students to take control of their online experiences and make educated, informed, and knowledgeable decisions as they actively engage in cyber activities. From September 2005 through March 2006 i-SAFE educated over 1.3 million students nationwide. That number continues to increase monthly as the i-SAFE program is expanded throughout school districts.

The i-SAFE Internet safety curriculum is a teaching and learning experience, which incorporates best practices as they are defined by the latest educational research, and correlates them to accepted educational standards. This is accomplished by providing a broad range of materials and formats which meet a variety of teaching and learning needs for students and educators in grades Kindergarten through 12. Topics are centered on up-to-date information pertinent to safety issues, which confront today's youth through continuing advances in Internet technology.

The curriculum creates a successful learning environment through a model of integrated critical thinking activities and guided opportunities for youth empowerment. Active participation in i-SAFE student activities promotes acquisition of knowledge, analysis of online behaviors, construction of solutions to Internet safety problems and issues, and involvement in the spread of Internet safety concepts to others through peer-to-peer. Through this process, students enhance and enrich their own lives, the lives of other students, and the community at large as they engage in creating a safer cyber community.

Our children now live in two diverse worlds: their physical world and the world of cyberspace. As such, they essentially live in two cultures that often conflict. Previously, many of the lessons learned in the physical world don't seem relevant in cyberspace as these children reach out to strangers as friends. This paradigm shift demands new innovative educational programs, and tools, for our children; their parents and the community. It is essential that children, as they travel their world of cyberspace alone, be provided with the knowledge and tools they need to independently recognize and avoid dangerous situations online; to actively engage learned proactive techniques to more safely interact with strangers online; to critically appraise situations in which they find



themselves; and to react appropriately when they find themselves in uncomfortable, compromising, or threatening situations.

Students today will be global citizens for the rest of their lives. Students view the Internet in a much different way than adults.

I would now like to address the “Parents Internet Assumptions” and the “Youth Perceptions/Behavior regarding the Internet.” At the time of this report approximately 100,000 students had participated in the survey process; students participating in our US program by grade level were:

- 15,000 K – 2 students
- 22,200 grades 3 & 4
- 62,800 grades 5 – 12

The i-SAFE assessment results show that in most cases there is a noticeable difference in a student’s participation in risky behavior from grade to grade. Older students are more likely to take risks and/or feel safe in the Cyber world. This finding reinforces the need to introduce and educate our youth in the early grades. For example: When asked if they had visited an “inappropriate” website; 15.5% of 5<sup>th</sup> graders said yes vs. 36% for 10<sup>th</sup> graders.

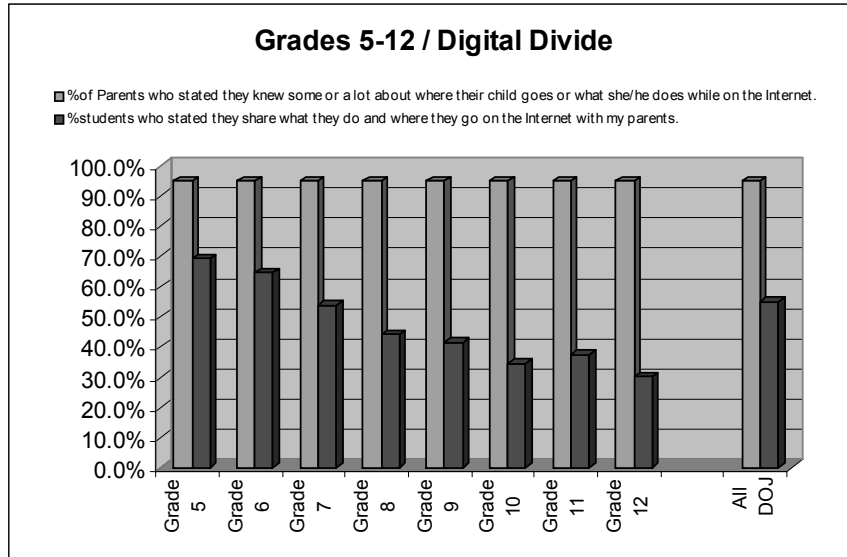
Relative to gender; males are more prone to visit an inappropriate place on the Internet than females (31.3% vs. 18.7%) and are likewise greater risk takers when asked if they were willing to meet someone from the Internet “face to face” (19.2% vs. 11.2%). Males were more likely to play games as their primary online activity while females were more likely to chat or use email.

Also, based on pre assessment results; it is evident that once a youth enters cyberspace there are no significant differences in behavior between ethnic groups. Therefore, the Internet has become the great equalizer. 90.4% of students’ in grades 5-12 and 84% of students’ in grades 3 & 4 have Internet access. And on an average 37% of all 3rd & 4th graders use some form of Internet communication; that figure rises to the 80-90% level in the upper grades. Interestingly, about 45% of students in grades 8-10 stated that online communications were their main method in keeping in contact with friends. In addition students in grades 5 –12 stated that:

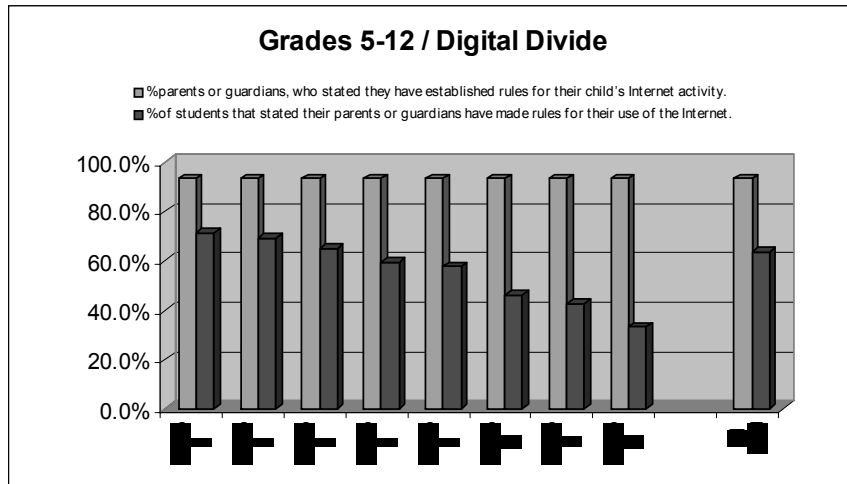
- 23% are online for more than 5 hours a week (86% are online at least 3 hour a week).
- 8% have been asked to keep their Internet friendship a secret.
- 12% have been upset by something that was said by a stranger they met on the Internet.
- 32% have the skills needed to get past filtering software and 20% have actually used those skills to get past filtering software.

#### **Digital Divide Between Parents & Youth**

There is a gap between what parents say they know and what youth claim they share with their parents. In an i-SAFE survey with over 2,000 parents, the vast majority (94%) of parents stated they had a pretty good idea about their child’s online behavior. In contrast, only 54% of the students said they share where they go and what they do on the Internet with parents. Our results also show that these differences between parents and students generally increase with increasing age.



Of the parents surveyed, 93% felt that they had set ground rules for their child’s online activities. However, the percentage of students acknowledging that their parents had established rules for their Internet use drops to 63.7% (see chart below).

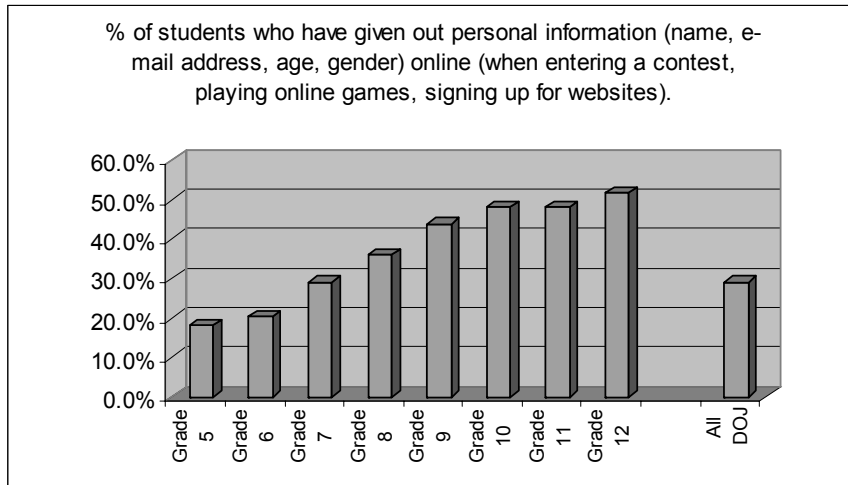


In addition, 21% of the students stated that their parents complained about the amount of time they spent on the Internet but 29% also felt that their parents really had no idea how much time they were actually spending online. 62% of the parents polled indicated that they were NOT concerned about the amount of time their child spends online. Interestingly, on average, 25% of the students stated that their parents, on some level, would disapprove of their online activities and 13.8% actually keep their Internet activities secret from their friends and family. The gap between what youth believes to be

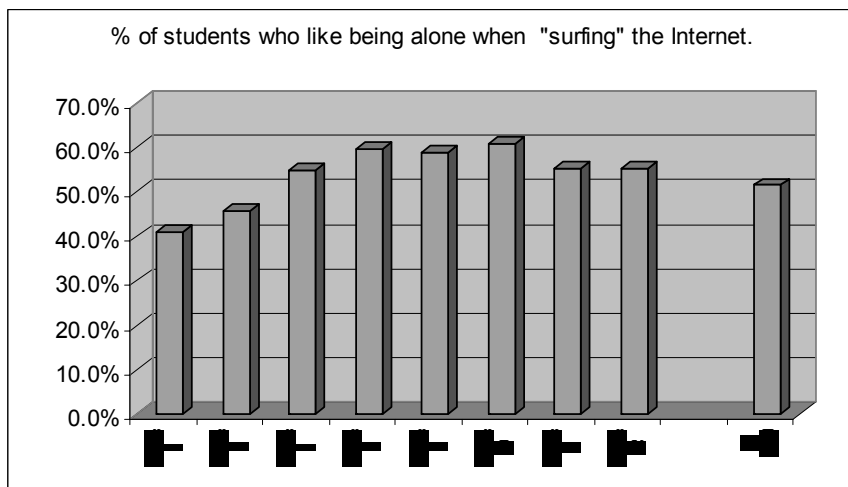
their parent's level of awareness regarding their online behavior and what parents have stated is significant and merits continued attention.

**At Risk Behaviors**

There are other individual statistics that underscore the need for constant Internet safety education. For example, the Internet has become a focus for youth to find entertainment, make new friends and make purchases. On an average 29% of the students have shared such information when going online. That figure goes up in the 50% in the higher grades.

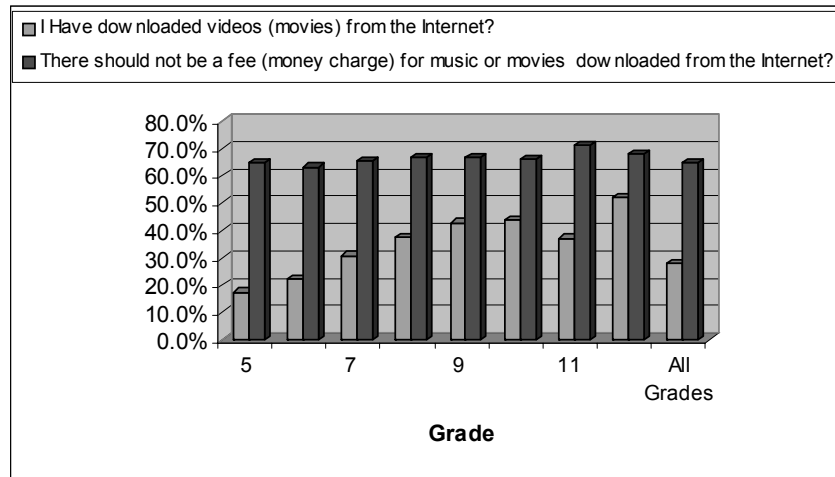


Two other factors compound this issue. More than half of all students prefer to be alone when accessing the Internet (see graph below). Combine that desire with a student having their own computer in their room (22% overall stated that the computer they use is in their bedroom); and students feel empowered or freer to do what they want on the Internet than they do in the real world (33%).



It should be pointed out that even in the very early grades our youth are being exposed to the cyber world. It is folly to suggest, as some have stated, that “kids that are young are not Internet savvy.” The vast majority of K-2 teachers (54%) stated that at least 50% of their students have used a computer at home and 16% of the teachers indicated that at least 50% of their students have used email. A significant number had also gone into chat rooms. The age demographics of these students consist of 5, 6, & 7 years olds.

28% of all students in grades 5-12 (43-52% in the upper grades) have downloaded music or movies from the Internet. On an average, 65% were against any type of fee being charged for the service.



In real life Kids/Teens spend twice as much time with peers as with parents or other adults. However, through the guise of anonymity the Internet provides a medium which allows a student to believe that the communication they are having online is a respective peer when in many instances it is an adult. Even though students may be aware of the dangers inherent in communicating with someone online, we continue to see they make decisions about engaging in a behavior as if it were a one-time thing.

Risk taking is a natural part of kids/teens lives. They take risks in order to grow, trying new activities, generating new ideas, experimenting with new roles. However, they can also find themselves in trouble with their risk taking. Concern over such risk behaviors have led to the creation of many types of intervention. Some of these interventions have attempted to manipulate kids/teens beliefs, values and behaviors hoping to get them to act more cautiously. Other interventions have attempted to improve their stability to make sensible decisions, hoping to get them to make wise choices on their own. Having general decision-making skills enable kids/teens to protect themselves in many situations.

#### Education Makes A Difference

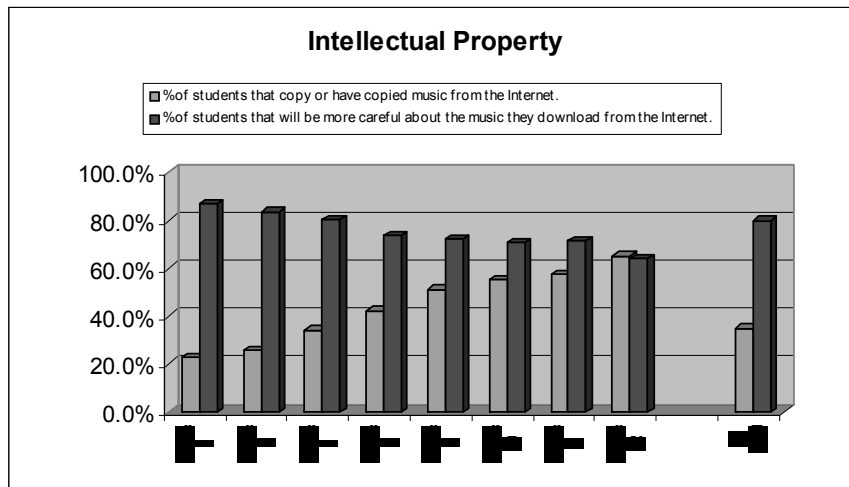
The good news is that in-classroom education and outreach efforts do make a difference. Students taking i-SAFE post assessments, immediately after completion of the i-SAFE curriculum, demonstrated a significant rise in their Internet dispositions.

84% of students stated an intention to be more careful about where they go and what they do on the Internet.

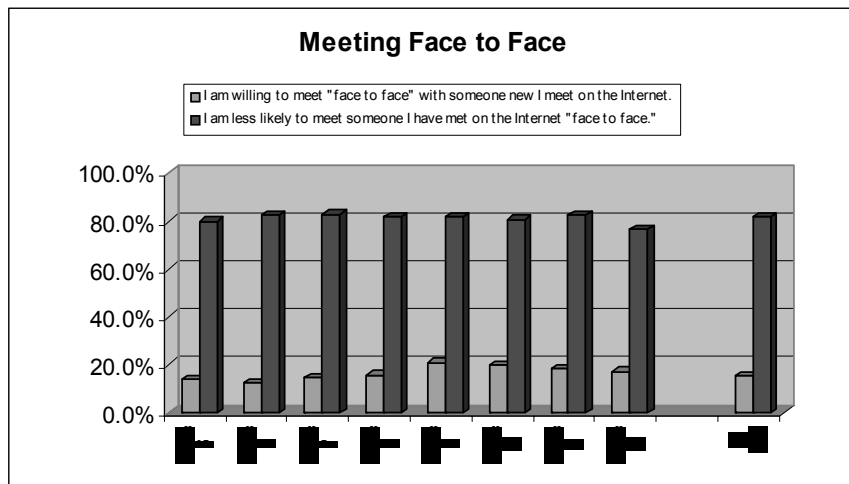
89% indicated that they would be more careful about the email attachments that they open.

88% will be more careful about sharing personal information with those they meet in chat rooms and other places on the Internet.

On an average, 80% of the students polled after completing the i-SAFE program were going to be more careful about downloading music from the Internet. However, older students were more inclined to download and less concerned about being careful.



An area that attracts quite a bit of attention is child predation. Our pre assessment data shows that on an average about 15% of the youth were willing to meet someone new from the Internet "face to face". After the i-SAFE program 82% of all students stated that they would be less likely to meet someone face to face.



Though individual statistics can be interesting and in some cases alarming, the real power of the data lies in the overall trends that reveal the impact of emerging cultural and social changes brought about by the Internet. The increasing amount of time spent in the Cyber world, the ability to remain “anonymous”, the perceived lack of rules, the ease of access; all contribute to a revolution in the way our youth interact with each another, the way they make friends, and the social skills they develop.

It is widely recognized and accepted that the main activity of kids/teens, as cyber citizens, is online two-way communication. That communication consists of chat, email and instant messaging. The nucleus of the Internet affords the opportunity of two-way communications and inherently the computer does not know whether the users communicating are that of a child or an adult. This means of communication allows users, regardless of age, gender or socioeconomic status to openly and freely exchange ideas and information. Our nation’s youth has now coined a new term for “ hanging out with my friends” and actively searching for new friends is done through a click of a mouse.

Kids/teens rarely “travel” with their parents or a chaperone to many of the online areas. Buddy lists and instant messaging has replaced the traditional “telephone and phone book.” Without education and the appropriate tools to raise their awareness and to empower them to recognize the danger of being alone in a room full of strangers, our nations youth will continue to be at risk for exploitation.

Let me begin by addressing specific examples of how dramatically the protective actions that have been employed historically have been impacted by this technologically-enabled, Internet-driven, paradigm shift.

Education: Parents teach children to be wary of strangers on the street, in public places, and at the front door; but now, the strangers that these children meet – are not on the street – they are in cyberspace. And, to the detriment of the parents, many of their children are more “Net” savvy than either parent. This inequality of knowledge hinders parents in their abilities to address cyber safety issues and to properly instruct their children about the dangers of meeting strangers online.

Historically, when parents taught their children to recognize and avoid dangerous situations, those situations were based on tangible, physical elements within their community. Now, danger lies in an amorphous cyber-world cloaked in the allusion of anonymity.

Parental Supervision: Many of our children’s activities have dramatically shifted from participatory activities (easily supervised by a parent and often enjoyable to watch) to solitary activities - engaged through the computer keyboard or joystick - that do not lend themselves to easy supervision nor enjoyment by a non-participant (such as a parent). Children may spend hours playing solitary games online, or they may play in tandem with their cyber friends, or they may even play with total strangers they connect with online in an Internet gaming community.

The Internet has broadened a child’s ability to meet other people and acquire “friends.” Historically, children made friends at school, through family acquaintances, and from participating in community organizations. A child is no longer confined to the local community from which to socialize and gain friends; literally, cyberspace eliminates all geographical barriers and frees a child to roam the world in search of that one, special “friend.” Predators are also free to roam.

The degree of difficulty for parents to monitor, or to simply meet, their child’s friends has increased tremendously.

Preventative Tactics: A commonly employed tactic for protecting our children is to provide an adult chaperone as our children explore outside of their community. Now, children explore the wonders of the world by transporting themselves through cyberspace and they travel this world alone, without the care and protection of a chaperone.

Physical Barriers. Historically, parents routinely lock their doors at home each night to keep intruders out; schools monitor persons who enter the campus. There are innumerable, vulnerable children who are isolated, lonely, and bored who constantly search the Internet for other children with whom they can make friends and chat. As these children search the web for friends so too the predator searches the web for prey. The predator will find the child, the child will find a “friend,” and the outcome will be devastating.

The effectiveness of currently employed physical barriers has been severely compromised. Predators lure and seduce their victims from within the privacy of the victim’s own home and operate in a world that is no longer constrained by physical limitations or geographical barriers. They stalk their prey through cyberspace and the ramifications of this universal, paradigm shift are staggering. When taken as a whole they can be overwhelming, perhaps paralyzing; but - if ignored - the ramifications will be devastating to our youth. To approach any entity of this magnitude and to effect change it is advisable to search for a common element, theme; or component against which a focused solution may be enjoined.

Up to this point in my testimony, I have provided insight into the incredible paradigm shift that has occurred in our society and how this new paradigm directly affects the safety of our children. To illustrate the critical points, I mapped the ramifications of this paradigm shift to a common element in cyberspace: two-way communication (ie. chat room, instant messaging and email)

The remainder of my testimony will focus on potential solutions that we as a society may embrace as our children extend into the farthest reach of cyberspace; as they interact virtually with persons throughout the world and as they evolve as “Net” citizens.

As Judith F. Krug, Director of the American Library Association’s Office for Intellectual Freedom, stated in her testimony before the COPPA Commission on August 3, 2000: “The children of today will be Net citizens for the rest of their lives. They need to be taught the skills to cope in the virtual world just as they are taught skills to cope in the physical world. Children should be educated in appropriate increments and appropriate settings on how to avoid inappropriate Internet content, to report illegal or unsafe behavior and to engage in safe interaction online. Children who are not taught these skills are not only in danger as children in a virtual world, they also will grow into young adults, college students and an American workforce who are not capable of avoiding online fraud, Internet addictions and online stalking.”

It is imperative that any domain that engages in the attraction of kids/teens recognize how children actually use the Internet. It is equally important to promote the online social activities within the domain to support the academic strategies that teach children to make safe and wise choices about using the Internet and to take control of their online experiences: where they go, what they see, to whom they talk, and what they do.

Our nations youth need to be given the tools to assist them in the acquisition of skills that will allow them to evaluate independently the information they are acquiring and exchanging online. By improving their "information and media literacy," they will become safe and responsible cyber citizens thus vitiating the “digital divide” that exists today between Youths Perception/Behavior regarding the Internet and those of their Parents.

Currently, both businesses and governmental agencies have begun to embrace digital certificate technology as an electronic means for identifying participants in transactions that occur online. They leverage this technology as a method for verifying and authenticating a person’s electronic identity. The simplest way to view a digital certificate is as an electronic ID card. However, digital certificate technology is far from simple. Given that the intent of this testimony is to identify and express how technology can be used, rather than to define the intricacies of the technology, I will refer to digital certificate technology in the simplest terms possible for the reader to understand.

A certification authority issues digital certificates. A certification authority can issue various levels of digital certificates that are dependent upon the amount of authentication that is required to ensure that the person who is applying for the digital certificate is in fact the person that he or she claims to be. In other words, to obtain a digital certificate a person must present proof of identity and the “level” of the certificate obtained depends upon the amount of proof required.

Example: Level 1 certificate - any photo ID required  
 Level 2 certificate - government issued photo ID required  
 Level 3 certificate - government issued photo ID required plus passport or birth certificate  
 Level 4 certificate - all requirements of Level 3 plus a background check  
 Level 5 certificate - DNA

How could digital certificate technology increase the safety of children who frequent a particular chat room or deploy two-way communications on the World Wide Web?

A public- or private-sector chat room provider could engage digital certificate technology as a means for permitting or denying access to any given chat room or online area that allows two way communication. Conceivably, a chat room provider could institute a policy that only children under the age of 13 are allowed to participate in a particular chat room. The intent of this policy is to provide a safer online environment by making their “best effort” at excluding adults and potential pedophiles from the chat room. To enforce the “under the age of 13” policy, the chat provider would require all participants to login using a Level 3 digital certificate. Through the use of the digital certificate and the chat provider’s policy of restricting access, the children participating in this chat room have a lessened degree of risk than those children that participate in unrestricted chat rooms.

This technology exists and i-SAFE, through the empowerment of our partnership with Verisign, has launched the first tool for our nation’s youth, using digital certification. The unprecedented Digital Credential program, “i-STIK” works to reduce the vulnerability of America’s students in all grades, K-12, with a unique digital credential that helps protect students as they engage in two way communications online.

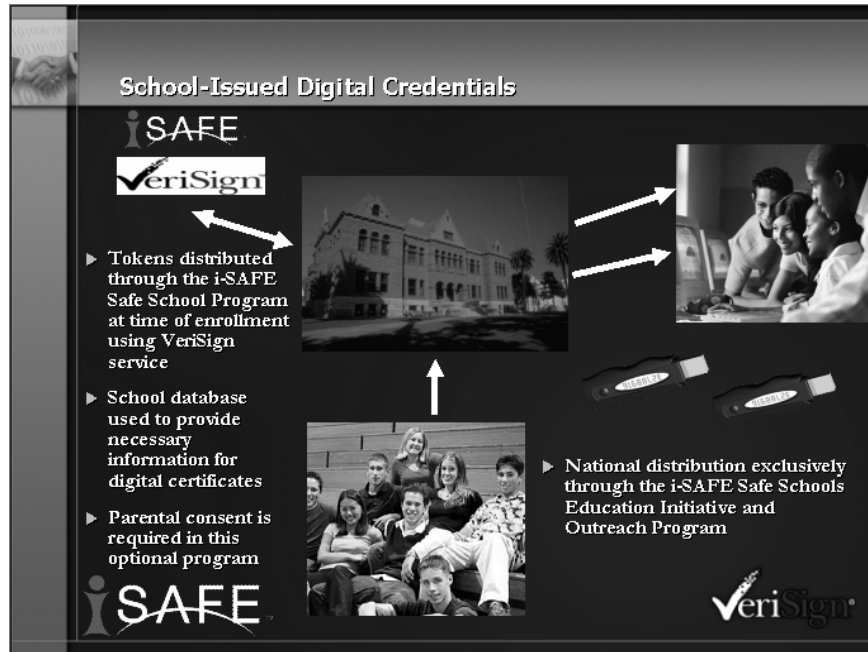
The Digital Credential is in the form of a small USB Token, which can be carried on a key chain and used at school, home; or on any computer with a USB port. The Digital Credential allows the kids and teens to enter an age centered chat room, or conduct two way communication, with confidence that everyone logged in will be who they say they are – chatters actual ages and genders can be confirmed from the digital credential token. The digital credential helps to safeguard the integrity of the child’s online experience.

The digital credential is distributed through the i-SAFE Safe School Program at the time of enrollment (with parental consent) helping confirm to parents that this program is offered through a trustworthy source.

The schools database, which remains with the school, provides all the necessary information contained on the digital credential and validation is provided to assure that the token is valid at the time of usage. Neither i-SAFE or Verisign has access to this information. The identity of the student is never disclosed, just the students age and gender. The program allows for easy revocation of the credential when the student transfers, graduates or is no longer enrolled in the schools.

I am showing you screen shots of how this new tool will be deployed and the interaction between the user and technology.





We currently use digital certificates to execute online financial transactions. Businesses use this technology to protect their monetary assets. In September of 2005 there was a deployment of a pilot project that allowed parents to opt in to have their son/daughter be issued their first digital certificated which is being deployed nationwide as the “i-STIK.”.

## Usage of Tokens



- ▶ **Tokens are portable containers for a child's digital credential**
  - Use on any USB port
  - Can be carried around on a key chain
  - Can be used at school, at home, or in any computer with a USB port
- ▶ **Digital Credentials only contains necessary info for usage online**
  - Gender
  - Age

**iSAFE** 

Protecting our children is at the very heart of this hearing. Thank you Chairman Whitfield and Ranking Member Stupak for inviting me to testify before the Subcommittee on Oversight and Investigations. In my testimony, today, I addressed the paradigm shift that has occurred within our society due the advancements in web technologies and the advent of two way communications that could be deployed to facilitate the establishment of an enjoyable environment for our nations youth. I have touched upon one technological approach that i-SAFE is launching to empower our nations youth with a “tool” to help protect our children from falling victim to online predators.

In conclusion, there is no single solution for protecting our children. However, the value of empowering our children - through “**education**” – with the knowledge and critical-thinking skills that they need to be able to independently assess the every-day situations they will encounter, while online, cannot be overstressed. Children must be able to effectively protect themselves from cyber predators, to recognize potentially harmful or inappropriate actions, to actively disengage from negative behaviors or compromising situations, and to seek help when threatened. These lessons are learned. Education and empowerment are key.

**iSAFE** I-SAFE America Presents

## The First Digital Credential Program for America's youth.



### The Facts

A 2003 i-SAFE America study shows that nearly 11% of kids and teens have met someone "face to face" who they "met" online.

Considering that more than 50 million youth in the United States use the Internet and countless online predators lurk in cyberspace waiting for unsuspecting victims, **millions** of American kids and teens are **at risk** of abduction or worse.

A lack of valid age authentication in the online areas kids and teens surf the most has compromised the safety of those who use those chat rooms, Instant Messaging services, and other public online areas.

Some websites allow the purchase of alcohol, cigarettes, and adult materials with the only validation being a credit card – no age verification is required!

### The Solution

On February 10, 2004, a revolutionary new way to help protect the safety of America's kids and teens online is officially introduced.

i-SAFE America, the nation's leader in Internet Safety Education and VeriSign, a leading provider of critical infrastructure services for the Internet and telecommunications networks, have partnered to create a groundbreaking program that provides the most innovative degree of online safety previously unavailable to our nation's youth.

The **unprecedented** Digital Credential Program works to **reduce the vulnerability** of American students in all grades (K-12) with a unique digital credential that helps protect students as they surf the Internet.

### The Empowerment



### The Technology

The Digital Credential is in the form of a small USB token, which can be carried on a key chain and used at school, home, or any computer with a USB port. Besides the convenience of portability, the Digital Credential provides a foundation for additional features such as a personal data storage device.

The Digital Credential allows kids and teens to enter an age-centered chat room with confidence that everyone logged in will be who they say they are – chatters' actual ages and genders can be confirmed from the Digital Credential token. The Digital Credential helps to safeguard the integrity of the child's online experience.

The Digital Credential is distributed through the i-SAFE Safe School Program at the time of enrollment (with parental consent), helping confirm to parents that this program is offered through a trustworthy source.

The school's database provides all the necessary information contained on the digital certificates and VeriSign provides validation to assure that the token is valid at the time of usage. The identity of the student is never disclosed, just the student's age and gender. The program also allows for easy revocation of the credential when students transfer, graduate, or are no longer enrolled in the school.

### The Future



i-SAFE has partnered with the American Football Coaches Association on their National Child ID Program. The paw imprint of i-SAFE's cyber dog, Browzer, is indicated within the token if a student has been ID'd through the i-SAFE/AFCA alliance.

The Digital Credential helps to build a natural association of online safety through its branding.

VeriSign will manage and update the service integrity of a national database which contains every participant's information.

[www.isafe.org](http://www.isafe.org) [www.verisign.com](http://www.verisign.com)

**References:**

NTIA and Economics and Statistics Administration. A Nation Online: "How Americans Are Expanding Their Use of the Internet" published by the National Telecommunications and Information Administration, U.S. Department of Commerce, Economics, and Statistics Administration (02/02)  
[www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htm](http://www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htm)

i-SAFE America student assessment data, 2005

MR. WHITFIELD. Thank you, Ms. Schroeder, very much. And Ms. Sullivan you are testifying also. Is that correct?

MS. SULLIVAN. Yes.

MR. WHITFIELD. Well you are recognized for 5 minutes, Shannon Sullivan who is a Teen Angel with WiredSafety.

MS. SULLIVAN. Thank you, Mr. Chairman.

I am Shannon Sullivan. I am 14 and I live in New Jersey.

About a year and a half ago, my mom found me posting personal information on a social networking site. My photos, address, the school I attended was all up on Myspace.com for 7 billion people to see. I was oblivious at the time that it was not just my friends looking at my page, it was anyone who wanted to. So we got into contact with Parry and she came to my school and she did a presentation on Teenangels and Internet safety and immediately my friends and I wanted to help. We realized that what we were doing was unsafe and was not going to help us in the long run. So we wanted to reach out and prevent other kids from doing what we did.

So we went through a long training session. It takes about a year to become a Teen Angel and we are now Teenangels. We graduated after we became Teenangels. And now we go out to our high school and we form other chapters of the Teen Angel Program. And our main goal is to spread Teenangels to as many places as we can because the more people we have protecting kids, teens, and teaching parents and adults about the dangers of Internet, the safer the Internet will be. The Internet is everything nowadays. It is like your car. You know, you can go anywhere you want on the Internet and when it is used improperly, it can be a very scary place.

So I saw that there was a big problem with Myspace.com so my friends and I wrote a guide, a Teenangels guide to Myspace and it is all in chat lingo. You probably did not understand it, but it helped a lot of kids because it is a lot easier for teens to understand what you are saying when a teen is saying it to you. You know you do not want to listen to your parents, you know, oh, do not go with that, do not go on the Internet after 10:00. But if your friend is telling you how to be safe on the Internet, you will listen a lot more.

I really wanted to become a Teen Angel because I thought it was very important for me to reach out to those teens who are oblivious as I once was. A lot of teens I see are posting very explicit pictures of themselves on the Internet and they do not realize how that can hurt them when they make goals or when they apply for college. Something they did when they were 12 can come back and bite them. And it is very scary so if we reach out to them now, then things will be different in the future.

It is amazing how much Teenangels has impacted my life and other people's lives. As Parry said, I was nominated and honored by Teen

People as one of the top 20 teens who change the world. And when I met the other teens who had changed the world, it was an amazing experience because I realized that things I do just to help one person be safer on the Internet can help a lot more people.

YFly is a safe social networking site. I do have a Yfly. It is basically like any other social networking site except it is only for 13 through 18-year-olds. It is a step closer to preventing kids from getting in trouble on the Internet. As Teenangels, we work with many corporations such as AOL, Disney, Marvel Comics, Microsoft, Yahoo!, and Google, and we help them make the Internet and other interactive games and cell phones, make them safer.

We are all unpaid volunteers and we do this from the bottom of our heart. We want to help other teens. We are not just teens who want to make a difference, we are teens who make a difference.

Thank you.

[The prepared statement of Shannon Sullivan follows:]

PREPARED STATEMENT OF SHANNON SULLIVAN, TEEN ANGEL, WIRESAFETY

**Opening Statement:**

Thank you for inviting me here today to share information about Teenangels, WiredSafety.org and how we can protect everyone online. My name is Shannon Sullivan, and I am 14 years old from New Jersey. I have been a Teenangel for one year. I became one after my mother found out I had a MySpace.

I have recently been honored by Teen People Magazine as a representative of Teenangels for our role in helping change the world. That is a big challenge. But it is one that teens can live up to.

Teenangels are more than teens who learn how to use the Internet and other interactive technologies more safely. They are experts who advise many leading corporations. They have become well-known for their special insight into technology from a teen's perspective. Teenangels now advise major corporations on Internet and technology uses, including Disney, the CTIA, Microsoft, AOL, Yahoo!, Marvel and others. They assist law enforcement agencies in designing more effective undercover investigation methods. They work with large industry groups, such as the Motion Picture Association of America, in building educational programs and public service messages.

They have helped create safer interactive gaming technologies, safer cell phone features and more secure social networking programs. They have hosted briefings at the House of Parliament, conducted training for law enforcement agencies and written articles for leading magazines. They do presentations within their community for parents, students and senior citizens on safe use of the Internet and new interactive technologies. They spend a great deal of time on Internet sexual predators issues, anti-piracy and cyberbullying. We teach good cybercitizenship and responsible technology use, not only safety and privacy.

Teenangels are 13-18 year olds who train in all aspects of Internet and interactive technology safety, security and responsible use. (Tweenangels is the younger and lighter version of Teenangels, comprised of 9 to 12 year olds.) Once we are trained by Parry Aftab, leading law enforcement agencies and industry leaders around the world, these special teen experts create their own programs to teach safe and responsible technology use.

Some Teenangels are technological experts, creating animations, Flash applications, videos and computer games that help deliver their messages. Others concentrate on law and policy. Many have good public speaking, research or writing skills. The best thing about Teenangels is that it helps young people develop their own talents and help others at the same time.

We challenge teens and preteens, "Think you know more than most adults about the Internet? Share what you know, and learn more from the experts. Be part of the solution. Be a Teenangel!"

It is important that we teach young people that being safe isn't lame. That it's not cool to pretend you were out drinking all weekend, or to pose in your bra online. Many teens and preteens are lying about their ages to use social networking websites. And when they are there, they are often doing high risk things. But, it's important that parents understand that most teens and preteens are using the technology safely and responsibly. We just need to address them in our own language.

Recently, Teenangels began working with Nick Lachey. When Parry wasn't able to attend a luncheon with Teen People introducing me (she was in Spain launching her new book), Nick came instead. He learned that Internet sexual predators were using his name to lure teens into sending sexual pics online. Since he first met Parry he has donated his time to helping us keep kids safer. He is even helping us with public service announcements and a fun new animated educational series we are producing using Teenangels to teach safer and more responsible technology use.

Teenangels is now working with Nick's new site, YFly.com, to help create a safer teen social networking site. We helped create Don't Be Stupid to teach teens that engaging in reckless behavior online is stupid, not cool.

As Teenangels, we have the mission of helping make the Internet safer. We need your help to do that. First I would like to thank you for helping us by providing funding. We just received an earmark from Congress, through the Department of Justice, for \$50,000. Since Teenangels hold bake sales and wash cars to raise money for our programs, this will change our world. We cannot thank you enough!

Next, I would like to share our wish list and thoughts about what we can all do to help keep young people safer online.....

Thank you for your time and caring enough to hold this hearing. And thank you for taking the time to listen to teens. It's nice to be included. And I will remember this day forever. On behalf of all my fellow Teenangels and Tweenangels, thank you.

Shannon Sullivan, age 14  
Teenangels.org

**Appendixes*****Appendix A: (from Teenangels.org)*****Safety Tips From the Mouths of Teenangels**

(The Real Experts)...

While we have more extensive safety tip lists in Parry's book, here is a summarized version of the tips we thought were most important!

As Teenangels, safety is our biggest concern. So here are some tips and ideas that we and others have to share. Some of the best suggestions come from TEENS, just like you!

If you have a safety tip or story of something that has happened to you and how you handled it, please send it to us. We would love to hear from you! Email Teenangels.

Thoughts for Parents, Teens & Kids from the Teenangels

Parents... Don't be afraid of the Internet. It's an extremely useful tool & can't be dismissed because it is new & sometimes confusing. The Internet can be an excellent way for you & your children to bond & share a common interest. Be open with your kids & get involved. Most of all, learn all that you can about being safe, keeping your child safe, & taking advantage of the Internet's myriad uses. Tell your children not to be afraid to come to you with problems of any kind.

Teenagers...Although the Internet is a great way to meet new people, do research, and chat with friends, there are dangers. Be aware of these dangers. Always use common sense. Although you may think that bad things won't happen to you, they most certainly can. Be open with your parents about what you do online. Don't meet people offline that you met online! Make sure a site is secure and trustworthy before giving in your personal information. Obey the law and don't steal music, motion pictures and software! Balance the time you spend online and offline. Remember your friends in real life and don't take them for granted. Go outside & enjoy life beyond cyberspace.

Kids... While it's great to chat with people in kid-safe chat rooms online, you should spend time with friends in real life. School, family, & friends should always come before the Internet. Always tell your parents about what you do online. Let them sit with you, & teach them about the Internet. When they do sit with you, don't get mad at them. Just know they care about you & don't want to see you hurt in any way. Always remember that people online don't always tell the truth. Don't give out a lot of information about yourself. If anything bad ever happens to you on the Internet, always tell your parents or someone you trust. Always remember that it's never your fault.

**Appendix B: Don't Be Stupid!****For Teens:****Don't Be Stupid!****What you need to know about cyberdating and staying safe****The Downers:**

You never really know who someone is online. They may sound hot and their pic may be even hotter, but they could be someone you don't expect. They could be your little brother's snotty 12-year old friends

having fun at your expense. Or three 15-year old mean girls posing as a heart throb to set you up for humiliation. Or they could be some 47 year old pervert. Either way, who needs it?

And even if it is a cute 16-year old guy or girl, there is no guarantee that when things are over, that sexy pic you shared with them won't end up on some website or profile somewhere. Or they could use the password you shared with them to change your profile, pose as you and harass your friends or even lock you out of your own account. Or they could cyberbully, flame, cyber-harass or cyberstalk you or your friends...When you breakup, all bets are off!

**The Buck Stops Here...You Need to Protect Yourself Online**

Smart teens have been fooled by slimy adults posing as teens. There is no safe way to meet someone you only know online, (with maybe from a few phone calls to help), in RL. If you're thinking about meeting someone, think again. Talk to your friends. Check out [Katiesplace.org](http://Katiesplace.org) and learn about how others have been hurt by adults posing as teens. Smart teens like you. Don't do it!

We can't emphasize this enough! But, we also know that if you are convinced that this is a cute 16 year old boy or girl is the love of your life and destined for you from birth, you may ignore this advice and plan on meeting them in RL. If you are intent on taking this risk, do what you can to minimize it. Make sure you follow these Don't Be Stupid tips:

**1. Don't disclose too much personal info.** Start by assuming that the person on the other end is a predator. That means no full names, street addresses, RL schedules or telephone numbers that can be reverse searched (check it out online or where you work, or similar info about your friends that can be used to find you offline. It's always a good idea to use a disposable e-mail address or IM account, something you set up just for this and that you can drop if things start going downhill (like yahoo, hotmail or MSN.) Make sure that this new screen name doesn't give away any information about who you are in RL either (Tiff1991@[fill in the blank]).

**2. Play detective.** Photos can give away more information than you ever intended. Things in the background of the photo, like the license plate on your car, your house, the store where you work, the school or camp sweatshirt you're wearing or a pic with you in front of your school can be risky. So can photos posted by your friends. While you may be very careful about what you are sharing online, they may not be as careful. If you link to their profile and haven't told anyone where you live, but they post their best friends



(including you), everyone can now figure out what town you live in and where you go to school. They just need to cross-reference a bit. The same thing happens with everything you or your friends post. Look over your profile and the profile of your friends. If you were a detective for Law & Order, could you find yourself in RL? If so, change whatever is giving too many clues away. Password protect it and guard your password, and ask your friends to do the same. Start a rule - never post info about a friend or their pic without asking first.

**3. Say Cheese!** There are three issues about pics online - posting something you'll regret, shooting a lame pic or posting a pic that can be abused or misused by others. Sometimes to get attention, teens pose in provocative ways or snap a pic when they are doing things their parents would not want to see. Unfortunately, parents do see them. And so do principals and predators (and shortly college admission staff).

We all know that lame "MySpace" pose - bad lighting, cheeks sucked in, lips pursed, head tilted up, with a flash in the mirror. :-) Is that really how you want to be remembered?

Putting your best foot forward and using a good pic or a fun one is much better than doing the "I am so hot I can't stand it" pose. Boys posing shirtless and trying to make their pecs look bigger by crossing their arms underneath them, or girls posing in a bikini top (or worse) or very low cut pants will get you attention. But not the attention you may want. And cyberharassment where an innocent G-rated pic is manipulated and used to make you look bad or to morph your head on someone else's naked body is commonplace. You can avoid that by using photo-editing software to pixilate or blur the image, turn it into a sketch or cartoon, sepia or black and white. This makes your photos harder to abuse and less attractive to the harasser or a predator.

Our new Best Food Forward (BFF) tips teach you how to make the impression you want to make, without being lame or stupid. You can read about them at [Teenangels.org](http://Teenangels.org) or at our Don't Be Stupid tips at [YFly.com](http://YFly.com). These will help you come across the way you want to online.

**4. Look for the red flags.** Beware of others online who:

- ask too many questions
- post things that don't make sense
- move too fast
- promise you ridiculous things (if it seems too good to be true, it's not true!)
- like everything that you like, exactly the way you like it
- know too much about you
- engage in cybersex
- just don't feel right or make you uncomfortable
- are evasive
- can't keep their story straight
- initiate sexual conversation or innuendo
- don't know the things most teens know (just know the experienced predators make it their business to know these things)
- pressure you to send sexy pics or meet in RL
- give you the creeps

**5. ThinkB4UClick.** It's so easy to do things online that you would never do in RL. You don't have to look the other person in the eye. No one else is there to tell you to cool it. You are stronger, smarter, more empowered and braver online. You may not like your coach, principal or former best friend or boy or girl friend.

You take their pic and morph it onto someone else's naked body. You post sex ads using their name and contact info. Maybe you take a pic of them with your cell phone in a locker room, bathroom, at a slumber party or in the changing room at the Gap. You build a profile telling everyone what a slut they are, or post these pics online anonymously. Or you send sexual images of yourself to someone you like, thinking they will want to go out with you if they see how sexy you are. They don't, but share the pic with their fifty nearest and dearest friends - who show it to their friends and so on and so forth....

You think no one can find you, trace you or figure out who you are (you're wrong!). There is nothing between your impulse and your click...no time to think about it, no time to calm down. No time to use the "filter between your ears."

You are also typing fast and aren't proofreading your text-messages, IM or posts, and often send it to the wrong person on your buddy list or misspell their screen name. You may forget to type in "jk" or the word "not." You may find yourself in trouble without knowing why. Think R-E-S-P-E-C-T! (Now do it like Aretha, with lots of style!) Taking that extra second to make sure you send it to the right person, aren't misunderstood and are willing to be accountable for what you are doing and saying online is crucial. It will save you lots of grief later!

*Appendix C*

For Teens:

**Finding Love in all the Cyberplaces...Don't Be Stupid!**

If you decide to meet someone in-person, and ignore everything we taught you -- at least follow these tips and trust your gut. If something feels wrong, get out of there and report it. And remember that about 30% of the victims are boys. They just don't report it. So be careful!

**1. Go public.** Find out what they will be wearing and arrange for a place to meet. Then get there early and stake things out. The idea is to spot them before they spot you. Make sure that you meet in a well-lighted public place. It should be big and public enough so you can help if you needed it, but not so big, crowded and noisy that you wouldn't be heard or couldn't get help. Don't meet in an amusement park, where screaming is part of the scenery. A mall is a good choice, but sit back and watch and see who shows up. If they are not what was promised, run...do not walk...home, to the security office or to the local police department. Make sure someone calls the police.

Never meet at your place or theirs. Never get in a car with them. Go with lots of friends (preferably Sumo wrestlers). Ignoring these tips could cost you your life. Really. Several smart teens have been killed in the US over the last four years by people they met online. Don't become a victim.

**2. Bring backup.** If you are going to meet, bring a lots of friends (preferably big ones :-)), and someone where you are going. Leave information about the person you are meeting. The bad guys will try and get you to erase the e-mails or bring your laptop or hard drive with you, so they can destroy the evidence. Best case scenario, trust your parents or another adult family member. This has saved more than one teen from being kidnapped, raped or killed.

**3. Find your own ride.** Don't accept a ride from them or offer a ride to them...even if they appear to be cute and cuddly. Stay in control of where you go and how you are going to get there and back. Bring a cell phone and make sure it's charged. Have others check in on you too.

**4. Take it slow.** Even if that's not your style, make it your style for any cyberdating situations. Just because they have told you their favorite bands, movies and food doesn't mean you have any idea who they really are. Treat it like a first date. It will feel weird at first. You feel closer than you would on a first date. They will know lots of things about you that you have shared. Often very personal things. But start from scratch. Don't move faster than you are comfortable doing and don't feel pressured. Keep others around for awhile as you get to know each other and trust your instincts.

**5. Rat on the Creep!** Your parents will kill you if they found out you met someone from the Internet in RL. But if you don't report it to someone, this creep may kill some teen in reality! Most of the time when police arrest an Internet sexual predator, they find lots of e-mails on their computer threatening to call the police if they bothered the teen one more time. Had someone actually called the police, another teen might have been saved. Even if you won't tell your parents, find a way to report the creep. Check out [Katiesplace.org](http://Katiesplace.org) for ways you can do that and more safety tips and real stories about real teens.

copyright 2006, Parry Aftab, all rights reserved. For permission to reprint this, contact Parry at [Parry@wiredsafety.org](mailto:Parry@wiredsafety.org).

*Appendix D*

For Teens:

Finding a Better Faith

A fictional account...

I thought I had met my dream guy. I really did. Now, I see where my mistake was, sure. It was in believing what I saw in the movies and on television. Believing what I read in magazines about true love and soul mates. I believed in the Madison Avenue picture of love, romance and happily ever after, and glossy views of happiness and popularity. I was taught these things my whole life by my everyone I knew and from books, movies, and songs. I was told that if I were good enough, thin enough, charming enough, pretty enough, and exciting enough my life would be fulfilling, happy and exciting. But no one ever tells you how dangerous this blind belief can be.

When I was a freshman in high school, I was miserable. I lived in one of those towns where the same kids are in your grade all the way through school, so everyone gets to know each other pretty well. They knew me in middle school when I had acne and bad clothing and was shy and self-conscious. And then I grew out of that, but no one much noticed. I know I was pretty in the year or two before I died because people started noticing me – people who didn't go to my school, who didn't remember how I used to be awkward.

And it felt good. I felt different and happy and hopeful. I thought to myself that maybe now I would have a boyfriend. Maybe he just couldn't find me before because I was shy and awkward, and it'll definitely happen now that I'm in high school and all the older boys can see how pretty I had become in the last few years. But it didn't. No one looked at me any differently than they ever had and I got depressed. I thought to myself that high school might just be middle school again – that maybe nothing would be different and I would have to go through three more years of being lonely and waiting until something better happened. For a while, I got resigned myself to this fate and then something changed and I got up one morning and said no. I think I said it out loud, actually, it's kind of funny to think of now. I decided that I would say no to this fate – that I wouldn't be alone and I wouldn't be miserable – not anymore. I decided that I would meet someone and I would have a boyfriend within a month or two – do or die – that I would take my life into my own hands. And that I did.

I started going online and searching for people to talk to – people who would be more mature and would understand me. I sorted through people's profiles on Friendster and Xanga.com and set up my own. And then I met someone, and it was just as easy as I ever dreamed it could be. We IMed for hours, about everything and I felt, for the first time, that someone really understood me. Sounds pretty silly now. We talked about our families, our dreams, books that had changed us – everything. I thought I was falling in love. I knew I had found "the one." I was the lucky one, and had found my soul mate early.

When he asked me if I wanted to meet, at first I said no, that I didn't know him well enough. He didn't push it, and instead, we started talking on the phone. He had a very deep voice, which didn't surprise me because he said he was 18, but it probably should have. Anyway, a month later he said he had to meet me. He said he couldn't stand it anymore – that he loved me – and said that if I wouldn't meet him he would come find me because if he didn't see me he'd die. In the end, it didn't quite work that way, though.

I realized that my parents would kill me if a random guy showed up at the house looking for me. I couldn't have that happen, so I agreed to meet him. It was stupid, I know, but I was told more time than one that it's okay to do stupid things when you're in love.

I met him at the mall, in the food court. He was 37, not 18. I started crying and told him that he lied to me and I never wanted to see him again. I felt betrayed, and confused. He handed me the rose he had brought and a book of poems. I just stared at them, having problems separating the 18 year old I knew so well, from this man standing in front of me with tears rolling down his cheeks.

While he cried quietly, he told me that he loved me so much – that he knew I would never date him if I knew how old he was, which is true. I worked up the courage to leave. But he started making a big scene – pleading with me not to leave him. Telling me how much he loved and appreciated me, when no one else did. I was afraid someone I knew or who my family knew might see so I agreed – his last request – to go outside to talk.

He said he had a present for me in his car, and could he just give it to me. I said ok, probably the stupidest thing anyone's ever done. He clamped his hand over my mouth so no one could hear the screams. Then he pushed me in his car, throwing a blanket over me and holding me down so no one could see. He poured some smelly chemical over the blanket near my face. At first I held my breath, but finally had to take a breath. I knew I was in trouble, and felt dizzy immediately. I must have passed out. I don't know how long it was before I woke up, and realized this wasn't a horrible dream. It was real. He took me someplace in the woods, dragged me from the car and tied me up. He beat me, while he raped me, crying and telling me he loved me the whole time. I felt like my insides were being ripped out. That was how I lost my virginity. And my innocence. And more.

I still feel like its all my fault. Why did I believe him? Why did I believe that anybody normal could be that into me? Even after all this time, the only answer I can come up with is that I had believed in make-believe. If I hadn't wanted to fall in love so badly, if I hadn't needed someone wanting me to validate how I felt about myself, I wouldn't have let my judgment get clouded. I would probably be alone in my room, depressed, but I'd be better off than I am now.

So believe in happily ever after, but reality too. It's okay to be hopeful because life would be too hard without it. But don't let it cloud your better judgment. Have faith in yourself and don't waste it on people who may or may not love you or save you or complete you. And don't trust people – at least for a while, at least till you know who they really are and what they are capable of. And never just because you talk with them online and on the phone and think you know them. Love and loneliness don't excuse stupid behavior, and they certainly don't buy you another chance to fix it.

I will never know what could have happened in my life – who I could have met or what I might have done, because he killed me before leaving my body for some hikers to find weeks later. I was almost unrecognizable. My parents had to identify me, and the hair, clothes and complexion I worked so hard to make perfect weren't even identifiable anymore. I was ashamed that I had done this to my parents, and my little sister, and most of all to myself.

My friends didn't envy my "kewl" new life. They, instead, mourned me, and even my dearest friends talked about how "stupid" I was.

My little sister couldn't stop sobbing. She held my hand, and clung to the casket when they tried to take it out of the church. I tried to hold her hand back, but nothing happened. I wanted to reach out and comfort her. But from now on, she wouldn't have a big sister to do that anymore. She couldn't climb into my bed and tell me about her kitten and why she wanted to be "just like me" when she grew up.

I hope she wouldn't be just like me. I hope she is smarter than I was, and not as trusting. Not as naive

I wish I had a second chance. I wish I could warn others about this kind of thing. But I can't. I'm dead.

This "love of my life", my "soul mate" didn't only rob me of my innocence and any chance at happiness – I'll never know if I could have made it. I never got a fair shot. If

you're in the same situation I was in, I can't say if it'll ever get better, or if you'll ever be successful, or rich, or pretty, or lose the weight, or get the guy, but I can say you better hang around and try, because I'd do just about anything for the second chance. A chance to find someone real. A chance to know if I could have been happy.

*Appendix E***About Teenangels from a school technology director in Wisconsin:**

About 5 years ago, I got a phone call from one of the parents in our school district asking that her daughter's Internet and email privileges be revoked. She decided that her daughter would no longer be allowed to be part of the "Cyber World."

When I spoke more with this parent, I learned that the daughter had been harassed online. She had given out personal information and was now receiving inappropriate emails and phone calls at her home.

I immediately looked for resources online to help this family. The Internet is such an incredible resource – I wanted to find a way to convince the family that education regarding Internet use was a better solution than instituting a complete ban for their high school daughter.

As a result of my searches, I happened on information about Parry – I contacted her and she agreed to speak at a school assembly with a parent information meeting to follow. After Parry's talk, I literally had a line of students in my office – these students wanted to help other teens to be safe online. From that group, our TeenAngel chapter was started.

The Teens devoted an entire Spring Break to intensive training and the rest is history. Our TeenAngel chapter works to educate Teens (and parents) about online safety. We have a "Tech" division that works on programming and helps community members with problems ranging from P.C. trouble to instructions on virus removal.

Our teens are highly motivated and highly technologically savvy. Among other things, our group has attended the Wired Kids Summit in Washington D.C. working with legislators and corporate executives to help make the Internet a safer place for kids. One of our teens was featured on "The John Walsh Show" in their "Hometown Hero" segment. Locally, our teens have presented to numerous school, church, and parent groups as well as presented at state conferences focusing on issues relevant to Teens.

This is a great program. In our high school, it has become a place and program for our "Tech" guys to devote their energy and talent.



*Appendix F*

From Katiesspace.org, written by one of our Teenangels who wants to teach others how to avoid being victimized in the way she had been.

**When Your Mentor Becomes Your Tormentor - Alicia's Story**

You never notice yourself growing. It's so gradual, so smooth a process that the daily or even monthly changes are simply undetectable. Mirrors don't help – its only in comparing photographs, in seeing yourself at different stages, that one can notice the differences.

My relationship online with Mac grew just that slowly. When we were first introduced online, he was courteous and interested and subtle, none of those childish IMs which are so common, among young teens, flaunting their new-found sexuality like so many new toys. He didn't try to have cyber sex with me, didn't make crude comments or ask me to go on the webcam. It doesn't work like that. He was thoughtful and gentle and nice, and, of course, entirely deceptive, and so we became friends. Just friends. And it was all very innocent - for a time.

It was in the slowest, least noticeable way that he eased me into a more intimate relationship online. He was an expert, but, of course, I didn't know that at the time. The way the conversation moved into more personal territory never felt threatening because it moved so slowly. We would talk for a few minutes more each day, about something a little more personal each day, and some days we could talk about nothing personal at all. He never pushed, never insisted and so convinced me that I wanted to tell him personal things, or 'parrot' those things that he so wanted to hear from me. And I did.

So we talked about everything – not just the sexual stuff. He was interested in me, as a person – my thoughts, my goals, my relationships with friends and family members. He gave me adult advice and always took my side. He was my advocate, unconditionally, at a time in my early teenage life where that was just what I needed. School was: well it was school, mean girls and nasty boys and everyone trying to be all that they're not- And my family and I, were very close, but we didn't always see eye-to eye about everything, sometimes they just seemed to think that I was still a child. But there was always Mac, and I could count on him to see things my way Always online. Always ready to talk. Always on my side. It was the most comforting thing imaginable.

Soon enough, he wasn't just someone that I could trust, he became the someone I needed – I began to believe that he was the only one I could depend on to understand the real me, which is exactly what he wanted, of course. Somehow, in this process, this grooming of me, he had changed me, had destroyed my ability to reason. Imagine, I walked out the door, right out of my own front door into the darkest iciest winter night, with no money and no coat, to meet a madman who I thought was my best friend.

Was I crazy? No. Was I duped? Entirely. When I review it all, comparing my mental photographs of our relationship at different times, I think, how could it have happened? How could my sanity, my reason, my mental state have decayed like that – how did he make me shrink away to nothing? How could I have gone from being a smart, sane girl having casual conversations with an online friend to doing something I would have sworn I could never do –who... shy timid little me?—never!!!!- meeting a total stranger in the dark, cold night – leaving home in the middle of a happy, loving, family holiday meal? My only answer is that I wasn't crazy – I was just under the spell of an incredibly skillful manipulator who knew that slow and steady wins the race – or at least the hearts of young girls. He took me apart and put me back together and bit by bit, day by day, byte by byte, he became the focus of my life and the one who understood me best. Why wouldn't I want to meet someone like that IRL? It felt right.

And yet it was so wrong. The moment he persuaded me into the car, I immediately knew that I was in trouble. I knew. I had this terrible sinking feeling in the pit of my

stomach as we drove down my street, out of my neighborhood, and then, onto the turnpike. Trapped “Quiet” he said. “Let’s keep the trunk empty.” I kept my eyes cast down, stealing quick furtive glances up at him from the corners of my eyes. Somehow, I instinctively knew that he was like a savage beast, and that I had only to make full eye contact to engage his anger, to force him to attack. I stared down at his shoes as we drove. At his pants, his socks, I studied them, eyes cast down. I could describe it all to you today – that image, that feeling, trapped ...it will haunt me forever. Those hours sitting there, the waiting....

What terrible fate awaited me when we arrived at his home? I never envisioned anything as terrible as the reality. When we arrived at his home it was – worse than even I had imagined it could be. It was way worse than a bad after-school movie. It was Friday the 13th and Texas- Chainsaw-Massacre! And he had it planned – days before, maybe months before, maybe the first time we ever spoke. I was stripped, tortured, beaten. .... Raped. Those words still stick to the roof of my mouth and are glued thickly to my tongue. I listened through the windows to cars passing by, to the voices of neighboring families going out for lunch and to the mall and coming home again at night, yet there I remained, collar around my neck, chained to a post, naked. This was me at age 13. Waiting for death. How would he do it? Would he stab me, would I bleed to death, my blood adding yet another stain to the filthy carpet? Would he beat me to death with whips and fists, chained helpless, unable to defend myself?

Into this morbid fantasy, unbidden, a fairy tale that my mother had read to me while tucked warm and safe into my silken little ‘blankie’ kept flashing into my mind. The one of an Arabian slave girl held captive by her master. The tale unfolds that at the moment her stories ceased to entertain him, to amuse him - then he would kill her, with this in mind, the helpless slave fought for her life with the only weapon she had - her mind... And she became my inspiration. I would persevere, I would not die. My captor would not win this battle. I knew that my family loved me, that they would move heaven and earth to find me. But I had to stay alive until they did. So I struggled, silently, determined to win back the life I had left behind. My life that somehow had seemed to become so empty, so sad... why? I understood now, in those cold hours alone, waiting for the monster’s return, it all began to come clear. I wanted my life back! I wanted to feel my mom’s gentle kisses good-night and my dad’s crushing hugs, I wanted to run outside into the sun, to add my voice to the other happy children’s, far, far away from the dark coldness of his dungeon. I wanted to experience anything – anything - except what was happening to me. I desperately wanted to live!

So I waited it out. I prayed. It might not seem, to you, like the most courageous thing to do – I didn’t fight him, didn’t engage his anger. But, somehow, I knew that he would kill me, throw me away like trash in some cold shallow grave if I resisted anymore. He enjoyed my pain. So, I just wasn’t there I left – mentally anyway. This wasn’t happening to me. I escaped into my head and tried desperately to hang on to my sanity. It took my whole being to merely breathe. One breath at a time I waited for my death. I knew that one wrong move would cost me my life and so I simply waited, telling myself “today, yeah today they’ll find me... rescue me,” convincing myself that this would not be how it all ends, that my parents would not find their only daughter’s dead and battered body in this evil man’s filthy house. I couldn’t, I wouldn’t, let it end that way. So I resolved to live. Breath by breath. Moment by moment.

And I did. I made it through, a miracle of survival, when so many other girls have been less fortunate. And I can’t say if it was faith, or luck, or personal resolve that saved me. And it doesn’t really matter. I truly feel that something greater than myself has directed me. I am alive. I was given the second chance that so many others had been denied.

I promised myself in those dark and painful days and endless nights that if I were spared, if I were given a second chance at life, I would share my horror, to teach others -

maybe you - how to avoid becoming his next victim. I would help them understand that the mentor you thought you found online might become the tormenter who steals your heart, your innocence and your faith in mankind. And ultimately, **your life**.... Mac failed. While the emotional and physical scars may last a lifetime, he didn't shake my faith in myself or in mankind. He may have stolen days, weeks, months, he may have taken my childhood, but the rest of my life is mine. And I have reclaimed it. I will not allow him to torment me anymore. Only I have the power to control my future. I refuse to be defined by his betrayal of my trust, by his cruel sadistic acts or by those dark days, however devastating they may have been. I have a mission and an important role to play. I want to inspire others to move on, past their exploitation, to find their own life mission. I was spared and given a second chance. And I don't intend to waste it. I will continue to speak to young people and dedicate my life to helping catch criminals, like Mac. I am also helping, here, to build KatiesPlace.org and as a volunteer with WiredSafety.org and others.

So, please don't remember me as the girl who was torn, twisted, confused, lured abducted and abused. Remember me for what I will accomplish. Please don't let this tragedy define me. I am so much more than that. And so are you. Join me in this mission. Together we can change the world, one child, and one life at a time. You can read about miraculous rescues and the dedicated and courageous men and woman responsible for bringing victimized children to safety here at KatiesPlace.org. And you can e-mail me through this site. **Please, be safe...be aware...**

MR. WHITFIELD. Well thank you very much Ms. Sullivan, we appreciate your testimony and look forward to asking you some questions later on.

Mr. Sallam, you are recognized for 5 minutes for your opening statement and thanks for being with us today.

MR. SALLAM. Thank you, sir.

As you know, my name is Moni Sallam. I am a ninth grader at Riverdale High School in Howard County. The Internet has opened up a new world of opportunity and dangers for kids today. On the plus side, we have instant access to any information, music, cultures, and opportunities that probably would have taken you months to access if at all when you were a kid. On the negative side, kids can talk to anyone they know or do not know at any time of the day or night. Kids are contacted on a daily basis by people they do not know. School bullies do not just find you at recess, they taunt you at any time of the day or night and they get others to join in too.

The major problem is that due to a lack of education, kids make bad decisions while online. Kids give out their personal information, they share pictures of themselves with people they do not know, and they download music illegally. That is the reality of kids today. Online predators know this and use the Internet to lure kids to danger.

It is all about education. Just like other safety issues like bike and water safety, education is the only way to help kids behave responsibly online. A perfect example is if you ask kids or teens if they would ever get into a car with a stranger, probably 100 percent of them would say

no. The reason is that we are told from the time we are old enough to play outside never to talk to strangers, never to get near a car with strangers. Kids know to look both ways before crossing the street. They know to wear helmets when riding a bike because we are taught these things from an early age. On the other hand, if you ask kids or teens if they would ever meet a stranger in person who they met online, an alarming number of them would say they saw nothing wrong with it.

Although informed people know that the Internet is a new way predators lure kids to danger and there are plenty of examples of tragedies that have happened to kids who met predators online. In my county alone, predators have been arrested for pretending to meet kids and trying to lure other kids to meet them. This is happening across the Nation. Internet safety education from an early age is required to change attitudes and behavior. Internet safety education is key to changing if you are going to be online. That is why i-SAFE is doing an amazing job. i-SAFE empowers kids like me with the decision tools we need to keep us safe and act responsibly online.

Thank you.

MR. WHITFIELD. Thank you, Mr. Sallam. How old are you by the way?

MR. SALLAM. I am 14.

MR. WHITFIELD. Oh, yeah.

And Ms. Sullivan, you have graduated from high school or--

MS. SULLIVAN. No, from grammar school. I am 14 also.

MR. WHITFIELD. You are 14. So having--

MS. AFTAB. Very articulate.

MR. WHITFIELD. Yeah, I almost felt guilty asking them how old they were after our subject matter here today, but how did you two come in contact with WiredSafety and i-SAFE? Ms. Sullivan, how did you become aware of WireSafety?

MS. SULLIVAN. Well my mom is a computer teacher at the grammar school I attended and she got in contact with Parry and Parry came to my school to do a presentation on Internet safety because a lot of my friends were posting personal information on the Internet using Myspace.com. So once she came, she told us very frightening stories about kids who listed personal information, who talked to strangers on the Internet, and she made us aware of the dangers that we were putting ourselves in.

MR. WHITFIELD. So were you shocked from what she said?

MS. SULLIVAN. I was sitting on the edge of my seat.

MR. WHITFIELD. Were you?

MS. SULLIVAN. Yes.

MR. WHITFIELD. Do you feel like or do you or some of your friends maybe had been contacted by predators but you had not really proceeded with them or--

MS. SULLIVAN. None of my friends have but I have many stories of people who have so I think that is why it is our job to aware these teens of what they are doing and how to keep themselves safe.

MR. WHITFIELD. And did you make contact on the Internet with people you really did not know or--

MS. SULLIVAN. No, I only used the Internet to talk to my friends.

MR. WHITFIELD. Okay. Mr. Sallam, what about you? How did you become aware of i-SAFE?

MR. SALLAM. I first became aware of i-SAFE when I was in seventh grade. I was watching TV actually and I happened to come across an i-SAFE professional development program just like Ms. Schroeder talked about in her presentation. And I watched it and I just realized that this is a huge problem and it could affect people that I know. And I was actually first worried about how my sister would be reacted by this big issue.

MR. WHITFIELD. Do you think that any of your friends or classmates have viewed child pornography online?

MR. SALLAM. No, sir, I do not think.

MR. WHITFIELD. You do not.

Ms. Schroeder, I know that you all have been quite successful in Kentucky with these programs that you have talked about and it is my--is it--am I correct that you are teaching this program now in every school district in Kentucky or is that right?

MS. SCHROEDER. Yes.

MR. WHITFIELD. Now how were you able to accomplish that and how many other States do you teach in every school district in the State?

MS. SCHROEDER. What we did this past year was Microsoft actually provided funding for us and we took our professional development online so we created I-learnonline and they provided funding for the professional development for educators, as well as the youth for the mentor side and they are just now providing funding for the parents, as well as for 50 plus. So what happens is, the way that we are able to do this now is that educators on their own can actually go in and review our module. And when they are through completing the module, they get professional development credit and then a gateway opens up and they have access to all the curriculum and the activities, the workbooks for the kids electronically.

MR. WHITFIELD. Well we thank you for the great job you are doing in Kentucky and elsewhere and how old is i-SAFE? How old is it?

MS. SCHROEDER. We were formed in 1998.

MR. WHITFIELD. Ninety-eight, okay.

And Ms. Aftab, how do you identify students to be Teenangels? How do you go about that?

MS. AFTAB. The Teenangels identify themselves.

MR. WHITFIELD. Okay.

MS. AFTAB. They share a belief that every child has something to offer. And when they see me on television, if I do Dateline or Good Morning America, or something often the kids will see that. We are in magazines. I do eight interviews a day sometimes. And so when kids see us or they see us in person or they want to make a difference, they will reach out to us. The program is free along with everything else we do. We who run it are also unpaid volunteers. I have one of them from Stone Ridge School here in Bethesda, Maryland, who is sitting back there with one of her Teenangels. The training is we email it out to them and help them do it and the kids come to us. And what we find is some kids are really great at public speaking. Others may be shy but they are terrific at research. And part of Teenangels, Teenangels is a little different from I-Mentor in that the kids who are Teenangels have to undergo extensive training and independent research. They have actually developed new product. They have to go out and research new interactive devices. They developed safer cell phone settings that are now being adopted by Disney. They have come up with safer interactive gaming for X-Box Live. So when they learn and we have all of the experts teaching them about everything they need to know, they develop things.

The Motion Picture Association of America honored one of my Teenangels who came up with a 30 second PSA--he is 15--called use it and lose it. It's about bringing your video camera into a movie theater and what is going to happen. This 15-year-old had social anxiety disorder and his mother came to me and asked if he could be a Teenangel. And I said well we work in chapters generally but she asked me if would make an exception and he has done extraordinary things. And a young girl from Pittsburgh who is 13 who had met an Internet sexual predator in their live, who was rescued 4 days later by the FBI where she was found chained to the floor, came to us and she wanted to be a Teenangel too. So the kids who come to us and want to make a difference, we give them a way to do it.

MR. WHITFIELD. All right.

Ms. Schroeder would you or Mr. Sallam explain the mentor program at i-SAFE?

MS. SCHROEDER. What happens with the mentor program is they actually go through a training. We have our own mentoring network.

And so what the kids actually learn to do is they become a little bit different than what the cyber angels do because this is--

MS. AFTAB. Teenangels.

MS. SCHROEDER. I am sorry, Teenangels. This is in school. So for instance as you saw with the Kentucky kids, high school kids, they will actually get service learning credits. We have service learning curriculum and they actually decide to adopt a class and they will actually go in and train that class and/or they may go into a lower division school and then they work the kids for the younger kids say K, first, or second grade and they may go in and do learning with them because we have a literacy curriculum as well. So there are various things that the kids can do from peer-to-peer in terms of being able to help promote Internet safety. We also have school assemblies so the kids actually participate in the school assemblies.

MR. WHITFIELD. And how many mentors are there around the country?

MS. SCHROEDER. Right now we have 156,000 I think that are actual certified mentors.

MR. WHITFIELD. One hundred fifty-six thousand?

MS. SCHROEDER. One hundred fifty-six thousand that are certified mentors. Now those are, the certified mentors, are the ones that actually conduct the training.

MR. WHITFIELD. I see.

MS. SCHROEDER. So every single student that goes through the curriculum, they actually become mentors because it is part of the curriculum that they do in the classroom.

MR. WHITFIELD. And how many Teenangels, Ms. Sullivan or Ms. Aftab?

MS. AFTAB. We are a different program. Ours is a train-the-trainers program so the Teenangels reach out and train others.

MR. WHITFIELD. Okay.

MS. AFTAB. We have 450 certified Teenangels who are the right age right now, a lot of them have grown up. And we have about 3,400 in the pipeline. Until recently, I had actually hand-trained all of my Teenangels. It was the most fun I have had. Now their training is put onto CDs so that anywhere we are not, the Teenangels can. And we are working with the scouts and with other organizations. In fact, we have got a new Teenangels chapter that is starting with Camp Fire Girls and Boys in Anchorage, Alaska.

MR. WHITFIELD. Really?

MS. AFTAB. Yeah.

MR. WHITFIELD. Do you operate in other countries as well?

MS. AFTAB. Seventy-six countries around the world.

MR. WHITFIELD. And what about i-SAFETY?

MS. SCHROEDER. Fifteen countries and schools.

MR. WHITFIELD. Okay. And how many Teenangels are back here in the corner this morning?

MS. SCHROEDER. One and one want to be.

MR. WHITFIELD. One and one want to be, okay. Well--

MS. AFTAB. They have to miss school to do this. But they are now. The interesting thing is they are doing hard consulting for big corporations. They are working on the inside with Myspace and Facebook and with Yahoo! and Google and Disney and Microsoft where they are helping advise on new product and ways that they can be misused and used by kids.

MR. WHITFIELD. So all of our mentors and Teenangels, they are all quite proficient and we know they will do well in whatever they decide to pursue.

MS. AFTAB. And we are lucky to have them.

MR. WHITFIELD. Yeah, absolutely.

I want to thank you all for the great job that you are doing for these programs and the good work that you are doing. And particularly want to thank the Teenangels and the mentor and mentors for their assistance you are doing with other students.

And at this time, I recognize Mr. Stupak.

MR. STUPAK. Thank you.

Ms. Sullivan or Mr. Sallam, what do you feel these sites--Myspace and there is another one we saw today Spotlife and Buddypicks--now what do you think of those as a general rule? Are they useful or helpful?

MS. SULLIVAN. They are a good way to keep in touch with your friends. Many teens are enticed by social networking sites because you can make it all about you. Sites like Myspace, you can change the background to whatever you want, whatever font you want, you can put funny pictures, you can put pictures of yourselves and your friends, you can comment on your friends' pages. It is very teen orientated. So they really enjoy it. It can be useful because it is different than just IM you friends it is more like staying in touch with your friends, more extensive, but they can be misused. You can post personal information.

MR. STUPAK. Well, do you think the benefits outweigh the risk?

MS. SULLIVAN. Excuse me?

MR. STUPAK. Do you think the benefits of these sites outweigh the risk?

MS. SULLIVAN. No, I do not. There is too many risks because many--

MR. STUPAK. Then why have them?

MS. SULLIVAN. Because--



MR. STUPAK. I mean you are the experts. I mean I have never been on the Internet and I could not tell you from the bottom, but I guess I am just trying to get your own feelings on it because it has been a tragic story what we have heard about today and unfortunately it is being repeated time and time and time again in this country and more offshore and everything else. So I just want to learn the value of these sites and if we cannot monitor them or police them better than what we are doing.

MS. AFTAB. And how can you use them safely I guess.

MS. SULLIVAN. Yeah. It depends how the teen or the child is using it.

MR. STUPAK. Sure.

MS. SULLIVAN. If someone has their profile set on private for only their friends to see and they are not talking to strangers or people they do not know, then it is safe. It is a good place for them to be. But otherwise if they are letting anyone who has a myspace or commenting, people they have never met, and people they never will meet, then it can be dangerous. So it depends on how you look at it. If you see that your child or teen is being safe on it and they are using it to contact their friends then it can be safe and it does have benefits. But otherwise, if they are posting too much personal information and they are talking to people they do not know, then it is dangerous.

MR. STUPAK. So I bet you a month does not go by here where there is an embarrassing email that came out of some office here. The issue is not when the sender sent that email to the other office probably thought it would go no further but somehow inadvertently, however, it gets sent all over and suddenly my privacy is everybody's public knowledge and not only is it embarrassing for the office that originated the email but it just, I think sort of reminds us that what we may think and what we believe and sitting behind that desk and doing your emails or going to your myspace, while we think it is private, it is really not and that is why I think we are all vulnerable and not just young people and us too with our emails. So I was just wondering about that.

Mr. Sallam, let me ask you this, the Chairman asked you and you sort of said no but these porn sites, there has been gregarious talk about sitting home or you are surfing the net. Do you have discussions with your friends about the fact porn sites are out there? As you surf you may hit them, things like that?

MR. SALLAM. That is a tough question.

MR. STUPAK. Yeah, I mean what I wanted to get at is--

MR. SALLAM. When you are surfing the Internet, the fact that stuff is out there and we do like stumble upon it and it is especially with myspace like some people post pornographic images on their myspace so

it is sort of people who have Myspace, it is sort of easy to stumble upon something like that.

MR. STUPAK. Do you talk about it with your friends?

MR. SALLAM. Not really.

MR. STUPAK. Couldn't that be a deterrent in the programs you are doing? I mean, we all know they are out there, acknowledge they are out there and discuss it, why you are not to go there and the dangers involved in it?

MR. SALLAM. Yeah, of course there is always a bad aspect of looking at these pornographic images, the factor of getting a virus, but it does not really come up in discussion with my peers.

MR. STUPAK. Okay. Ms. Schroeder, would you submit the FCACY study on the i-SAFE Program? I would be interested in learning a little bit more about that. And you said it has been around since about 1998. Has there been some studies as to the effectiveness of the program?

MS. SCHROEDER. Yes. MIJ did a 2 year study on i-SAFE and they presented it to me about 2 months ago so, absolutely, I will request that study.

MR. STUPAK. The 2 year program you said or 2 year study, I am sorry, has there been anything else who have measured the effectiveness of i-SAFE?

MS. SCHROEDER. Well we do pre-polls and delayed assessments and actually we have our national assessment center so we are providing assessment data. We even provide it to the FBI because we do trainings for them as well and I would be happy to provide that to you.

MR. STUPAK. You mentioned the FBI, do you work with local law enforcement and things like--

MS. SCHROEDER. Yes, we do. We have--

MR. STUPAK. There is at least one more. Maybe three more. It looks like a new agenda, three more. Okay.

MS. SCHROEDER. We have our i-SAFE Task Force and our i-SAFE Task Force actually is a partnership with local law enforcement, FBI, the Attorney General's office. School resource officers from around the country actually are trained and they participate, as well as FBI and their outreach department, so they are actually teaching the classes, as well as in schools.

MR. STUPAK. In your testimony, I think you mentioned something about 30 minutes once a week for 5 weeks. Do you have any follow-up with that because I would think there may be more to this?

MS. SCHROEDER. Yes, we do.

MR. STUPAK. Well what is that? What does that consist of follow up?

MS. SCHROEDER. What happens is is that the classroom curriculum actually is comprised of a 30 minute segment because you have to fit it into a class day. So once it is implemented into a school district and/or a classroom, it really is up to that teacher in terms of that. We create and we have five core modules and then we have supplemental modules. So what the teachers usually do is they always do the five core modules and then after that they go and they do the supplemental modules. The way that we follow up with them is the fact that we are always supplementing the information. For instance when cyber bullying came out, we created a cyber bullying curriculum. So they go online, they request that curriculum. It has its own life within that school district in terms of its being taught all the time. And then students too as well, they have their school assemblies that they are doing as well and then that involves, they will bring local law enforcement in and we have our parent nights.

MR. STUPAK. Okay. You just mentioned cyber bullying again. Explain that for us for the record so we know what is cyber bullying.

MS. SCHROEDER. Yes. What that is is you know you would be bullied on the school grounds? Well now what kids have done is they have taken it online. So for instance if I am a student and I have something to say about you I will blog it or I will go and maybe post different pictures about you, crop them, then I will go and call attention to them. So for instance for me as a student when I come back to school the next day everybody knows about it not just a few kids that on a school ground it would just be one on one. One situation that was such a tragedy was a student in Vermont and actually his father was an IBM executive and they contacted us. IBM did and said this is what is happening to one of our executives and that is when we really looked into this. In this particular situation, this boy was bullied at his school, it then went on and on and he ended up taking his own life. Ms. Teen New Jersey who is a spokesperson for us, her parents moved her three States when she was bullied online as well.

MR. STUPAK. Okay. You are also promoting the digital certificate technology for children.

MS. SCHROEDER. Correct.

MR. STUPAK. And one of the requirements to obtain such a certificate is they have a government-issued photo ID, do I understand it? Do many students have such a photo ID? I do not usually think that the school IDs are accepted as a government ID cards or government-issued ID cards. Where would students use them?

MS. SCHROEDER. The way that this technology works is it is called the i-STIK.

MR. STUPAK. Okay.

MS. SCHROEDER. On the first day of school when parents actually sign the acceptable use policy, they will say yes my son or daughter can have an i-STIK. So next to biometrics it is actually authenticated there at the school.

MR. STUPAK. I see.

MS. SCHROEDER. So we did a study with ten States and most kids took their i-STIK and went to the school administrator, they had their ID there, they knew that that was Susie Brown and Susie Brown was issued that i-STIK and so that, it is just very simple. It is actually like an ATM card. It can be used anywhere on the Internet. Right now it is empowered by VeriSign and also eBay; Yahoo! was actually participating in this study as well. And we are looking at this being a place where if you are a student, you would be able to go to these areas online and it would be able to authenticate you so it only knows in terms of male, female, age range, and demographics in terms of West Coast, East Coast.

MR. STUPAK. And that is a pretty safe, secure site so no one can access this information?

MS. SCHROEDER. Well, the goal is that you are educated so when you are actually getting into an area if I am going to go chat or communicate, then it will only allow other people within those parameters to chat or communicate with me. So it really empowers the students quite a bit because now they choose where they want to go.

MR. STUPAK. Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you, Mr. Stupak.

I am going to just ask one other question of Ms. Aftab and then we will conclude the hearing. But and you had a lot of experience with this. You were a lawyer prior to getting involved in WiredSafety. And do you find that parents' perceptions of what their children are doing online differ significantly from the reality of what their children are doing online?

MS. AFTAB. Yes, and Mr. Chairman, I have actually written all of the leading books for parents on Internet safety in the United States and around the world. And WiredSafety, the volunteers before me have been doing this for 11 years so it was a long track record here. Parents are clueless, totally clueless. And even the parents who use the Internet are clueless. And it is interesting, we have been talking about this for years and I will go out and I address 1,000 parents a month and 5,000 students myself in person and every single month, and when I go out to them, the parents keep saying not my kid. And I say your kids are communicating with strangers, no. Twenty-four percent of the teens that were polled by family PC magazine, teen girls admitted to meeting strangers off line that they met online, 24 percent. And 60 percent of the survey that we did

with the University of Southern Florida in 1999, 60 percent of the teen girls, 11,000 teen girls between the ages of 13 and 16 engaged in cyber sex, admitted to it. One of the girls said that she would not, she had cyber sex but she did not go all the way. I always joke, that means she did not use punctuation. But these kids are doing this because they can and the parents have always said not my kid. And then Myspace became popular. And Myspace has put fear in the hearts of parents everywhere and I think it is seriously overblown. They have the most liberal law enforcement, pro-law enforcement policy on the Internet today. So they get it but the parents do not. So now the parents are saying not my kid, my cherubic 13-year-old, 14-year-old would never do those things and they go onto their site and they see them posing in their bra, or licking their lips and arching their back and they are thinking oh my goodness. And a lot of these kids who are home coloring with their 5-year-old niece over the weekend are pretending that they were out drinking last weekend. So they are not really a drunken slut, they are just playing one on Myspace. And their parents have no idea. And so what we now need to do is awaken parents, get them to open their eyes at the same time they do not throw out the Internet which all of our children need. We have hearings about the dangers online and the terrible things that can happen to children but the greatest single risk our children face in connection with the Internet today is being denied access. We have got a solution for everything else.

MR. WHITFIELD. Ms. Aftab, I thank you very much. And Ms. Schroeder for the good work that you are doing. And Ms. Sullivan and Mr. Sallam, we really appreciate your being here and the great leadership that you are providing.

Before concluding, I would ask unanimous consent that we enter into the record the letter from the Department of Justice from Mr. Ryan regarding Justin Berry's--both letters to and from. And oh, yes, Ms. Schroeder, we would like to put your overheads in the record as well. Do you have problem with that?

[The information follows:]

**manatt**  
manatt | phelps | phillips

**Stephen M. Ryan**  
Manatt, Phelps & Phillips, LLP  
Direct Dial: (202) 585-6550  
E-mail: sryan@manatt.com

March 28, 2006

**BY FACSIMILE AND MAIL**

Andrew Oosterbaan, Esq.  
Child Exploitation & Obscenity Section Chief  
United States Department of Justice  
Bond Building  
1400 New York Ave., NW  
6th Floor  
Washington, DC 20005

**Re: Justin Berry and the Status of the United States Department of Justice's  
Investigation and Prosecution of Gregory John Mitchel, Timothy Ryan  
Richards, et. al.**

Dear Mr. Oosterbaan:

I am writing to raise a concern about the Department of Justice's failure to consistently communicate with Mr. Berry regarding the status of the Department's cases against Gregory John Mitchel, Timothy Ryan Richards and other individuals identified by Mr. Berry. Mr. Mitchel, Mr. Richards, and others, sexually victimized Mr. Berry. Mr. Berry risked his safety, and that of his family members, when he voluntarily came forward to the Department to disclose the existence of websites that permit pedophiles to prey on underage children and the identities of the adults who managed and profited from the websites and their counterparts, the adults who paid for subscriptions to these services. As you are well aware, Mr. Berry was himself a victim of many of the pedophiles, such as Mr. Mitchel, whom he has identified to the Department.

We understand that Mr. Mitchel agreed to plead guilty to all charges in January of this year. Normally, a step in the Department's case against Mr. Mitchel would be a sentencing hearing. The normal process for such a sentencing hearing would be to obtain and present victim statements from persons such as Mr. Berry. However, to the best of my knowledge, there has been no communication between the Department and Mr. Berry regarding the status of Mr. Mitchel's sentencing or a request for a victim statement from Mr. Berry. I recently pulled the docket sheet for the United States District Court for the Western District of Virginia and was dismayed to discover that Mr. Mitchel's sentencing hearing is currently scheduled for April 12, 2006.

**manatt**  
manatt | phelps | phillips

Andrew Oosterbaan, Esq.  
March 28, 2006  
Page 2

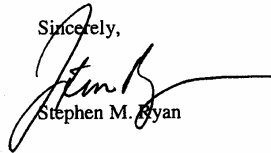
In September 2005, the Department acted on the information provided by Mr. Berry when Mr. Mitchel was arrested. The totally improper and unnecessary unsealing of the Federal Bureau of Investigation's agent's sworn affidavit, and a local reporter publishing a story on the arrest of Mr. Mitchel and the contents of the affidavit, disclosed information which was used to identify Mr. Berry as the source of the Bureau's information. This misstep created serious concerns for Mr. Berry. Given that the Department of Justice permitted this, perhaps the Department could assist Mr. Berry in providing information the District Court judge would undoubtedly find useful about Mr. Mitchel that is uniquely known to Mr. Berry.

Mr. Berry has continued to cooperate with the Department and provide it with any information requested. The Department, on the other hand, has not kept Mr. Berry appropriately informed on the status of these public matters.

Given Mr. Berry's degree of cooperation, I hope that the Department would step up its level of communication about the status its prosecution of individuals identified by Mr. Berry.

Please see whether Mr. Berry's statement can be placed in the court's records for Mr. Mitchel's sentencing hearing. I look forward to discussing possible solutions to the other issues raised in this letter.

Sincerely,



Stephen M. Ryan

4-03-06 16:05 From-CEOS

202 514 1793 T-179 P.002/003 F-871



U.S. Department of Justice

Criminal Division

---

*Child Exploitation and Obscenity Section**1400 New York Avenue, NW  
Suite 600  
Washington, DC 20530  
(202) 514-5780 FAX: (202) 514-1793*

APR 3 2006

*By Facsimile (202-585-6600) and U.S. Mail*

Stephen M. Ryan, Esq.  
Manatt, Phelps & Phillips, LLP  
700 12th Street, N.W., Suite 1100  
Washington, D.C. 20005

Dear Mr. Ryan:

Thank you for your letter of March 28, 2006, regarding contact with your client, Justin Berry, and your concerns that the Department of Justice has failed adequately to communicate with him about the status of our ongoing cases against individuals about whom he has provided information. As outlined below, however, we believe that we have made substantial efforts to keep Mr. Berry appropriately apprised, and we will continue to do so.

It is my understanding that you have allowed the case agent, Special Agent Monique Winkis of the Federal Bureau of Investigation, to directly communicate with Mr. Berry. If that understanding is incorrect, please let me know as soon as possible. Special Agent Winkis has advised that she has had regular and recent contact with Mr. Berry and has informed him about both Mr. Mitchel's guilty plea and the pendency of his sentencing proceedings, although she does not believe that she provided Mr. Berry with the precise sentencing date. I regret that Mr. Berry may feel that he has not been timely advised of the sentencing date, which, as you note, is April 12, 2006.

You ask that the Department of Justice assist Mr. Berry by providing the District Court his statement for use in Mr. Mitchel's sentencing hearing. We are committed to ensuring that the District Court has all the relevant facts before it decides on an appropriate sentence, to include Mr. Berry's victim impact statement, whether oral or written. We look forward to working with Mr. Berry to facilitate putting this information before the District Court. The prosecutors and agents involved in this case have devoted substantial resources in following up on other important leads from this investigation. The prosecutors assigned to the Mitchel case will soon be contacting Mr. Berry to prepare for the sentencing hearing.

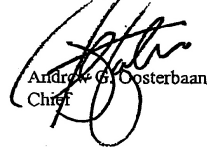


I also want to ensure that Mr. Berry is fully apprised of any other victim/witness resources that might be available to him. The FBI has advised that, in August 2005, Special Agent Winkis provided Mr. Berry with a list of victim/witness resources in his area that he could contact for assistance, and it is our understanding that Mr. Berry then advised that he would avail himself of these resources if he chose to do so, but he did not want Special Agent Winkis to share his current address with anyone. Accordingly, we have not contacted any resource or service on his behalf. If you think we should discuss these resources with him again at this time and in more detail, we will be happy to do so.


Finally, with respect to the unsealing of the affidavit in the Western District of Virginia, the prosecutors involved had obtained a sealing order in the case and confirmed with the Clerk of Court on the day after the initial appearance that the affidavit was not unsealed and would remain sealed for thirty days. For reasons that remain unclear to us, the affidavit was unsealed the following day. We very much regret that this occurred. Moreover, we took seriously your concerns that the unsealing could potentially endanger your client, and immediately offered to provide any assistance you believed necessary to ensure your client's safety. To date, it is my understanding that your client has declined our offers. Please be assured that these offers remain open and we remain committed to taking appropriate steps to keep Mr. Berry secure.

I hope this information is helpful. I appreciate your writing to raise your concerns, and look forward to continuing to work with you as we move forward.


Sincerely,



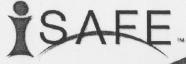
Andrew G. Oosterbaan  
Chief



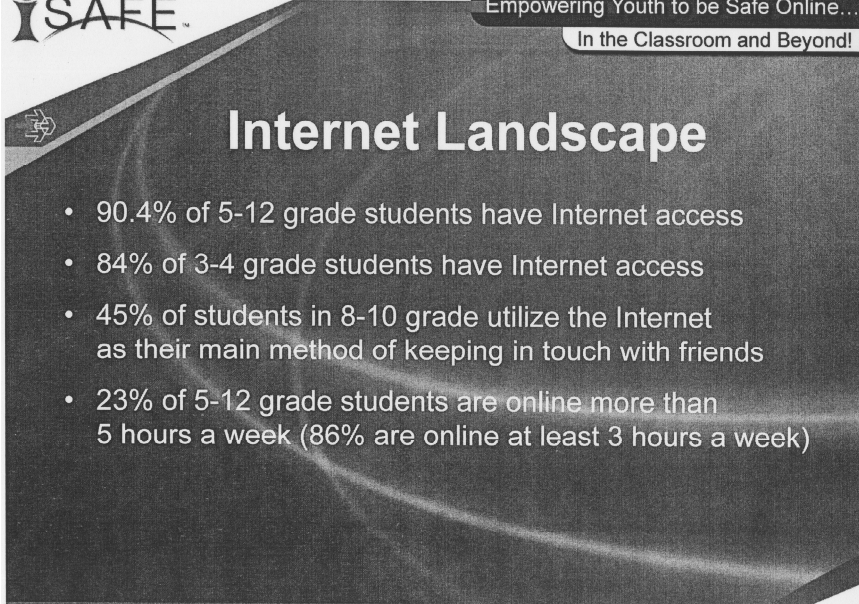
Empowering Youth to be Safe Online...  
In the Classroom and Beyond!



## i-SAFE Safe Schools Initiative

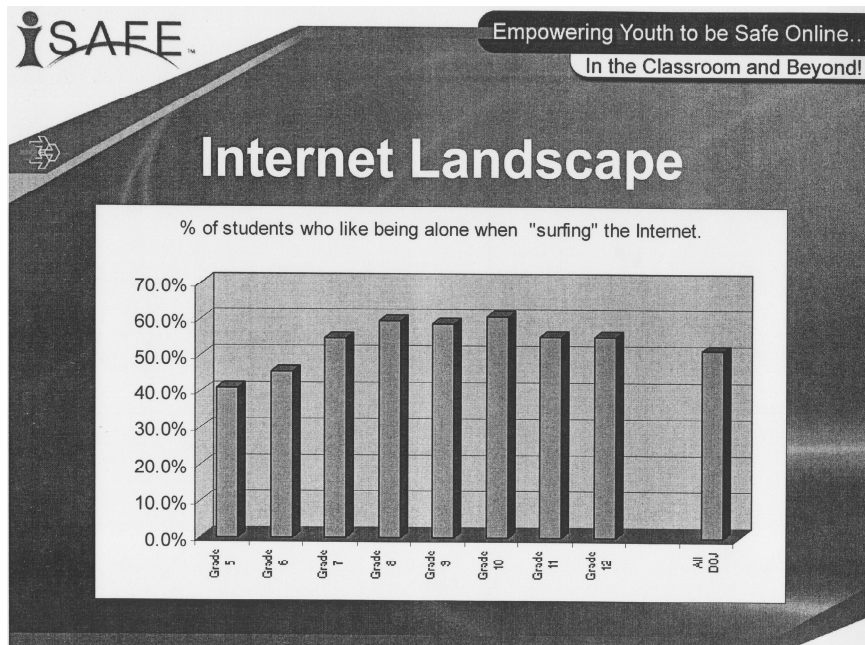


Empowering Youth to be Safe Online...  
In the Classroom and Beyond!

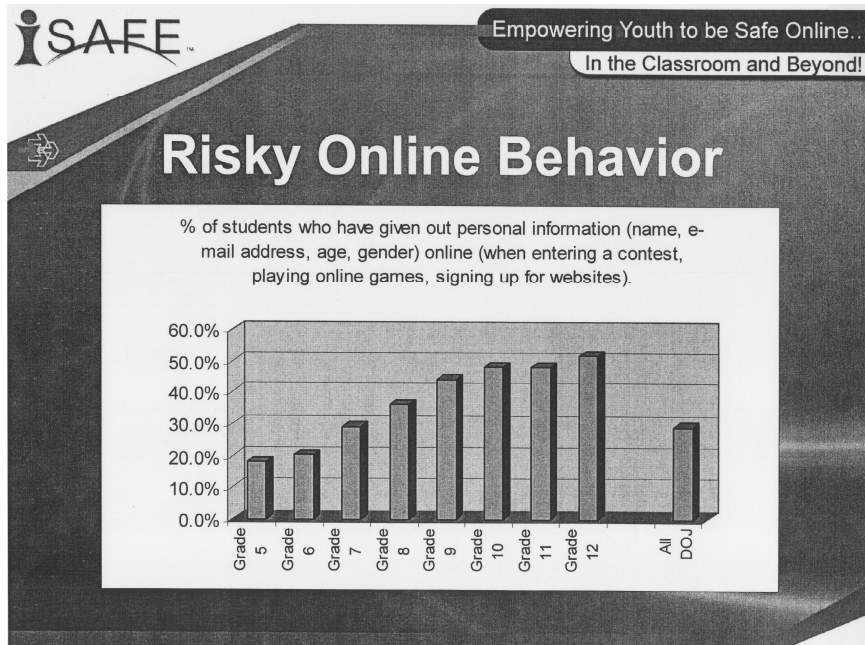


## Internet Landscape

- 90.4% of 5-12 grade students have Internet access
- 84% of 3-4 grade students have Internet access
- 45% of students in 8-10 grade utilize the Internet as their main method of keeping in touch with friends
- 23% of 5-12 grade students are online more than 5 hours a week (86% are online at least 3 hours a week)



- iSAFE** Empowering Youth to be Safe Online...  
In the Classroom and Beyond!
- ## Internet Landscape
- 33% of students feel freer to do what they want on the Internet than they do in their physical world.
  - 29% of students feel that their parents have no idea how much time they spend online.
  - 25% of students stated that on some level, their parents would disapprove of their online activities.
  - 34% actually keep their Internet activities secret from their friends and family.



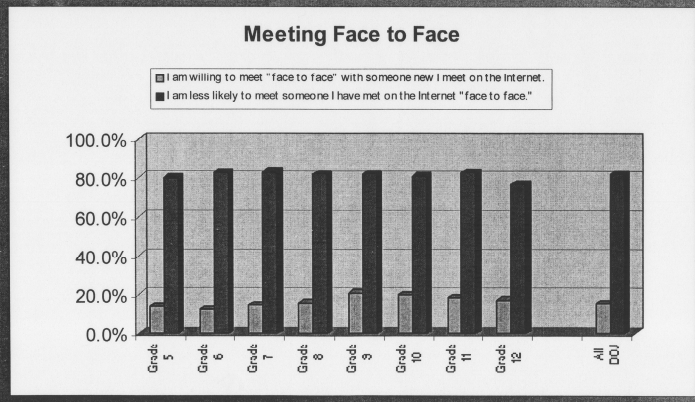
**iSAFE™** Empowering Youth to be Safe Online...  
In the Classroom and Beyond!

## i-SAFE Makes a Difference

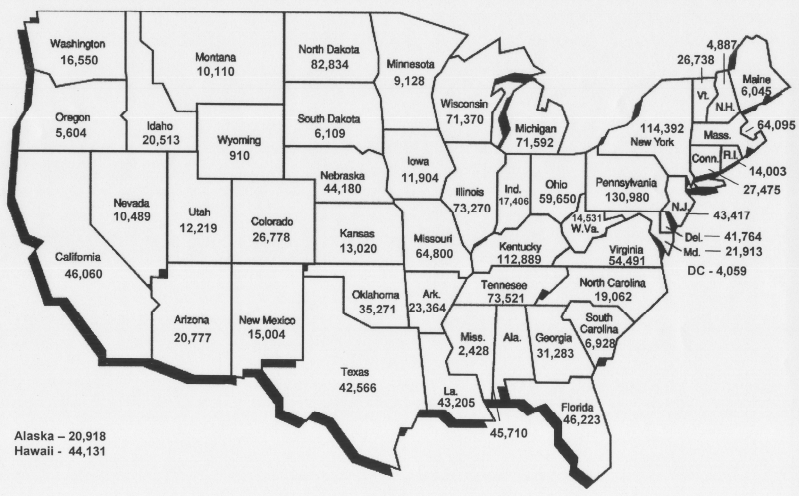
**After the i-SAFE Curriculum**

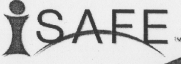
- 84% of students stated an intention to be more careful about where they go and what they do on the Internet
- 89% indicated that they would be more careful about the email attachments that they open.
- 88% will be more careful about sharing personal information with those they meet in chat rooms and other places on the Internet.

## i-SAFE Makes a Difference



## i-SAFE Makes a Difference





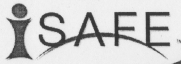
Empowering Youth to be Safe Online...  
In the Classroom and Beyond!

## i-SAFE Model: Kentucky

- Task Force Meetings with DOE, Law Enforcement, and Policy Makers
- 5 Sets of Launch Events: Professional Development Programs, Parent Programs and Community Leaders Meetings
- Key Stakeholders Adopted the i-SAFE Program and Facilitated Additional Events.

Kentucky Stats:

- 129 Professional Development Programs
- 88 Parent Programs
- 23 Assembly Experiences
- 515 Student Mentors
- 112,889 Students Received Internet Safety Education

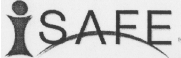


Empowering Youth to be Safe Online...  
In the Classroom and Beyond!

## i-SAFE Makes a Difference

### i-SAFE Trains Educators

- 1,995 Professional Development Programs
  - 304 Tier 1 PDPs
  - 711 Tier 2 PDPs
  - 980 Tier 3 PDPs
- 28,828 Registered PDP Attendees
- 2,360 Registered i-LEARN Online Participants



Empowering Youth to be Safe Online...  
In the Classroom and Beyond!

# i-SAFE Makes a Difference


## i-SAFE Empowers Parents and Students

**i-PARENT**

- 357 Parent Train the Trainer Sessions
- 1,900 Parent Programs

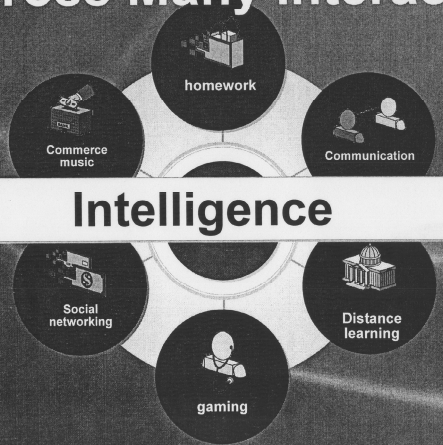
**Students**

- 182 Assembly Train the Trainer Workshops
- 477 Assembly Experiences
- 12,260 Student Mentors
- 1.8 Million Students Received Classroom Instruction



Empowering Youth to be Safe Online...  
In the Classroom and Beyond!

# Sharing One Identity Across Many Interactions



**Intelligence**

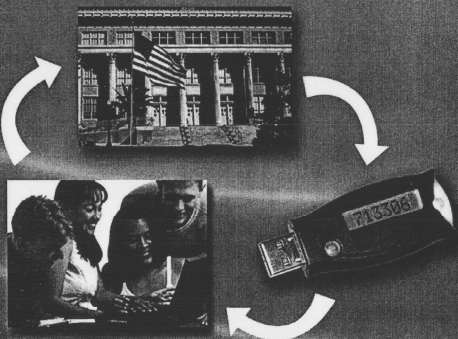
- homework
- communication
- distance learning
- gaming
- social networking
- commerce music

**iSAFE**™ Empowering Youth to be Safe Online...  
In the Classroom and Beyond!

## School-Issued Digital Credentials

**VeriSign**

- Tokens distributed through the iSAFE Safe School Program at the time of enrollment using the VeriSign service
- School database used to provide necessary information for digital certificates
- Parental consent is required in this optional program
- National distribution exclusively through the iSAFE Safe Schools Education Initiative and Outreach Program

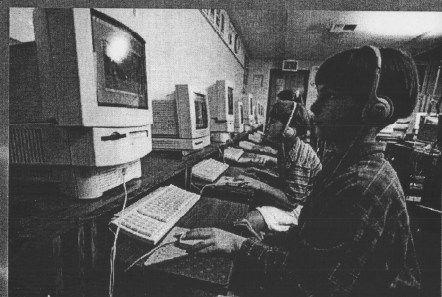


**iSAFE**™ Empowering Youth to be Safe Online...  
In the Classroom and Beyond!

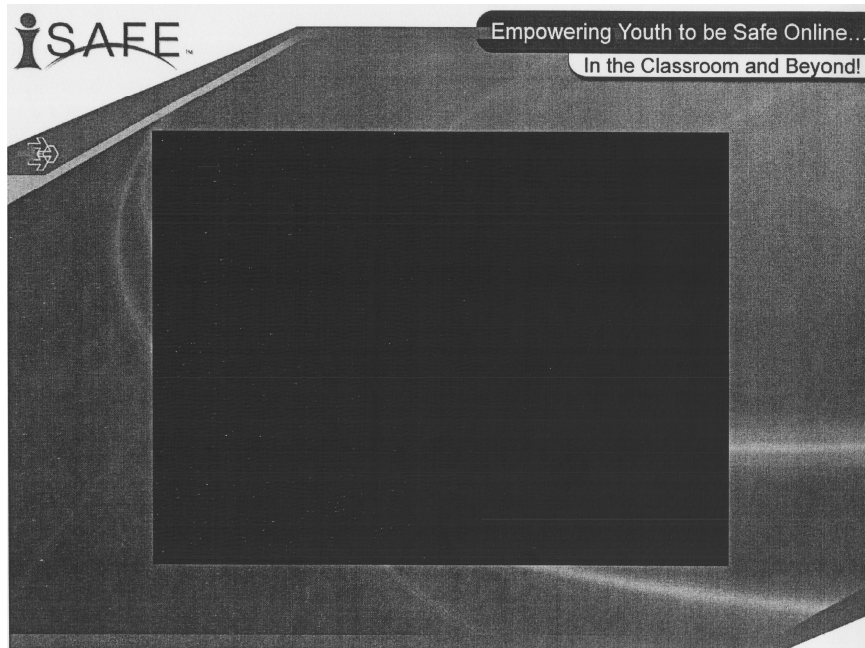
## Usage of Tokens

**VeriSign**

- Tokens are portable containers for a child's *digital credential*
  - Use on any USB port
  - Can be carried around on a keychain
  - Can be used at school, at home, or in any computer with a USB port
- *Digital credentials* only contains necessary info for usage online
  - Gender
  - Age







MS. SCHROEDER. Not at all.

MR. WHITFIELD. Okay.

MS. SCHROEDER. Thank you.

MR. WHITFIELD. With that, the record will remain open for 30 days and I think Dr. Burgess may have some additional questions and if he does we will get them to you all. But that concludes today's hearing and thank you very much for your patience.

[Whereupon, at 3:36 p.m., the subcommittee was adjourned.]

**SEXUAL EXPLOITATION OF CHILDREN  
OVER THE INTERNET: WHAT PARENTS,  
KIDS AND CONGRESS NEED TO KNOW  
ABOUT CHILD PREDATORS**

---

**THURSDAY, APRIL 6, 2006**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ENERGY AND COMMERCE,  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10:00 a.m., in Room 2322 of the Rayburn House Office Building, Hon. Ed Whitfield (Chairman) presiding.

Members present: Representatives Bass, Walden, Ferguson, Burgess, Blackburn, Barton (ex officio), Stupak, DeGette, Inslee, and Whitfield.

Staff Present: Mark Paoletta, Chief Counsel for Oversight and Investigations; Alan Slobodin, Deputy Chief Counsel for Oversight and Investigations; Kelli Andrews, Counsel; Karen Christian, Counsel; Michael Abraham, Legislative Clerk; Edith Holleman, Minority Counsel; and David Nelson, Minority Investigator/Economist.

MR. WHITFIELD. This hearing will come to order, and today marks the second day of hearings that the Oversight and Investigations Subcommittee is having on child pornography and sexual exploitation of children over the Internet.

Today, as I said, this is our second day of hearings on the sexual exploitation of children over the Internet. Today, we hope to gain a better understanding of how U.S. law enforcement is working to combat the horrifying and growing commercial business of sexually exploiting children over the Internet, and what is being done to put those online child predators behind bars.

The testimony we heard on Tuesday was disturbing. For example, in this \$20 billion a year business of commercially exploiting children, the images of child victims are increasingly younger and increasingly more violent. I cannot fathom who these people are that seek to view these images of children being sexually abused and, frequently, being abused on demand. As one witness on Tuesday described it, these images are digital crime scenes, and it sickens both our heart and soul.

Some of the most disturbing testimony at Tuesday's hearing came from Justin Berry, a victim of online predators. Justin's testimony about the Department of Justice's handling of his case was particularly troubling. Justin testified that he himself has no faith in the Department of Justice's Child Exploitation and Obscenity Section. This is a section of prosecutors in the Department that are supposedly experts in handling cases like Justin's. When a victim witness has no faith in the people that are supposed to be his advocates, there is clearly something wrong with the process.

While I am sympathetic to the Department's concern over discussing ongoing investigations, the allegations raised by Justin Berry's testimony on Tuesday raise important process questions that need to be addressed by the Department. We have some specific questions for the Department of Justice at today's hearing. These questions include: why has it taken so long for the Department to act and rescue children in imminent danger of being molested; why Justin's father, Knute Berry, a man who allegedly profited off of the sexual exploitation of his son, has not been charged or arrested; why there have been no arrests from the over 1,500 names of subscribers to Justin's website, that featured images of children being sexually abused, and which he supplied to the Department of Justice; why Aaron Brown, the person who ran a credit card processing company called Neova.net, that processed the orders for sexually exploitive images of children, has not been arrested and charged in connection with Justin's case; why Ken Gourlay has not been charged or arrested in connection with the alleged money he made hosting Justin's own website, nor for his alleged sexual abuse of Justin while Justin was still a minor; and finally, why the Department of Justice allowed an affidavit to be unsealed and remain unsealed for 6 months, and still is unsealed today, in a criminal case that had the effect of putting Justin Berry's life in danger?

We do not want these disturbing details about the handling of Justin's case to go unanswered by the Department, and hope that some insight will be gained through this hearing today, and that is one of our clear intents.

I would like now to briefly turn to the other witnesses that we will hear from today. Law enforcement has a very difficult task ahead, and is fighting an immense criminal enterprise of online child predators. We need to give law enforcement the necessary resources to save our children from online predators. I look forward to hearing from the various law enforcement witnesses today about their successes in the field, as well as concerns and problems they face. Child predators on the Internet are using all technological means available to avoid law

enforcement efforts, and law enforcement must respond in an effective way.

Finally, it is critical that we have an understanding of what is going on in the various State legal systems. About 70 percent of all prosecutions involving child pornography are handled at the State and local level. Therefore, the State laws regarding the illegality of possession, manufacturing, distribution, and enticing of minors in child pornography need to be as strong as the Federal laws. My home State of Kentucky, as an example, recently passed legislation that will make possession of child pornography a felony instead of a misdemeanor. I look forward to hearing from witnesses, including Mr. Weeks from PROTECT, about sentencing issues surrounding these cases involving the sexual exploitation of children over the Internet.

And at this time, I will recognize Mr. Stupak of Michigan for his opening statement.

[The prepared statement of Hon. Ed Whitfield follows:]

PREPARED STATEMENT OF THE HON. ED. WHITFIELD, CHAIRMAN, SUBCOMMITTEE ON  
OVERSIGHT AND INVESTIGATIONS

GOOD MORNING.

TODAY THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS BEGINS ITS SECOND DAY OF HEARINGS ABOUT SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET. TODAY WE HOPE TO GAIN A BETTER UNDERSTANDING OF HOW U.S. LAW ENFORCEMENT IS WORKING TO COMBAT THE HORRIFYING AND GROWING COMMERCIAL BUSINESS OF SEXUALLY EXPLOITING CHILDREN OVER THE INTERNET AND WHAT IS BEING DONE TO PUT THESE ON-LINE CHILD PREDATORS BEHIND BARS. THE TESTIMONY WE HEARD ON TUESDAY WAS DISTURBING. FOR EXAMPLE, IN THIS 20 BILLION DOLLAR A YEAR BUSINESS OF COMMERCIALY EXPLOITING CHILDREN—THE IMAGES OF CHILD VICTIMS ARE INCREASINGLY YOUNGER AND INCREASINGLY MORE VIOLENT. I CANNOT FATHOM WHO THESE PEOPLE ARE THAT SEEK TO VIEW THESE IMAGES OF CHILDREN BEING SEXUALLY ABUSED AND IN MANY INSTANCES--ON DEMAND. AS ONE WITNESS ON TUESDAY DESCRIBED IT—THESE IMAGES ARE “DIGITAL CRIME SCENES”. IT SICKENS MY HEART AND MY SOUL.

SOME OF THE MOST DISTURBING TESTIMONY AT TUESDAY’S HEARING CAME FROM JUSTIN BERRY—A VICTIM OF ON-LINE PREDATORS. JUSTIN’S TESTIMONY ABOUT THE DEPARTMENT OF JUSTICE’S HANDLING OF HIS CASE WAS PARTICULARLY TROUBLING. JUSTIN TESTIFIED THAT HE HAS NO FAITH IN THE DEPARTMENT OF JUSTICE’S CHILD EXPLOITATION AND OBSCENITY SECTION. THIS IS A SECTION OF PROSECUTORS IN THE DEPARTMENT THAT ARE SUPPOSEDLY EXPERTS IN HANDLING CASES LIKE JUSTIN’S. WHEN A VICTIM WITNESS HAS NO FAITH IN THE PEOPLE THAT ARE SUPPOSED TO BE HIS ADVOCATES—THERE IS SOMETHING CLEARLY WRONG WITH THE PROCESS. WHILE I AM SYMPATHETIC TO THE DEPARTMENT’S CONCERN OVER DISCUSSING ON-GOING INVESTIGATIONS, THE ALLEGATIONS RAISED BY JUSTIN BERRY’S TESTIMONY ON TUESDAY

RAISE IMPORTANT PROCESS QUESTIONS THAT NEED TO BE ADDRESSED BY THE DEPARTMENT. WE HAVE SOME SPECIFIC QUESTIONS FOR THE DEPARTMENT OF JUSTICE AT TODAY'S HEARING. THESE QUESTIONS INCLUDE—

- WHY HAS IT TAKEN SO LONG FOR THE DEPARTMENT TO ACT AND RESCUE CHILDREN IN IMMINENT DANGER OF BEING MOLESTED?
- WHY JUSTIN'S FATHER—KNUTE BERRY—A MAN WHO ALLEGEDLY PROFITED OFF OF THE SEXUAL EXPLOITATION OF HIS SON HAS NOT BEEN CHARGED OR ARRESTED?
- WHY THERE HAVE BEEN NO ARRESTS FROM THE OVER 1500 NAMES OF SUBSCRIBERS TO JUSTIN'S WEBSITE THAT FEATURED IMAGES OF CHILDREN BEING SEXUALLY ABUSED?
- WHY AARON BROWN, THE PERSON WHO RAN A CREDIT CARD PROCESSING COMPANY --CALLED NEOVA.NET—THAT PROCESSED THE ORDERS FOR SEXUALLY EXPLOITATIVE IMAGES OF CHILDREN, HAS NOT BEEN ARRESTED AND CHARGED IN CONNECTION WITH JUSTIN'S CASE?
- WHY KEN GOURLAY HAS NOT BEEN CHARGED OR ARRESTED IN CONNECTION WITH THE ALLEGED MONEY HE MADE HOSTING JUSTIN'S WEBSITE AND FOR HIS ALLEGED SEXUAL ABUSE OF JUSTIN WHEN JUSTIN WAS STILL A MINOR?
- AND FINALLY—WHY THE DEPARTMENT OF JUSTICE ALLOWED AN AFFIDAVIT TO BE UNSEALED---AND REMAIN UNSEALED FOR OVER SIX MONTHS-- IN A CRIMINAL CASE THAT HAD THE EFFECT OF PUTTING JUSTIN'S LIFE IN DANGER?

WE DO NOT WANT THESE DISTURBING DETAILS ABOUT THE HANDLING OF JUSTIN'S CASE TO GO UNANSWERED BY THE DEPARTMENT AND HOPE THAT SOME INSIGHT WILL BE GAINED THROUGH THIS HEARING.

I WOULD LIKE NOW TO BRIEFLY TURN TO THE OTHER WITNESSES THAT WE WILL HEAR FROM TODAY. LAW ENFORCEMENT HAS A VERY DIFFICULT TASK AHEAD AND IS FIGHTING AN IMMENSE CRIMINAL ENTERPRISE OF ON-LINE CHILD PREDATORS. WE NEED TO GIVE LAW ENFORCEMENT THE NECESSARY RESOURCES TO SAVE OUR CHILDREN FROM ON-LINE PREDATORS. I LOOK FORWARD TO HEARING FROM THE VARIOUS LAW ENFORCEMENT WITNESSES TODAY ABOUT THEIR SUCCESSES IN THE FIELD, AS WELL AS, CONCERNS OR PROBLEMS THEY SEE IN INVESTIGATION AND PROSECUTING THESE CASES. CHILD PREDATORS ON THE INTERNET ARE CLEARLY USING ALL TECHNOLOGICAL MEANS AVAILABLE TO AVOID LAW ENFORCEMENT EFFORTS AND LAW ENFORCEMENT MUST RESPOND.

FINALLY, IT IS CRITICAL THAT WE HAVE AN UNDERSTANDING OF WHAT IS GOING ON IN THE VARIOUS STATE LEGAL SYSTEMS. ABOUT 70% OF ALL PROSECUTIONS INVOLVING CHILD PORNOGRAPHY ARE HANDLED AT THE STATE AND LOCAL LEVEL. THEREFORE, THE STATE LAWS REGARDING THE ILLEGALITY OF POSSESSION, MANUFACTURING, DISTRIBUTION AND ENTICING OF MINORS IN CHILD PORNOGRAPHY NEED TO BE AS STRONG AS THE FEDERAL LAWS. MY HOME STATE OF KENTUCKY RECENTLY PASSED LEGISLATION THAT WILL MAKE POSSESSION OF CHILD PORNOGRAPHY A FELONY INSTEAD OF A MISDEMEANOR. I LOOK FORWARD TO HEARING FROM WITNESSES, INCLUDING MR. WEEKS, FROM PROTECT, ABOUT SENTENCING ISSUES

SURROUNDING THESE CASES INVOLVING THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET.

THANK YOU.

MR. STUPAK. Thank you, Mr. Chairman.

April is Child Abuse Awareness Month, and so, it is appropriate we are holding these hearings. As we learned Tuesday, this problem has many sordid faces: commercial websites, predator seduction over peer-to-peer networks, pedophile groups that demand and trade new materials as the price of admission to complete their set of pornographic photos, and sex tourism, which are trips organized by American men to foreign countries for the purpose of sexually molesting and filming sex acts with young people.

We learned other disturbing facts too numerous to list here, but a few that are noteworthy. Victims of this disgusting trade are 28 times more likely to become prostitutes 86 percent of the victims develop serious, long term mental illness. Eighty percent of these predators have material depicting victims under the age of 12, 40 percent under the age of 6, and 20 percent under the age of 3. Unfortunately, yesterday's news revealed that a Deputy Press Secretary at the Department of Homeland Security had been arrested by authorities who were posing as a 14-year-old girl. The arrest occurred as the officer portraying herself as a 14-year-old girl was to pose nude for him on a webcam.

As Mr. Justin Berry testified, there is no reason for a 13 or 14-year-old to have a webcam. Mr. Chairman, the committee staff has spent many hours interviewing key Federal officials who investigate child pornography every day. Unfortunately, they are not here to testify today. Today, we will hear from a few frontline law enforcement officers, and some witnesses purporting to represent the frontline prosecutors and the Federal law enforcement officers. I say purportedly, because I don't believe that the most experienced witnesses are here today.

On Tuesday, we heard a withering indictment of the Child Exploitation and Obscenity Section at the Department of Justice, CEOS. CEOS are the prosecutors responsible for coordinating these horrible cases nationwide. Unfortunately, the head of CEOS is not here. Instead, Justice sent us a U.S. Attorney from the State of Montana to present its testimony. I hope this individual has some knowledge in this area he will be talking about today.

The Department of Justice is not the only agency that did not provide its most knowledgeable staff as a witness today. Both the Federal Bureau of Investigation and the Bureau of Immigration and Customs Enforcement, ICE, have incredible, underfunded cybercrime operations with great expertise in working these cases nationally and internationally. These critical law enforcement agencies have two of the most articulate

and committed special agents working on child exploitation. These talented and dedicated supervisors, Arnold Bell of the FBI's Innocent Images Unit, and Claude Davenport of the Child Exploitation Section of the ICE Cybercrime Center, have not been permitted to give testimony today. Instead, the individuals who will appear here have job titles bestowed upon them by bureaucratic politicians. Again, I suspect that they have little recent law enforcement experience in the dirty world of Internet child pornography and sexual exploitation.

That makes our job extremely difficult, for us here in Congress to do oversight work when agencies do not send the witnesses we request. I will be pressing for answers as to why those that labor so hard to protect our children from the worst of all crimes are denied adequate personnel and critical technical resources. The agents that actually work these cases need much more recognition and support in what they receive from their superiors. These men and women are overwhelmed by the size of the problem, and handicapped by timid prosecutions, at least on the Federal level. The FBI, ICE, and the Inspectors of the U.S. Postal Service have brought down networks involving tens of thousands of criminals that have, or likely will physically molest children, yet despite their efforts, the Federal prosecution of these perpetrators is rare.

On the State and local level, the story is different but widely variable. We are aware of a county district attorney in New Hampshire that averages one prosecution every 10 days of these predators. He says he could do one a day if he had more attorneys on staff. He does have the assistance of the ICAC, coordinated Federal and State local computer crime specialists, assisting him in developing the necessary cases and evidence, but he still needs the manpower to present the cases in court. I find the ICAC's testimony about the Internet service providers being a major obstacle to the investigation of child exploitation over the Web particularly troubling. I can't help but believe that the credit card companies and PayPal accounts also have responsibility to police their clients who are accessing these child pornography sites.

Yesterday, I was pleased that our colleagues unanimously accepted my amendment in the Telecommunications markup to crack down on Internet child pornography. My amendment orders the Federal Communications Commission to devise regulations that require both cable service and phone companies offering cable service and technologies to prevent child pornography from being conveyed over Internet networks. This will serve as a good start at curtailing child pornography on the Internet, but we also need stepped up law enforcement at all levels, Federal, State, and local.

Mr. Chairman, the Federal prosecution effort is far less vigorous than that found on the State and local level. As I noted Tuesday, in a major

case where 20,000 verified American child sex offenders are out still walking our streets, prosecutors have been able to convict less than 2 percent of the identified perpetrators, while law enforcement in Australia obtained convictions of over 55 percent of their countrymen identified in the same international bust. If Australia can do 55 percent, I am sure we can do better than 2 percent here in this country.

We, Congress, have a long way to go to assist law enforcement to help in this fight. I hope that we don't stop with this hearing today. As a former law enforcement officer, I will use every opportunity to crack down on illegal Internet activity, bank card transactions, and inadequate Federal statutes that tie law enforcement hands when pursuing child pornography perpetrators.

With that, Mr. Chairman, I yield back, and I thank you for having this hearing.

MR. WHITFIELD. Mr. Stupak, thank you, and I want to also thank you for raising this issue of the witness from the Justice Department today. Of course, we are glad to have Mr. Mercer here. He is a U.S. Attorney from Montana, and I know he has experience in these child pornography cases, but we specifically asked for Raul Roldan, who is the FBI's cybercrimes expert, and we also asked for Drew Oosterbaan, who is the Director of CEOS, and neither one of them is here, but I did notice that Raul Roldan was on CNN today on the Today Show, so he had time to go on television, but he didn't have time to be here with us.

At this point, I would like to recognize the gentleman from New Jersey, Mr. Ferguson, for his opening statement.

MR. FERGUSON. Thank you, Mr. Chairman, and thank you for holding this second hearing.

Mr. Chairman, I, too, think it is outrageous that we have law enforcement agencies that are willing to, and perfectly happy, to send some of their most knowledgeable representatives to do interviews on national media, but they can't come before a subcommittee in the Congress to share their expertise and their thoughts and strategies with the Congress and the American people. I think it is outrageous.

I certainly appreciate the witnesses for being here today. I appreciate the expertise and the insights that they will lend to these hearings. But I think it is a very, very serious issue, and I hope that we will follow up on that. I want to thank you, Mr. Chairman, and Mr. Stupak, for your leadership on this issue. I am happy to see that as parents and as Members of Congress who are serving on this committee, that we are making a concerted effort to get to the bottom of an industry which so horribly affects many children in our country. I also want to thank the witnesses for testifying and helping us get to the real causes of this problem, and why it is so pervasive in our society.



I am sure that it is safe to say this past Tuesday's hearing touched and shocked every one of us who was there in that room, or who got to watch it on television. Although we have been aware of this problem, many of us have been aware of this problem, I think it is doubtful that prior to Tuesday, that any of us genuinely knew the details of this sordid world that so many children find themselves victims of.

The question running through everybody's minds and my mind is how, how could this happen to so many children? How could it be so easy for a sexual predator in today's world of advanced crime fighting and investigative techniques? And how is it that we, as a society, seem to be incapable of putting a stop to it? I can't thank enough organizations like WiredSafety and i-SAFE, people like Kurt Eichenwald from the New York Times, who is here again today, who have brought national attention to this issue. We must recognize that it is our job as Members of Congress to give these organizations and our law enforcement officials the tools they need to fight this unbelievable crime.

With yesterday's revelations about a high ranking DHS official being charged with online seduction, and yesterday's announcement of 27 people being charged in an international child pornography ring, it is clear that we are just beginning to scratch the surface of this industry, and we have a long, long way to go.

Recently, the National Center for Missing and Exploited Children reported that 39 percent of people who are caught with images of child sexual abuse had images of children younger than 6 years old. We have a 6-year-old daughter. Nineteen percent of people who have been caught with these images, one in five, were caught with images of children under three years old. We also have a 3-year-old daughter. This evil is beyond our comprehension.

As proven by these hearings, my colleagues and I have made a commitment to do everything in our power to fight this problem, and to punish offenders to the fullest extent of the law. These people are not normal criminals. Their offences go above and beyond typical crimes. They steal the innocence of a child, and leave in their wake emotional and physical scars that will affect these young victims for their entire lives. After hearing Justin's heart-wrenching testimony on Tuesday, it became apparent that it is a problem within our justice system that allows this industry to continue and remain profitable. Justin told us that these predators laugh at law enforcement, but an estimated \$20 billion industry that makes it profits by violating children is absolutely nothing to laugh at.

I am anxious to hear the testimony of our witnesses, and to have an opportunity to question them regarding what needs to be done by lawmakers and parents and teachers and law enforcement officers, to put

an end to this industry, and to find out how we have fallen so sadly short of our goals so far.

Thank you again, Mr. Chairman, and thank you, Mr. Stupak, for your commitment, and I look forward to hearing from the witnesses.

MR. WHITFIELD. Thank you, Mr. Ferguson. At this time, I will recognize the gentlelady from Colorado, Ms. DeGette, for her opening statement.

MS. DEGETTE. Thank you very much, Mr. Chairman.

Mr. Chairman, this is a little unusual for this committee, because having jurisdiction over telecommunications and the Internet, we are usually always jumping at the chance to talk about the wonders of the Web. And the Internet has been one of the most incredible creations of the last century. At the beginning of the new millennium, we look forward to a future of untold promise and new innovation that we can't even imagine today, and I think what we are seeing this week, sadly, is sometimes this innovation can move in ways that are horrific to us.

The Internet has changed the way we do business, conduct research, play, and communicate with each other, and it has made many day-to-day activities like shopping so much easier. Those of us who have teenage children know that young people often are the ones who figure out the ways to use the Internet in new and different, but that is the problem is the activities that have been made easier by the Internet are being used now to commit crimes against humanity in a much more facile way, and that is the sexual exploitation of children.

That is what we are faced with when we conduct these hearings today. Our technological pride and joy has been hijacked. It has enabled a plague of proportions that none of us here today every imagined. Cloaked in anonymity, and enabled by technological innovation, this blight has been growing to extreme conditions under our very noses. How do we preserve the things that we value about the Internet? Can we find the right balance between privacy and freedom, in eradicating this heinous epidemic? I don't think we have the answers today, but that is what we are here to determine, and I would say we have a very difficult job ahead of us. We can't stand idly by and let our young people be devoured by this terrible use of technology.

One thing that is clear to me, after hearing Justin's testimony and reading the newspaper articles and other materials, is that these terrible predators are working a lot faster than we are, and government, for a change, needs to thing about working faster than the people who are taking advantage of our kids.

All of us agree that these hearings have been a horrific eye opener. Mr. Ferguson talked about his young children, 3 and 6. Well, I have two girls, who are age 12 and 16, and I don't think any of us realized how

pervasive this child exploitation over the Internet is. I will tell you this, I certainly intend to go home and talk to my two daughters about this problem, and what they can do, when I go home tomorrow.

We have learned that it is now an industry that now nets a profit close to the gross product of some small countries, and so I, too, am glad, Mr. Chairman, that you and Mr. Stupak are holding these hearings, because it is an issue that would be easy for us to try to sweep under the rug. But I think it is too important for that, and so, I think every member of this subcommittee needs to make a commitment right now to accomplish three things as the result of these hearings: first, to identify the problems with the Federal response to this crisis; second, to figure out how we are going to address this scourge; and third, to pledge that by the end of the 109<sup>th</sup> Congress, which is about 15 weeks away, we will have made an impact on this.

What we should not do is have these hearings, make ourselves feel better, go home and talk to our kids ourselves, and then breathe a sigh of relief that we fixed the problem, because that is not going to fix the problem. This scourge is just a mouse click away from directly impacting us, our families, and our communities, and so, I would say we have a moral imperative to take action.

I share the disappointment that everyone else has, that the witnesses that were requested from the FBI and the other agencies are not here today. If there was ever an issue that the executive branch should work with the legislative branch on, it was this issue. This is an investigative hearing, and with all due respect, we need facts, not generalized policy statements.

And so I just want to say, Mr. Chairman, as Americans, we should be disgusted that our country is the number one consumer of child pornography. How did we get here, and how are we letting this happen to our children? We cannot let this issue go away. We can't be a do nothing Congress, and if we can make an impact on this issue, Mr. Chairman, I would suggest that everybody on both sides of this committee can go home and hold our heads up very proudly.

So, I think let us commit together to get to work. Thank you very much.

MR. WHITFIELD. Well, thank you, Ms. DeGette, and you raise some penetrating questions, and we hope to get those answers. Ever since Kurt Eichenwald wrote the first articles in the New York Times about this issue, our committee has been focused on it, and no one has been more focused on it than our full committee Chairman of Energy and Commerce, Joe Barton of Texas, and at this time, I would like to recognize Mr. Barton for his opening statement.

CHAIRMAN BARTON. Thank you, Chairman Whitfield.

I do have a formal opening statement, but I have to get something off my chest. We have been working on this subcommittee, and Mr. Dingell and I, the full committee on this issue for 6 months or so, maybe longer, and we keep trying to cooperate with the Justice Department and the FBI, and you folks seem bound and determined to be as uncooperative as possible.

This is the opening statement time, so I am not going to ask any questions, but I want you to know, Mr. Mercer, that I am going to call the Attorney General one more time, and we had better get the people we want to testify. Not that you are not a credible witness, but I didn't hear of all of Ms. DeGette's statement, but my guess is, having scanned your testimony, that she has scanned it too, we don't need to know specifics of case investigations. That shouldn't be public. But on behalf of the people of the United States of America who we represent, as the most closely elected officials to the people, we do deserve to get the witnesses that they are supposedly hands on, trying to solve these problems, and we are not doing it. You are not giving them to us. Your Department is not giving them to us, and the FBI is not giving them to us.

Now, I am told half the room are FBI agents, and when the second panel comes, I am going to have some pretty straight questions for the FBI. But we are going to get the facts one way or the other. This is just too important an issue to let bureaucratic, I am trying to think of the right word, turf wars impede it. And when you have a Republican majority in the Congress and a Republican President, we ought to be able to work on a bi-branch basis, if that is the right term, to get the facts out, and that is not happening.

So, Mr. Chairman, I am going to ask that my entire statement, formal statement, be put into the record. But this is probably the most important investigation. We have got all the investigations going on in all the other bodies and other committees, but child pornography is the most pernicious thing that is affecting our society at its very roots, and we need to root it out, and we need to put an end to this Internet child pornography system that is growing like a weed on our society, and one way or the other, we are going to get our executive branch officials to cooperate with us and testify. That is just going to happen.

So with that, Mr. Chairman, I am going to yield back. But I want to thank you and Mr. Stupak for your perseverance on this issue.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY  
AND COMMERCE

Thank you, Chairman Whitfield, for holding this second day of hearings on sexual exploitation of children over the Internet.

Just two days ago, we heard testimony from witnesses who described the sickening world of Internet child pornography. As repulsive as Tuesday's testimony was regarding the magnitude of the child pornography problem, I was just as troubled by the opinion shared by some of the witnesses that the fight against child pornography in the United States is, if not a losing battle, one that is not being won.

Only one conclusion could be drawn from the witnesses' testimony: the sexual exploitation and abuse of children over the Internet has reached a crisis point. Today, we are here to learn about what is being done to find, prosecute, and convict these child predators.

I look forward to learning whether the witnesses from the Federal Bureau of Investigation, United States Immigration and Customs Enforcement, and the United States Postal Inspection Service share this opinion and what they believe must be done to bring child predators to justice. In particular, I hope to hear more about the role of Internet Service Providers and credit card companies in these investigations, and whether more should be required of them with respect to retaining data and conducting due diligence of those who use their servers and financial networks to distribute child pornography.

I also look forward to learning more about state efforts to prosecute those who commit crimes related to the sexual exploitation of children. While the federal government is actively pursuing investigations of child predators, the vast majority of investigations and prosecutions of these crimes are being conducted at the state and local level. Unfortunately, penalties for child sex crimes in some states are the equivalent of a slap on the wrist. It is inconceivable to me that some who possess, create, or distribute child pornography go home on probation. Their victims don't get off so easily. They suffer for the rest of their lives.

Finally, I believe this hearing should address some of the concerns raised by Justin Berry at Tuesday's hearing. Justin, Kurt Eichenwald, the New York Times reporter who investigated and reported Justin's story, and Justin's lawyer, Stephen Ryan, all testified that the Justice Department has failed to adequately pursue investigations against the men who molested Justin and the customers who sexually exploited him over the Internet. I have personally talked to Attorney General Alberto Gonzales about these concerns, and he has assured me that his department is serious and is actively pursuing this investigation. I don't doubt his word, but I do hope the testimony offered today by the Department of Justice will provide further information about the status of the investigation.

In closing, I want to commend the law enforcement agents who are here today as well as their colleagues in the field. I believe all my colleagues join me today in saying that we are prepared to do everything possible to help you put an end to the child pornography industry and bring child predators to justice.

I look forward to hearing from the witnesses and yield back the balance of my time.

MR. WHITFIELD. Well, thank you, Mr. Chairman, and we look forward to continue working with you as we attempt to get the key witnesses before the committee.

However, your opening statements in their entirety will be placed in the record without objection. And at this time, I will recognize Dr. Burgess of Texas for--oh, I am sorry--recognize Mr. Inslee for his opening statement.

MR. INSLEE. I just want to follow on Chairman Barton's statement that this country really is enraged, and is demanding answers, and ultimately, we will obtain them, and we hope that the message that is

delivered is that we need to move forward together quickly. The country is not going to wait any longer.

Thank you.

MR. WHITFIELD. Thank you, Mr. Inslee. At this time, we recognize Dr. Burgess of Texas.

MR. BURGESS. Thank you, Mr. Chairman.

In the interests of time, too, I am going to submit a statement for the record, because we do have a full day ahead of us, but I just can't help but observe that the one piece that I took away from Tuesday's lengthy hearing was the comment that the perpetrators were laughing at law enforcement, and law enforcement is in this room today. They are laughing at you on the Internet about this problem, and I want you to take that very, very seriously.

I wanted to also take a moment of personal privilege, and once again, recognize don't tell anyone home in my district, but I want to recognize the New York Times reporter for doing the right thing, and I think if he had not stopped and picked up the person at the side of the road, they might not be with us today. So Mr. Eichenwald, again, I want to congratulate you, and thank you for doing the right thing when you were faced with a situation that you probably didn't completely understand right at the beginning.

I, myself, have to wonder why it has gotten to this point. I mean, we are a society that puts warning labels on airplanes that says danger, you may die if this crashes. Why don't we put a warning label on a webcam, not age appropriate for those under 18 years of age to use by themselves in their bedrooms for longer than 12 hours at a time. I wonder about America's legal system.

We have heard testimony in this committee on multiple occasions about the abuses of the class action system. Where are the lawsuits against the payment companies that allow this to happen? Why have they not stepped up to protect America's children, but mostly, I am embarrassed by the Federal agencies, and by the fact that we haven't taken definitive action in Congress. I know it is going to be difficult. I want all of us in the Federal government, those in Federal agencies and those in Congress, to muster the institutional courage to do the right thing.

With that, Mr. Chairman, I will yield back.

MR. WHITFIELD. Thank you, Dr. Burgess. And at this time, I will recognize the gentlelady from Tennessee, Mrs. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman. I thank you for the work that you and the staff have done on this hearing, and the series of hearings, and I thank you also, say thank you to our witnesses for continuing to work with us, to be here and work with us on the issue, as

we seek to crack down on child pornography and sexual exploitation and abuse.

This past Tuesday, the subcommittee did hear testimony from Justin Berry on the pervasiveness of child predators on the Internet. He described to us how the predators help to lure teenagers, to setting up the websites, the webcam situation, as Dr. Burgess just mentioned, and then, gradually lure them into sexual acts for money.

He also told this committee that the Department of Justice's CEOS has failed to act on information he provided to them at the risk of his own life, to find over 1,500 child predators and distributors of child pornography. And I am looking forward to hearing from the Department of Justice on why this happened. It is incomprehensible to me that there are people who are employed by the Federal government of this Nation who will hide, arrogantly hide behind bureaucracy, stonewall behind bureaucracy, and allow this to happen. That is inexcusable. It is absolutely inexcusable.

The Federal budget should reflect our main priority, to defend the citizens of our country. To protect our children from those who would abuse them clearly falls into this area.

I look forward to hearing from law enforcement on their efforts to shut down this industry, and send a message to these despicable, despicable people that this country will not tolerate those who knowingly, who willingly, who seek to abuse our children.

Chairman Whitfield, I yield back my time. I thank you for looking into this delicate issue, and I hope to see some positive results from the hearing.

Thank you, sir.

MR. WHITFIELD. And thank you, Mrs. Blackburn. At this time, I recognize the gentleman from Oregon, Mr. Walden, for his opening statement.

MR. WALDEN. Thank you very much, Mr. Chairman.

I have read through the testimony from our witnesses today, last night, and I will tell you, after sitting through the hearing last week, or earlier this week, I guess, and listening to what occurred there, I have got to tell you, my confidence is pretty shaken in the Justice Department, and I hope we will hear today that something is happening, more than what Mr. Berry indicated, and his attorney.

I want to know about the affidavit, why it was unsealed, why wasn't it resealed. I think this case, to me, would send certainly, a chill across the land, that if you are caught up in one of these things, coming forward may not produce the results that you think it may. I mean, when Justin Berry sits here and says he wouldn't necessarily recommend that others bring their cases forward, something is broken, and I realize you have got

an open case, you may not be able to get into all the details of the case. My concern is looking at the system, and to figure out if it is working, how is it working that we don't understand, and if it is not, how do we fix it? And I hope we hear that today.

Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you. I think that concludes all the opening statements, so the first panel consists of one witness, and that is Mr. William Mercer, who is the Principal Associate Deputy Attorney General, and also, U.S. Attorney for the District of Montana, of the U.S. Department of Justice, and we do welcome you, Mr. Mercer, and I guess it is clear to everyone now, you are not our first choice, but we know that you are a prominent prosecutor, and we do look forward to your testimony.

You are aware that the committee is holding an investigative hearing, and when doing so, we have the practice of taking testimony under oath. Do you have any objection to testifying under oath this morning?

MR. MERCER. No, Mr. Chairman.

MR. WHITFIELD. Under the rules of the House and rules of the committee, you are entitled to legal counsel, but I am assuming that you don't need legal counsel. Is that correct?

MR. MERCER. That is correct.

MR. WHITFIELD. Okay. If you would, then, raise your right hand.

[Witness sworn.]

MR. WHITFIELD. Thank you very much. You are now under oath, and you may proceed with 5 minutes for your opening statement.

**STATEMENT OF WILLIAM M. MERCER, UNITED STATES  
ATTORNEY FOR THE DISTRICT OF MONTANA,  
PRINCIPAL ASSOCIATE DEPUTY ATTORNEY GENERAL,  
UNITED STATES DEPARTMENT OF JUSTICE**

MR. MERCER. Mr. Chairman, Ranking Member Stupak, and distinguished members of the subcommittee, thank you for inviting me to testify before you today about the Department of Justice's efforts to protect children from sexual exploitation on the Internet.

Unfortunately, the Internet can be used to facilitate the sexual exploitation of children. Accordingly, the Department of Justice is unequivocally committed to enforcing Federal laws in these areas, and particularly, the possession, production, and distribution of child pornography, and the use of the Internet to coerce and entice minors to--

MR. STUPAK. Mr. Chairman, I am not sure his microphone is on.

MR. MERCER. Oh, I am sorry. I don't have--now I do.



Let me turn to child pornography. Unfortunately, the very term we commonly use to describe these awful images, child pornography, does not adequately convey the horrors these images depict. A more accurate term would be images of child sexual abuse, because the production of these images involves the sexual abuse of a child. These images are, thus, permanent visual records of child sexual abuse. In the past several years, the children we have seen in these images have been younger and younger, and very regrettably, the abuse depicted has been increasingly more severe, and is often sadistic.

As if the images themselves were not harmful enough, the sexual abuse inherent in child pornography is increasingly exacerbated by pedophiles who choose to disseminate these images to millions of people over the Internet with a few clicks of a computer mouse. Once on the Internet, the images are passed endlessly from offender to offender, and perhaps used to whet the appetite of another pedophile to act out the deviant fantasies of the image on yet another child, thereby continuing the cycle of abuse.

The Department of Justice is absolutely committed to obliterating this intolerable evil. We are equally concerned about the number of online predators who lurk in chat rooms in search of kids who they hope to meet in person, for the purpose of engaging in sexual activity.

I would like to focus on what the Department of Justice has done to address this problem in the last 5 years. Prosecutors in the Criminal Division's Child Exploitation and Obscenity Section, in conjunction with Assistant U.S. Attorneys and FBI agents with our Federal partners in the Bureau of Immigration and Customs Enforcement, the United States Postal Inspection Service, and the Secret Service, and our partners in State and local law enforcement, work continuously to identify the vulnerabilities of the child pornography industry, and to attack them at every angle, both domestically and overseas.

We are focusing our efforts on everyone, from the consumer to the website operator to the facilitators, including those who provide credit card processing and the subscription services. For agents and Assistant U.S. Attorneys assigned to these cases, and for the prosecutors in the Child Exploitation and Obscenity Section who do this work every day, we do not take lightly the fact that their work revolves around review of the most troubling and graphic material, depicting children of all ages engaged in illegal sexual acts. They are engaged in this effort because they know, from their professional experience and a number of studies, that their efforts are essential to the prevention of future sexual abuse of children. The leaders in the Department of Justice are truly grateful for their efforts.

A concrete reflection of our intensified efforts is the fact that the Child Exploitation and Obscenity Section within the Department's Criminal Division has generated a more than 445 percent increase in its caseload, including child pornography cases and investigations, over the past 4 years. In addition to increasing the sheer number of investigations and prosecutions brought by the Department's prosecutors, the quality and import of the cases have increased substantially, with a focus on the producers, commercial distributors, and other high impact offenders. The Department's prosecutors in the 94 United States Attorney's offices are critical to the efforts to enforce Federal laws prohibiting crimes against children. According to the Executive Office of the U.S. Attorneys, total Federal prosecutions of child pornography and abuse cases rose from 344 cases in fiscal year 1995 to 1,576 cases in fiscal year 2005, a 358 percent increase during that time period. The number of Federal investigations of crimes against children continues to increase at an exponential rate.

Since the late 1990s, through the Department of Justice's Office of Juvenile Justice and Delinquency Prevention, Congress has funded Internet Crimes Against Children Task Forces. The ICACs have played a critical role in law enforcement's efforts to stop Internet criminal activity which poses harm to children. In just the first 6 months of calendar year 2005, ICAC investigations resulted in 3,423 State charges and 563 Federal charges. Moreover, the Attorney General has made very clear his and the Department's commitment to protecting children from sexual exploitation over the Internet. On March 15, he announced a new Department initiative, Project Safe Childhood, aimed at combating the growing threat of children being exploited online through child pornography and enticement offenses.

As this initiative is implemented in the coming months, it will provide for even better coordination by law enforcement at all levels in investigating and prosecuting child exploitation cases. It will enable us to bring even more Federal prosecutions in the area. It will make more training available for officers and prosecutors, and will further ongoing community education and awareness efforts. Through this comprehensive initiative, the Attorney General has made clear that this is an important priority for the Department. Project Safe Childhood is a true partnership. It involves the key entities in this battle, Federal law enforcement agencies and prosecutors, the ICACs, our other partners in State and local law enforcement, the National Center for Missing and Exploited Children, and other nonprofit organizations dedicated to the protection of children.

As part of our strategy to focus on the most pervasive and detrimental forms of child pornography distribution, CEOS is currently

coordinating 16 multidistrict operations involving child pornography offenders. These investigations of national impact have the potential for maximum deterrent effect on offenders. Nearly each one of the 16 investigations involve hundreds or thousands, and in a few cases, tens of thousands of offenders. It is our hope and desire to use the Project Safe Childhood initiative to ensure that the number of leads created from these major investigations are coordinated, pursued, and prosecuted in State or Federal courts.

The Department of Justice is also working to identify and rescue victims depicted in child pornography. Seven of these previously unknown adult subjects appearing in child pornography images have been profiled by America's Most Wanted and with the assistance of tips from viewers, six have been identified. More importantly, 35 victims so far, in Indiana, Montana, Texas, Colorado, and Canada, have been identified as a result of this initiative. All of the victims had been sexually abused over a period of years, some since infancy. The Department will continue to ensure that this program is utilized to its maximum potential.

Finally, at the end of successful prosecutions, it is essential that the purposes of punishment established by the Congress in the Sentencing Reform Act are met. Sentences in child pornography cases, and coercion and enticement of minors for sexual purposes cases, must deter others from committing these crimes. They must also protect the public, promote respect for the law, and incapacitate.

Early last year, the Supreme Court issued a decision in *United States v. Booker*, which altered Federal sentencing law. Before *Booker*, Federal judges were required to sentence pursuant to the sentencing guidelines. The guidelines are now merely advisory. Recently, I testified before the House Judiciary Committee on this subject, and noted the importance of making the guidelines binding again. In this area, child pornography and coercion and enticement, the Sentencing Commission reports the year after the *Booker* decision, Federal courts imposed sentences below the applicable guideline range in 26.3 percent of the cases involving possession of child pornography, and in 19.1 percent of the cases involving trafficking in child pornography. We believe that these non-guideline sentences jeopardize the purposes of punishment established by the Congress.

I appreciate the opportunity to be here today. As you noted, Mr. Chairman, I have worn the hat of a U.S. Attorney for 5 years. I have been the Chief Deputy to the Deputy Attorney General of the United States now for about 10 months. I have been very involved in the development of the Project Safe Childhood initiative, both during my time as Chairman of the Attorney General's Advisory Committee, and

now, as the Principal Associate Deputy Attorney General, and I am confident that I can be helpful to this committee, in terms of understanding what the Department has done, the tremendous efforts made on behalf of CEOS, and by a number of line prosecutors and agents, and certainly want to help the committee in its essential oversight function.

I thank you for the opportunity to be here.

[The prepared statement of William W. Mercer follows:]

PREPARED STATEMENT OF WILLIAM W. MERCER, UNITED STATES ATTORNEY FOR THE DISTRICT OF MONTANA, PRINCIPAL ASSOCIATE DEPUTY ATTORNEY GENERAL, UNITED STATES DEPARTMENT OF JUSTICE

Mr. Chairman, Ranking Member Stupak, and distinguished Members of the Subcommittee, thank you for inviting me to testify before you today about the Department of Justice's efforts to protect children from sexual exploitation on the Internet. While we recognize that the Internet can deeply enrich our lives by greatly increasing our access to all types of information, we also know that it can be exploited for criminal activity and can cause grave harm, including by facilitating the sexual exploitation of children. Accordingly, the Department of Justice is unequivocally committed to enforcing federal laws in these areas.

The Attorney General himself has made very clear his and the Department's commitment to protecting children from sexual exploitation over the Internet. On February 15th, he announced a new Department initiative, "Project Safe Childhood," aimed at combating the growing threat of children being exploited online through child pornography and enticement offenses. As this initiative begins to be implemented in the coming months, it will provide for even better coordination by law enforcement at all levels in investigating and prosecuting child exploitation cases; it will enable us to bring even more federal prosecutions in this area; it will make more training available for officers and prosecutors; and it will further ongoing community education and awareness efforts. Through this comprehensive initiative, the Attorney General has made clear that this is a priority for the Department.

Federal law, codified at Chapters 1 10 and 11 7 of Title 18, United States Code, prohibits all aspects of the child pornography trade, including its production, receipt, transportation, distribution, advertising, and possession, as well as the enticement of children to engage in unlawful sexual activity.

Unfortunately, the very term we commonly use to describe these awful images - child pornography - does not adequately convey the horrors these images depict. A more accurate term would be "images of child sexual abuse," because the production of these images involves the sexual abuse of a child. These images are thus permanent visual records of child sexual abuse. In the past several years, the children we have seen in these images have been younger and younger, and, very regrettably, the abuse depicted has been increasingly more severe and is often sadistic.

As if the images themselves were not harmful enough, the sexual abuse inherent in child pornography is increasingly exacerbated by pedophiles who choose to disseminate these images to millions of people over the Internet with a few clicks of a computer mouse. Once on the Internet, the images are passed endlessly from offender to offender and perhaps used to whet the appetite of another pedophile to act out the deviant fantasies of the image on yet another child, thereby continuing the cycle of abuse. The Department of Justice is absolutely committed to obliterating this intolerable evil.

The Department of Justice works continuously to identify the vulnerabilities of the child pornography industry and to attack them at every angle, both domestically and overseas. We are focusing our efforts on everyone, from the customer, to the website operator, to the facilitators - including those who provide credit card processing and subscription services. A concrete reflection of our intensified efforts is the fact that the Child Exploitation and Obscenity Section (CEOS) within the Department's Criminal Division has generated a more than 445% increase in its caseload, including child pornography cases and investigations, handled in the past four years. In addition to increasing the sheer number of investigations and prosecutions brought by the Department's prosecutors, the quality and import of the cases has increased substantially, with a focus on the producers, commercial distributors, and other high-impact offenders.

The Department's prosecutors in the 94 U.S. Attorney's Offices are critical to the efforts to enforce federal laws prohibiting crimes against children. According to the Executive Office for United States Attorneys, total federal prosecutions of child pornography and abuse cases rose from 344 cases in FY 1995 to 1,576 cases in FY 2005, a 358% increase. The number of federal investigations of crimes against children continues to increase at an exponential rate.

Because child pornographers continue to find ways to employ the everevolving technology of the Internet and computers to commit their deviant crimes, we in law enforcement must respond to these technological advances in order effectively to combat these crimes. In order to ensure our ability to do so, the Criminal Division created the High Tech Investigative Unit (HTIU) within CEOS in August 2002. The HTIU consists of computer forensic specialists who team with expert prosecutors to ensure the Department of Justice's capacity and capability to prosecute the most complex and advanced offenses against children committed online. HTIU computer forensic specialists render expert forensic assistance and testimony in districts across the country in the most complex child pornography prosecutions conducted by the Department. Additionally, the HTIU regularly receives and reviews tips from citizens and non-governmental organizations, such as the National Center for Missing and Exploited Children, and initiates investigations from these tips.

It is important to know that the Department's specialized expertise in this area housed at CEOS and its HTIU is disseminated nationwide, greatly enhancing federal law enforcement's fight against child pornography. CEOS conducts advanced training seminars on the investigation and prosecution of child exploitation cases attended by Assistant United States Attorneys and federal law enforcement agents from all over the country. CEOS also provides critical expert assistance to the field in a variety of other ways. CEOS attorneys are on call to answer questions from prosecutors in the field about how best to investigate or prosecute their cases. CEOS also keeps field agents and prosecutors abreast of current legal and technological developments through such mechanisms as its quarterly newsletter. Most importantly, CEOS' expert resources are widely employed by the United States Attorneys' Offices to resolve the most difficult issues presented in child exploitation cases and to ensure a successful prosecution.

Child pornography is distributed over the Internet in a variety of ways, including: online groups or communities, file servers, Internet Relay Chat, e-mail, peer-to-peer networks, and commercial websites. The Department of Justice investigates and prosecutes offenses involving each of these technologies. Sophisticated investigative techniques, often involving undercover operations, are required to hold these offenders accountable for their crimes. For example, an investigation of a commercial child pornography website requires us not only to determine where the servers hosting the website are located and who are the persons responsible for operating the website, but also to follow the path of the financial transactions offenders use to purchase the child pornography, whether by credit card or other means. Such cases require detailed information about all aspects of the transaction in order to determine the identity and

location of the offenders. Additionally, many of these cases require coordination with law enforcement from other countries. It is essential that these complex cases be handled by law enforcement agents and prosecutors with the necessary specialized expertise.

To defeat the misuse of these various technologies, however, the Department must demonstrate equal innovation to that being shown by the online offenders. For example, CEOS' HTIU has developed a file server investigative protocol and software programs designed to identify quickly and locate individuals distributing pornography using automated file-server technology and Internet Relay Chat. Because file servers, or "f-servers," provide a highly effective means to obtain and distribute enormous amounts of child pornography files, 24 hours a day and 365 days a year, with complete automation and no human interaction, this trafficking mechanism is a premier tool for the most egregious child pornography offenders. The protocol recommends standards for identifying targets, gathering forensic evidence, drafting search warrants, and making charging decisions. It is designed for both agents and prosecutors to ensure that all aspects of these relatively complex investigations are understood by all members of the law enforcement team. The software program written by the HTIU automates the process of stripping from the computers used as file-servers all of the information necessary to make prosecutions against all of the individuals sharing child pornography with the file-server computer.

In addition, law enforcement has launched several national enforcement initiatives against the use of peer-to-peer networks to commit child pornography offenses. These initiatives encompass operations by the FBI, the Department of Homeland Security, Immigration and Customs Enforcement (ICE), and state and local Internet Crimes Against Children Task Forces, which are funded through the Department's Office of Justice Programs. To give you a sense of the scope and impact of federal law enforcement's operations, FBI's "Operation Peer Pressure," as of January 2006, has resulted in over 300 searches, 69 indictments, 63 arrests; and over 40 convictions.

In addition, in recognition of the growing threat to children posed by the Internet, as part of the fiscal year 1998 Justice Appropriations Act (Pub. L. No. 105-1 19), the Department's Office of Juvenile Justice and Delinquency Prevention (OJJDP) created a national network of state and local law enforcement cyber units to investigate cases of Internet crimes against children. The result is the Internet Crimes Against Children (ICAC) Task Forces. The ICAC Task Force program helps state and local law enforcement agencies develop an effective response to cyber enticement and child pornography cases. The help consists of forensic and investigative components, training and technical assistance, victim services, and community education. Forty-six task forces have been established throughout the nation. The ICAC program was developed to address the increasing number of children and teenagers using the Internet, the proliferation of child pornography, and heightened online activity by predators searching for unsupervised contact with underage victims.

ICACs have played a critical role in law enforcement's efforts to stop Internet criminal activity which poses harm to children. In FY 2003, ICACs received 3,741 reports of Internet crimes against children, including but not limited to travel, enticement and child pornography complaints. In FY 2004, that number rose to 24,138. In FY 2005, ICACs received 198,883 complaints of Internet crimes against children. The largest number of complaints (154,545) were reports of child pornography distribution, and the second largest number (34,062) were complaints of child pornography manufacturing. The dramatic increase from FY 2004 to FY 2005 in the number of child pornography manufacturing and distribution complaints is linked to ICAC undercover operations in Internet based file sharing applications (*i.e.*, peer-to-peer networks). ICAC Task Forces efforts are resulting in the prosecution of many cases. For example, in the first six months of calendar year 2005, ICAC investigations resulted in 3,423 state charges and 563 federal charges.

Also, as part of our strategy to focus on the most pervasive and detrimental forms of child pornography distribution, CEOS is currently coordinating 16 multidistrict operations involving child pornography offenders. These investigations of national impact have the potential for maximum deterrent effect on offenders. Nearly each one of the sixteen investigations involves hundreds or thousands, and in a few cases tens of thousands, of offenders. The coordination of these operations is complex, but the results can be tremendous. By way of example, the FBI is currently investigating the distribution of child pornography on various Yahoo! Groups, which are "member-only" online bulletin boards. As of January 2006, the FBI indicated that the investigation has yielded over 180 search warrants, 89 arrests, 162 indictments, and over 100 convictions.

The Department of Justice is also working to identify and rescue victims depicted in images of child pornography. One method for achieving this goal is already underway. The FBI Endangered Child Alert Program (ECAP) was launched on February 21, 2004, by the FBI's Innocent Images Unit, and is conducted in partnership with CEOS. The purpose of ECAP is proactively to identify unknown offenders depicted in images of child pornography engaging in the sexual exploitation of children. Since ECAP's inception, seven of these "John Doe" subjects have been profiled by *America's Most Wanted*, and with the assistance of tips from viewers, six have been identified. More importantly, 35 victims (so far) in Indiana, Montana, Texas, Colorado, and Canada have been identified as a result of this initiative. All of the victims had been sexually abused over a period of years, some since infancy. The Department will continue to ensure that this program is utilized to its maximum potential.

The Department recently has had significant success in destroying several major child pornography operations. Three examples are an operation announced by Attorney General Gonzales on March 15, 2006, in which 27 individuals in four countries have been charged with child pornography offenses, the case of *United States v. Mariscal* (S.D. Fla.), and the *Regpay* case, which was followed by *Operation Falcon* (D.N.J.).

In the recent operation announced by the Attorney General, a private Internet chat room was used by offenders worldwide to facilitate the trading of thousands of images of child pornography - including streaming videos of live molestations. The chat room was known as "Kiddypics & Kiddyvids," and was hosted on the Internet through the WinMX software program that also allowed users to engage in peer-to-peer file sharing. The chat room was infiltrated in an undercover investigation, resulting in charges against 27 individuals to date in the United States, Canada, Australia, and Great Britain (13 of these 27 have been charged in the United States). One of the 27 charged defendants is a fugitive. Seven child victims of sexual molestation have been identified as a result of the investigation, and four alleged molesters are among the 27 defendants charged to date in the continuing investigation. This investigation underscores the tremendous scope of many child pornography offenses and the necessity of an international law enforcement response. Demonstrating our ability to work together effectively to fight these crimes, the Department of Justice, the U.S. Immigration and Customs Enforcement, state and local authorities, Internet Crimes Against Children Task Forces, and international law enforcement agencies have cooperated successfully in this investigation.

In the *Mariscal* case, Angel Mariscal received a 100-year prison sentence on September 30, 2004 in the Southern District of Florida, after he was convicted on seven charges including conspiracy to produce, importation, distribution, advertising, and possession with intent to sell child pornography. Mariscal traveled repeatedly over a seven-year period to Cuba and Ecuador, where he produced and manufactured child pornography, including videotapes of Mariscal sexually abusing minors, some under the age of 12. As a result of Mariscal's arrest, his customers across the country were targeted in Operation Lost Innocence, which was coordinated by the U.S. Postal Inspection Service and CEOS. To date, Operation Lost Innocence has resulted in 107 searches, 55 arrests/indictments, and 44 convictions.

The *Regpay* (D.N.J.) case, which led to *Operation Falcon*, is an example of how one child pornography investigation into the activities of individuals involved in a commercial website operation can lead to the apprehension of thousands of other offenders. Regpay was a Belarus-based company that provided credit card processing services to hundreds of commercial child pornography websites. Regpay contracted with a Florida company, Connections USA, to access a merchant bank in the United States. In February 2005, several Regpay defendants pled guilty to various conspiracy, child pornography, and money laundering offenses in the District of New Jersey. Connections USA and several of its employees also pled guilty in connection with this case. The Regpay investigation spawned the U.S. Immigration and Customs Enforcement's "Operation Falcon," an international child pornography trafficking investigation that, as of February 2006, has resulted in 372 open investigations, 579 search warrants, 341 domestic and approximately 703 foreign arrests, and 254 indictments, generating 241 convictions.

In addition to these efforts to protect children from online sexual exploitation, the Department is also involved in two key efforts to protect children from commercial sexual exploitation. The first of these is the "Innocence Lost Initiative," which combats domestic child prostitution. The Innocence Lost Initiative is conducted by CEOS in partnership with the Violent Crimes and Major Offenders Section of FBI Headquarters and the National Center for Missing and Exploited Children, and has so far resulted in at least 139 open investigations, 505 arrests, 60 complaints, 70 indictments, and 67 convictions. The second is our initiative to protect children from child sex tourism. Since the passage of the PROTECT Act in April 2003, which facilitated the prosecution of these cases, there have been approximately 50 sex tourism indictments or complaints and at least 29 convictions. While investigations of these types of cases are harder to track, we believe the number of active sex tourism investigations is roughly 60.

#### **Conclusion**

In these brief comments, I hope to have given you a sense of the Department of Justice's efforts to protect children from sexual exploitation on the Internet. We consider this a critically important task and will continue to do our utmost to protect children as well as society at large by enforcing these statutes.

Mr. Chairman. I again thank you and the Subcommittee for the opportunity to speak to you today, and I would be pleased to answer any questions the Subcommittee might have.

MR. WHITFIELD. Well, thank you for your testimony.

Mr. Mercer, I want to get a better understanding of the layers of organizational supervision over the CEOS section in decision-making at the Department, and it is my understanding that Drew Oosterbaan is the head of the section. Is that correct?

MR. MERCER. He is the head of CEOS, yes.

MR. WHITFIELD. Okay. And that section is part of the Criminal Division. Is that correct?

MR. MERCER. That is correct.

MR. WHITFIELD. And Mr. Oosterbaan reports to the Deputy Assistant Attorney General for the Criminal Division.

MR. MERCER. That is also correct.

MR. WHITFIELD. And her name is Laura Parks.

MR. MERCER. That is correct.



MR. WHITFIELD. And Mrs. Parsky reports to the Assistant Attorney General for the Criminal Division, who is Alice Fisher, is that correct?

MR. MERCER. That is correct.

MR. WHITFIELD. And Alice Fisher reports to Paul McNulty, the Deputy Attorney General.

MR. MERCER. That is correct, and that is who I work for.

MR. WHITFIELD. And you work for McNulty.

MR. MERCER. Correct.

MR. WHITFIELD. And McNulty reports to the Attorney General, Mr. Gonzalez.

MR. MERCER. That is correct.

MR. WHITFIELD. Okay. And that is the line of review for any decisions made by the Chief of the CEOS section?

MR. MERCER. That is an accurate description of the hierarchy that the Department of Justice has for that section. That is correct.

MR. WHITFIELD. Now, could you explain what your role is as Principal Associate Deputy Attorney General, as it relates to the decision-making at CEOS, the Child Exploitation and Obscenity Section?

MR. MERCER. Yeah, and in fact, if I can give a little additional context, obviously, the Deputy Attorney General has general, as sort of a chief operating official for the Department of Justice. The Federal Bureau of Investigation is part of the Department of Justice. Many other components are part of the Department of Justice. There are occasions where the Office of the Deputy Attorney General is asked to referee various conflicts, and in this area, our office would get involved, to the extent that there were different issues that needed to be resolved, where say, an Assistant U.S. Attorney, or a U.S. Attorney challenged the way a case was being worked, to the extent that there was a conflict with another section of the Department.

So, it is important, I think, for the committee to understand that CEOS plays a crucial role in coordinating cases, in leading these multi-jurisdictional investigations, providing advice, training, and counsel, but you also have within the United States, 93 U.S. Attorneys and 94 districts, and you have a number of Assistant U.S. Attorneys around the country that are also responsible for prosecuting these cases. As is reflected in my statement, that is how we have been able to charge such a large number of cases. We have charged 1,500 cases involving child pornography and coercion and enticement just in fiscal year 2005.

MR. WHITFIELD. Okay.

MR. MERCER. So, that is the role that we play, and I mentioned this Project Safe Childhood initiative. The Deputy Attorney General has worked very closely with the Attorney General in shaping that initiative,

which we believe is going to lead to even greater production in this area the committee is so interested in.

MR. WHITFIELD. Well, today, one of the focuses of this hearing relates to information that came out of Justin Berry's testimony, and that, particularly, relates to CEOS and their decisions, because he provided them with a lot of information regarding 1,500 people that were using his website, credit card numbers, whatever whatever. And so, I would like to ask you, do you have any decision-making authority over CEOS yourself?

MR. MERCER. No. CEOS reports to the Assistant Attorney General for the Criminal Division, but I think, given my role as a U.S. Attorney, what I have seen in the country, what I have seen in my work in the Deputy Attorney General's Office, I can be helpful to the committee, not in terms of talking about this specific investigation, which the Department wouldn't do.

MR. WHITFIELD. Yeah.

MR. MERCER. If the committee had said we want to ask about why a person was charged, why a case was declined, why an investigation was pursued this way, that isn't something we are going to do during the pendency of a case, but I think I can be helpful, in terms of understanding how these cases are made, and it would be of value to the committee.

MR. WHITFIELD. Well, I do hope that you will report back to them that, since you don't have any decision-making over CEOS at all, and you do have a broad background in criminal justice and prosecution, but we were specifically interested in the CEOS decision-making as it relates to this case, and I hope you would convey our disappointment about that.

Now, did you have any involvement in Justin Berry's immunity agreement?

MR. MERCER. No.

MR. WHITFIELD. All right.

MR. MERCER. But again, Mr. Chairman, it wouldn't matter who the Department's witness was. The Department doesn't participate in ongoing discussions when we have a case that is pending. That is something that certainly would not advance the purpose--

CHAIRMAN BARTON. Would the Chairman yield on that point?

MR. WHITFIELD. Yes, sir.

CHAIRMAN BARTON. What is the appropriate title that I should call you, Mr. Deputy, or Mr. Attorney General, or Mr. Associate Principal Deputy? I mean, I am a little confused here.

MR. MERCER. I wear two hats. I am the U.S. Attorney in the District of Montana, and I am also the Principal Associate Deputy Attorney General, so--

CHAIRMAN BARTON. What do you want me to call you?

MR. MERCER. Mr. Mercer is fine.

CHAIRMAN BARTON. Okay, Mr. Mercer. Have you ever actually led an investigation or prosecuted a case?

MR. MERCER. Oh, yeah. I was an Assistant U.S. Attorney for 7 years before I became a U.S. Attorney.

CHAIRMAN BARTON. All right. When you were leading this investigation or prosecuting this case, I assume that you wanted to talk to the witnesses, if possible, if you knew who they were, to the crimes that were committed. Is that true or not true?

MR. MERCER. Well, actually, the role of investigating cases is typically carried out by investigative agencies, so in the FBI--

CHAIRMAN BARTON. Well, let us say the investigative agency that you were working with, you said this is the investigation. Here is who you need to go see. They went out and came back, said oh, those people don't want to talk to us. But their best friends, or their boyfriend or their girlfriend, who they talked to the case about, will talk to us, how did you take that?

MR. MERCER. I am not sure I understand the question.

CHAIRMAN BARTON. Well, let me be clear. We didn't ask for you. Okay? We have asked for Laura Parsky, who is in the direct line of chain of command. We didn't get her. We have asked her for Alice Fisher. We didn't get her. We have asked for Drew Oosterbaan. We didn't get him. We got you. Now, you are a fine gentleman, but you are not even in the line of command. You are staff. You have no control over this. You probably had to be briefed to come testify. Now, let me be straight. I am calling the Attorney General, my friend from Texas, who I know personally. We are going to get the people we want, one way or the other. Do you understand that? Not that I am not impressed with your background, but when you are conducting your investigations, you don't talk to secondary people. You talk to the people you want to talk to. When the FBI is conducting an investigation, they talk to the people they want to talk to. They don't talk to, well, we can't talk to you, but go see the neighbor down the street. Mr. Whitfield is much more polite than I am, but I am fed up with this. I had to call the Attorney General to get you here, and it is not that we are not impressed with you, don't misunderstand me, but you are not the people that are doing this. We want to work with you, but in order to do that, we have got to get the people that are actually doing the work. We could have picked somebody at random in the audience, and gave them a 30-minute brief, and they could have testified to what you testified to.

MR. MERCER. Well, Mr. Chairman, I am confident that I can be helpful to the committee.

CHAIRMAN BARTON. Well, you had better start.

MR. MERCER. Not only because I have done this work as an Assistant U.S. Attorney, and then a U.S. Attorney, and then as Chair of the Attorney General's Advisory Committee.

CHAIRMAN BARTON. Your credentials are not at risk. We are not questioning your credentials as an admirable citizen, but we are questioning the judgment of the Justice Department of the United States of America, who seems to think they can thumb its nose at the Congress of the United States.

MR. MERCER. Well, we--

CHAIRMAN BARTON. And that will not happen. I am going to tell the Attorney General straight, but you go back and tell him for me, or report to the Deputy Attorney General, who will report to the Attorney General, that we are going to hold another hearing, and these people are going to be here. Now, if you want to sit out in the audience, that is fine. If you want to stand up beside him and hold their hand, that is fine. They are going to be here, and hopefully, the cameras will be here, and the committee will be here, and we will finally get this investigation going.

I yield back to you, Mr. Chairman.

MR. WHITFIELD. Well, thank you, Mr. Chairman, and I think Mr. Mercer gets a clear understanding of how we feel about this issue, and there is a lot of cynicism about the Congress in a lot of different areas, but in this area of child pornography, when we do request certain people from the Justice Department, who are involved in the investigations, they can talk to us specifically about issues, and then they just thumb their nose and do not attend the hearing, it does upset all of us, and it particularly upsets us that in the Justin Berry case, when 1,500 names were given to the Justice Department, to the CEOS section, and individual names and pictures of young children being molested, in danger, given to the Department, and still no action has been taken, it is something that we find particularly upsetting

And let us see, my time has expired as well now, so I will recognize the gentleman from Michigan, Mr. Stupak.

MR. STUPAK. Mr. Chairman, in light of not having the witnesses we need, why don't we just adjourn this hearing until we get the witnesses we need? We have subpoena power on this committee. I urge that we use our subpoena power. And we have next panel, one, two, three, four, five, six, seven people, that I don't think are going to be able to provide us any information. I mentioned two other people in my opening statement I would like to see here. They are not here.

You went through a list of people you requested. They are not here. I think on this side, on both sides of the aisle here, we are frustrated with not having the people who can answer questions.

CHAIRMAN BARTON. Will the gentleman yield?

MR. STUPAK. Yes, sir.

CHAIRMAN BARTON. We may want to release Mr. Mercer, but some of the other witnesses that are here on the second panel, from the Postal Service and the Immigration Service have been working with the committee, and I think we need to give them a chance to testify. I am not at all opposed, if it is the will of the committee, to--

MR. STUPAK. Then I would move we let Mr. Mercer go until we get the people from Justice we need, and then, let us bring the other witnesses up and do their opening statements. We will have votes here in a few minutes, and let them do their openings, and let us go move on, because we don't want to waste everyone's time with a witness that can't answer questions.

MR. WHITFIELD. Is there any objection to releasing Mr. Mercer? Well, then, Mr. Mercer, you are released, and thank you for being here today.

At this time, I will call the second panel: Mr. William Kezer, who is the Deputy Chief Inspector for the U.S. Postal Inspection Service; Mr. Raymond C. Smith, Assistant Inspector in Charge for Child Pornography and Adult Obscenity, the U.S. Postal Inspection Service; Mr. John Clark, Deputy Assistant Secretary for U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security; Mr. James Plitt, Director, Cyber Crimes Center, Office of Investigations, U.S. Immigration and Customs Enforcement, at the Department of Homeland Security; Mr. Frank Kardasz, Sergeant, Phoenix Police Department, Project Director for the Arizona Internet Crimes Against Children Task Force; Mr. Flint Waters, Lead Special Agent of the Wyoming Division of Criminal Investigation, Internet Crimes Against Children Task Force; and Mr. Chris Swecker, who is the Acting Assistant Executive Director for the FBI, U.S. Department of Justice.

I want to thank all of you gentlemen for being with us here today, and as you know, this is an Oversight and Investigations hearing, and it is our practice to take testimony under oath. Do any of you object to testifying under oath, and do any of you have a need for an attorney today?

Then, if you would please stand, and I would like to swear you in. Raise your right hand.

[Witnesses sworn.]

MR. WHITFIELD. Thank you very much. All of you are now under oath, and Mr. Swecker, you are recognized for 5 minutes for your opening statement.

**STATEMENTS OF CHRIS SWECKER, ACTING ASSISTANT EXECUTIVE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE; JAMES PLITT, DIRECTOR, CYBER CRIMES CENTER, OFFICE OF INVESTIGATIONS, UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT, UNITED STATES DEPARTMENT OF HOMELAND SECURITY; DR. FRANK KARDASZ, SERGEANT, PHOENIX POLICE DEPARTMENT, PROJECT DIRECTOR, ARIZONA INTERNET CRIMES AGAINST CHILDREN TASK FORCE, UNITED STATES DEPARTMENT OF JUSTICE; FLINT WATERS, LEAD SPECIAL AGENT, WYOMING DIVISION OF CRIMINAL INVESTIGATION, INTERNET CRIMES AGAINST CHILDREN TASK FORCE TECHNOLOGY CENTER, UNITED STATES DEPARTMENT OF JUSTICE; JOHN P. CLARK, DEPUTY ASSISTANT SECRETARY, UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT, UNITED STATES DEPARTMENT OF HOMELAND SECURITY; WILLIAM E. KEZER, DEPUTY CHIEF INSPECTOR, UNITED STATES POSTAL INSPECTION SERVICE; AND RAYMOND C. SMITH, ASSISTANT INSPECTOR IN CHARGE, CHILD PORNOGRAPHY AND ADULT OBSCENITY, UNITED STATES POSTAL INSPECTION SERVICE**

MR. SWECKER. Good morning, Mr. Chairman, and I do appreciate the opportunity to come here today to talk to the committee.

Let me talk a little bit about our Innocent Images Initiative, and define the scope of the problem, as you already know. As the National Center for Missing and Exploited Children has reported, one in five children will be solicited while online. Unfortunately, only 10 percent of these children will ever report it. In its 8 years of operation, the Cyber TipLine has generated over 385,000 leads, and reports of online enticement have increased by 400 percent.

The FBI's Innocent Images Initiative, formed in 1993, is comprised of 36 undercover operations nationwide. These operations involve FBI agents working online in an undercover capacity to seek child predators and individuals responsible for the production, dissemination, and possession of child abuse images. This is accomplished by using a variety of techniques, including purchasing child abuse images from commercial websites, creating online personas to chat in predicated chat rooms, and co-opting predators' email accounts. Our primary focus is addressing child pornography or documented child abuse websites,

where predators are featured abusing children and profit from these terrible crimes. These investigations always span multiple jurisdictions, and usually expand beyond the borders of the United States. The FBI has taken a global approach in addressing this problem, by closely partnering with several countries, who work side by side with FBI agents in a task force setting. As I sit here today, officers from Norway, Thailand, the Philippines, and Belarus are working with our agents just a few miles from where we are here. Additionally, task force membership includes officers from 11 other countries and Europol.

Other priorities include persons or groups who engage in production of child abuse images, as the production of this material signifies the violent rape or sexual abuse of a child.

We also investigate sexual predators who travel from one jurisdiction to another to engage in sex with minors. These persons are particularly dangerous, as they have gone beyond merely looking at images, and have now engaged in activity to make contact with a child. However, these predators often find a cadre of agents and task force officers on the other end. Persons with large collections of child abuse images also represent a danger, as we find a large percentage of those we arrest for possession are also committing contact offenses with minors.

Over the past 10 years, the Innocent Images program has grown exponentially. Between fiscal years 1995 and 2005, there has been a 2050 percent increase in cases opened, from 113 to 2,500. During this 10-year period, the program has recorded over 15,556 cases opened, over 4,700 criminals charged, over 6,100 subjects arrested, over 4,800 convictions obtained. These cases, which led to these statistics, were multi-jurisdictional with no geographical boundaries, and both national and international in scope.

We have come a long way from the early electronic bulletin boards that predated the Internet. Today, an estimated 21 million teenagers use the Internet, with 50 percent online daily. As these children use the computer more and more, online predators take advantage of emerging technologies to facilitate their unimaginable criminal activities.

Today, this program is an intelligence-driven, proactive, multi-agency initiative that pursues offenders who utilize websites, chat rooms, peer-to-peer networks, instant messaging programs, eGroups, newsgroups, file servers, and other online services. To address all of our priorities, this program readily draws on the resources of State, local, and Federal, and now international law enforcement partners.

While conducting these investigations, agents have found documented child abuse to be readily available using the most basic of search terms. As an example, child abuse images were easily available

when innocuous search terms, such as “Britney Spears” or the word “young” were used.

Through the use of covert techniques and administrative subpoenas, agents can determine which individual users possess and distribute these images over the Internet. Using search warrants, interviews, and computer forensic tools, our agents can strengthen their cases to eventually arrest and prosecute the criminals.

As you may have noticed, I have not used the word “child pornography,” because it does not adequately describe the type of crime that we are talking about today. To some people, pornography may imply adult models posing for the camera. “Child pornography” does not describe the reality of the crime problem we are facing today. This crime deals with the violent rape and sexual exploitation of young children, some as young as a few months old. Therefore, each image represents evidence of the criminal reality of a violent rape or sexual abuse.

The FBI has partnered with the National Center for Missing and Exploited Children in a significant and meaningful way. Currently, there are two Special Agents and four FBI analysts assigned full time at the Center, and in March of 2005, we merged our database, the Child Victim Identification Program, with that housed at the Center. The merger has drastically increased the number of known victims in the database, and has made the data available to all other law enforcement agencies that investigate these violations. Ultimately, this partnership benefits both the FBI and the Center, but more importantly, it benefits the public and the children we serve.

I am not sure about time here, sir. How much time do I have?

MR. WHITFIELD. You are about 10 seconds over.

MR. SWECKER. Okay. All right. Well, I would just rest on the rest of the data in my opening statement.

MR. WHITFIELD. Okay.

MR. SWECKER. And I would just say that I am, first and foremost, I am a Special Agent. I have come through the ranks. I have supervised investigations of this nature. I hope I can help you today.

[The prepared statement of Chris Swecker follows:]

PREPARED STATEMENT OF CHRIS SWECKER, ACTING ASSISTANT EXECUTIVE DIRECTOR,  
FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE

Good Morning Chairman Whitfield, Ranking Member Stupak, and other members of the Subcommittee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI’s role in combating the sexual exploitation of children through the use of the Internet.

As the National Center for Missing and Exploited Children (NCMEC) has reported, one in five children will be solicited while online. Unfortunately, only ten percent of



these children will report it. In its eight years of operation, the Cyber tipline has generated over 385,000 leads and reports of online enticement have increased by four hundred percent.

The FBI's Innocent Images National Initiative is comprised of thirty six under-cover operations nationwide. These operations involve FBI Agents working on-line in an undercover capacity to seek child predators and individuals responsible for the production, dissemination, and possession of child abuse images. This is accomplished by using a variety of techniques, including purchasing child abuse images from commercial web sites, creating on-line personas to chat in predicated chat rooms, and co-opting predators' e-mail accounts. Our primary focus is addressing commercial child abuse image websites where predators are featured abusing children and which profit from their terrible crimes. These investigations always span multiple jurisdictions and usually expand beyond the borders of the United States. The FBI has taken a global approach in addressing this problem by closely partnering with several countries who work side by side with FBI agents in a task-force setting. As I sit before the Subcommittee today, officers from Norway, Thailand, the Philippines, and Belarus are working with our agents just a few miles from here. Additionally, task force membership includes officers from 11 other countries and Europol.

Other priorities include persons or groups who engage in the production of child abuse images, as the production of this material signifies the violent rape or sexual abuse of a child.

We also investigate sexual predators who travel from one jurisdiction to another to engage in sex with minors. These persons are particularly dangerous as they have gone beyond merely looking at images and have now engaged in activity to make contact with a child. However, these predators often find a cadre of FBI agents and task force officers on the other end of their travel. Persons with large collections of child abuse images also represent a danger as we find a large percentage of those we arrest for possession, are also committing contact offenses with minors.

Over the past 10 years, the Innocent Images program has grown exponentially. Between fiscal year 1996 and 2005, there has been a 2050% increase in cases opened (113 to 2500). During this ten-year period, the program has recorded over 15,556 cases opened; 4,784 criminals being charged; 6,145 subjects being arrested; and 4,822 convictions obtained. The cases which led to these statistics were multi-jurisdictional with no geographical boundaries, and both national and international in scope.

We have come a long way from the early electronic bulletin boards that pre-dated the Internet. Today an estimated 21 million teenagers use the Internet, with 51 percent online daily. As children use computers more and more, online child predators take advantage of emerging technologies to facilitate their unimaginable criminal activities.

Today, this program is an intelligence-driven, proactive, multi-agency investigative effort, that pursues offenders who utilize websites, chat rooms, peer-to-peer networks, Instant Messaging programs, eGroups, NewsGroups, File Servers, and other online services to sexually exploit children. To address all of our priorities, this program readily draws on the resources of its federal, state, local, and now international law enforcement partners.

While conducting these investigations, FBI agents have found child sexual abuse images to be readily available using the most basic of search terms. As an example, child abuse images were easily available when innocuous search terms were used, such as "Brittney Spears" or the word "young."

Through the use of covert investigative techniques and administrative subpoenas, FBI agents can determine which individual users possess and distribute child abuse images over the Internet. Furthermore, utilizing search warrants, interviews, and computer forensic tools, our agents can strengthen their cases to eventually arrest and prosecute these dangerous criminals.

As you may have noticed throughout my presentation, I have not used the phrase "child pornography," because it does not adequately describe the type of crime we are talking about today. To some people, pornography may imply adult models posing for the camera. Child pornography does not describe the reality of the crime problem we are facing today. This crime deals with the violent rape and sexual exploitation of young children, some as young as a few months old. Therefore, each image represents evidence of the criminal reality of a violent rape, or sexual abuse of a child.

The FBI has partnered with NCMEC in a significant and meaningful way. Currently there are two FBI Special Agents and four FBI support personnel assigned full time at the Center. Further, in March of 2005, the FBI merged its Child Victim Identification Program (CVIP) Database with that housed at the National Center. This merger has drastically increased the number of known victims in the CVIP database and has made FBI data available to all other law enforcement agencies that investigate these violations. Ultimately this partnership benefits both the FBI and the National Center, but more importantly it benefits the children we serve.

In June of 2003, the FBI, along with our partners in the Department of Justice, Child Exploitation and Obscenity Section, and NCMEC implemented the "Innocence Lost National Initiative" to address the growing problem of child prostitution. Initially, the FBI identified 14 field offices with a high incidence of child prostitution. In FY 2005 and through the first quarter of FY 2006, an additional ten field offices were identified as areas in which these criminal enterprises were operating. These criminal enterprises use the Internet to advertise the children they have forced or tricked into prostitution, often masquerading as escort services, which leads to further victimization of the children.

These investigations are manpower intensive, intelligence driven and make use of sophisticated investigative techniques such as Title III wiretaps. To date, five FBI field offices have utilized Title III wiretaps in these investigations. As a result, since FY 2004, 166 cases were opened, 28 criminal enterprises disrupted, 16 enterprises dismantled, 101 individuals indicted, 75 subjects convicted and 80 seizures claimed. Since the inception of Innocence Lost, over 300 children have been recovered.

According to NCMEC, in FY 2005 there were 7,000 reports of endangered runaways and 774 reports of children involved in or suspected of being involved in child prostitution. FBI personnel assigned to the NCMEC review these intake reports daily and disseminate the information to the appropriate FBI field office for investigation.

#### **Conclusion**

In closing, the FBI looks forward to working with other Law Enforcement agencies, private industry, and the Department of Justice's prosecutors in continuing to combat this heinous crime problem. The protection of our children requires the combined efforts of all sectors of our society. I would like to express my appreciation to the Subcommittee for addressing this very serious problem, and I would also like to thank Chairman Whitfield, Ranking Member Stupak, and the Subcommittee for the privilege of appearing before you today.

MR. WHITFIELD. Thank you very much. And Mr. Plitt, you are recognized for your 5 minutes, and you are Director of the Cyber Crimes Center at the Homeland Security.

MR. PLITT. Yes, Mr. Chair. I appreciate the opportunity to present some additional information about the Cyber Crimes Center today, its responsibilities with respect to investigating child exploitation.

Our Cyber Crime Center is C3, recognized nationally and internationally as a leader in the investigation of international criminal

activities conducted or facilitated by the Internet. Created in 1997, C3 brings the full range of ICE's technical services, such as digital media forensics, and cyber investigative services together in a single location to investigate the cyber aspects of violations of immigration and customs law. Contrary to general perceptions, C3 does not currently investigate what would be termed as more traditional cyber crimes, as hacking, denial of service, or phishing. In addition to trans-border child exploitation crime, C3 investigates other trans-border crimes, such as international money laundering, illegal cyber banking, illegal arms trafficking, derivative pharmaceuticals sold over the Internet, intellectual property rights violations.

C3 essentially serves as the mission control for ICE's Internet-related investigations by refining investigative leads generated by domestic and international sources, validating those leads, that constitute immigration and customs violations, and working in partnership with the ICE field offices to implement the various investigations through national training, best practices. Meeting with our foreign counterparts and more than 50 attaché locations, C3 builds strong international partnerships that are crucial to the trans-border category of investigations.

ICE derives its trans-border child exploitation investigative authorities from its customs responsibility to prevent the smuggling of contraband, such as child pornography, and its immigration responsibility, to investigate and administratively remove foreign nationals guilty of crimes of moral turpitude. As a result, ICE limits its child exploitation investigations to two situations: one, when there is a reasonable nexus to the U.S. border; and when, as a second situation, when ICE's assistance is specifically requested by international, Federal, State, or local law enforcement prosecutors. Currently, ICE participates in approximately 60 of the Internet Crimes Against Children Task Forces across the country, to assist their State and local law enforcement officers with the trans-border component of their investigations.

Through this trans-border specialization, ICE is able to focus its resources to achieve better resource efficiency and develop investigative projects that maximize the international partnerships. C3's Child Exploitation Section coordinates their responsibilities through Operation PREDATOR, the program that organizes trans-border child exploitation investigations, including those of criminal alien child predators, international child sex tourists, international smugglers and traffickers of children for sexual purposes, and Internet child pornographers.

ICE, through the Crimes of Exploitation Section, has achieved notable operational efficiencies. For example, with less than 3 percent of ICE's worldwide investigative resources, ICE manages more than 1,000

investigations annually, concerning international child sex tourism, and international Internet child pornography cases alone.

Previous testimony from Mr. Clark is going to detail some of those accomplishments. C3's Child Exploitation Section is also responsible for managing and implementing all phases of the systems development life cycle for the National Child Victim Identification System. Mr. Clark will go into more detail about that, as well.

And C3 is responsible for maintaining partnerships with non-government organizations. Some of the non-government organizations would include the National Center for Missing and Exploited Children, ECPAT, i-SAFE, and World Vision. With respect to the Internet portion of ICE's international child exploitation investigations, C3 supports the ICE offices, and upon request, foreign law enforcement operations, by providing training and investigative support. While prudence recommends that the details of C3's technical investigative methods perhaps not be communicated in a public forum, some appropriate examples would include the development of undercover websites, making undercover purchases of websites, and communicating through undercover methods with investigative targets. C3 provides these services on investigations involving all Internet technologies, including commercial and noncommercial websites, peer-to-peer groups, newsgroups, and Internet Relay Chat channels.

C3 will continue patrols on all these Internet environments for the trans-border aspect of individual illegal downloads, criminal conspiracies, and illegal commercial operations, through its presence in public areas and court-ordered intercepts. C3 draws on ICE's renowned international money laundering prowess to trace associated financial transactions, including the new e-currency methods, and of course, to seize instrumentalities and proceeds.

C3's latest endeavor involves the development and implementation of systems, telecommunications, and operational processes that directly link to the international Internet child exploitation investigative organizations of other countries. The end result is innovative, collaborative project, maybe the implementation of the first non-investigation-specific virtual, worldwide law enforcement task force on trans-border child exploitation.

In summary, ICE investigations focus on the trans-border aspect of child exploitation over the Internet. These investigations are organized under Operation PREDATOR, and coordinated by ICE C3. ICE is honored to work with any individual or organization that is interested in protecting children, making the Internet a safe and enjoyable place. ICE C3 knows that it cannot alone substantially impact the macro problem of Internet child safety.

A coordinated, cooperative approach between all the aforementioned participants is vital, and the most important participants on these teams are parents. Parents are physically and emotionally closer to teach and guard the potential victims, the children. Parents, in addition to the children, are also the most impacted by the offline consequences of online behavior.

Thank you.

MR. WHITFIELD. Thank you. Dr. Kardasz, you are recognized for 5 minutes, and you are Project Director of the Arizona Internet Crimes Against Children Task Force, and we welcome you.

MR. KARDASZ. Thank you, Mr. Chairman, and distinguished members of the committee, thank you for permitting me to speak today.

Arizona joined the ICAC, you will also hear it called ICAC, Task Force Program in the year 2000. We work cooperatively with our law enforcement colleagues from the FBI, ICE, Postal Inspection Service, and the Secret Service. Although the names of our agencies differ, we share the common goal of trying to keep children safe from Internet sexual predators and child pornographers.

The Arizona ICAC Task Force has recorded over 2,000 investigations and over 200 arrests. Although Arizona has the toughest laws in the Nation against child pornography, this has not stopped the trafficking of unlawful images, and like all of our colleagues nationwide, we have many more solvable case files at the ready than we have personnel and resources to bring in the offenders. Sadly, while these cases await investigation, children and teens continue to suffer at the hands of Internet sex offenders.

I have had the opportunity to speak with many citizen groups about Internet crime, and at the end of each presentation, there is often some senior individual in the group who raises his hand and says: "Why don't they just shut that dang Internet thing off?" As if we have a control panel somewhere with a dial that we can turn, and it will regulate Internet misconduct.

Your legislation is the closest thing we have to an Internet control dial, and although opponents of controls argue that regulations are costly, imperfect, and violations of Constitutional freedoms, I sometimes wonder what the framers of the Constitution would have thought if they had known what we know now about computers and the Internet. Would they have permitted the Internet crimes against children that we are witnessing today?

I would like to talk about two things today, the threat from those predators who are using social networking sites, and the legal help we need regarding data retention by Internet service providers.

The luring of minors for sexual exploitation remains a continuing threat to our youth. Beyond the chat rooms that predators have always frequented, social networking sites are now wildly popular, and there are dozens of such free sites, including MySpace, Xanga, Friendster, Facebook, and others. Curious young people visit the sites every day, and post images and personal information about themselves. They can browse and search for others, according to age, sexual preference, zip code, and school name. They can communicate with one another, and then arrange to meet in person, and as you might imagine, the sites are also popular among sexual predators.

We received a phone call a few months ago from an Arizona woman who said that her young daughter, while using a social networking site, was contacted by a man from their neighborhood who she knew as a registered sex offender. We found the man's webpage, where he described himself as a kindly lover of poetry, plants, and flowers, who was seeking female friendship for dating. Fourteen other young people were listed on his profile as friends, with whom he had networked through the site. There was no mention, of course, in his profile that he is a high risk registered sex offender in Arizona. Now, since that time, the original webpage is no longer available at the site, but there is nothing stopping him from re-subscribing to the same site, or one of the many other sites, under another assumed name. The use of the sites by sexual predators remains a serious threat to our safety and the safety of our children.

Now, this problem will likely get worse before it gets better, as kids flock to the sites and more communities, schools, libraries, and businesses provide unrestricted Internet access through wireless access points that sometimes leave law enforcement investigations at a dead end. My written attachments contain some suggestions for improving the social networking site environment, but in the interest of time, I don't want to review them all now.

I would like to talk about an item of great importance to my investigative colleagues nationwide. Last week, I sent a survey to Internet crimes against children investigators at all of our nationwide affiliates throughout the United States. The survey asked one question: what law could be created or revised to assist investigators who work cases involving Internet crimes against children, and the most frequent response involved data storage by Internet service providers, and the retrieval of data from Internet service providers. What our people are telling us is that investigators need ISPs to retain subscriber and content information so that when legal process, in the form of a subpoena or search warrant, are served, there is data remaining with the ISP that the investigator can use to find the offender.

Now, most ISP organizations are operated by conscientious and professional business people who are equally horrified, as are we all, by Internet crimes against children. Some ISPs have graciously extended themselves to help investigators. Some reluctant ISPs will only assist to the extent that the law mandates them to assist.

Mandating that ISPs retain data is not a privacy violation. Law enforcement only needs the data preserved, but not disclosed to us, except in response to legal process.

Internet industry professionals may cite the financial burden of data storage, but consider the potential cost of not retaining data. For example, when law enforcement is seeking a predator identifiable only by the information associated with a screen name, but the responsible ISP did not preserve the information, the investigation ends, while the predator roams free.

Based on the requests of my colleagues, I respectfully ask for two improvements to the law: one, that Internet service providers be mandated to retain information about subscribers for at least 1 year, with penalties for noncompliance; and two, that Internet service providers be mandated to respond to subpoenas involving crimes against children investigations within 1 week of receiving a subpoena, and more quickly under exigent circumstances, where a child is missing.

I will conclude by saying that investigators need your help in order to navigate those dark alleys of the Internet, where they work diligently to help protect children. I recognize that turning the Internet control dial comes with a cost, but failing to turn the dial carries a greater human cost to our young people.

Thank you, sir.

[The prepared statement of Dr. Frank Kardasz follows:]

PREPARED STATEMENT OF DR. FRANK KARDASZ, SERGEANT, PHOENIX POLICE  
DEPARTMENT, PROJECT DIRECTOR, ARIZONA INTERNET CRIMES AGAINST CHILDREN TASK  
FORCE, UNITED STATES DEPARTMENT OF JUSTICE

Congressman Stupak and distinguished members of the sub-committee, thank you for permitting me to speak today. Arizona joined the Internet Crimes Against Children (ICAC) Task Force Program in 2000. We work cooperatively with our law enforcement colleagues from the FBI, ICE, Postal Inspection Service and the Secret Service. Although the names of our agencies differ, we all share the common goal of trying to keep children safe from Internet sexual predators and child pornographers.

The AZ ICAC Task Force has recorded over 2,000 investigations, with over 200 arrests. Although Arizona has the toughest laws in the nation against child pornography, this has not stopped the trafficking of unlawful images, and like all of our colleagues nationwide, we have many more solvable case files at the ready than we have personnel and resources to bring in the offenders. Sadly, while these cases await investigation, children and teens continue to suffer at the hands of sex offenders.

I have had the opportunity to speak with many citizen groups about Internet crime, and at the end of each presentation there is often some senior individual in the group who

raises a hand and asks: "Why don't they just switch that whole dang Internet thing off!"...as if we have a control panel somewhere with a dial that we can turn and it will regulate Internet misconduct.

Legislation is the closest thing we have to an Internet control dial. Although opponents of controls argue that regulations are costly, imperfect and violations of constitutional freedoms, I sometimes wonder what the framers of the Constitution would have thought if they had known what we now know about computers and the Internet. Would they have permitted the Internet crimes against children that we are witnessing today?

I would like to talk about two things today: the threat from those predators who use social networking sites, and the legal help we need regarding data retention by Internet service providers.

The luring of minors for sexual exploitation remains a continuing threat to our youth. Beyond the chat rooms that predators have always frequented, social networking sites are now wildly popular. There are dozens of such free sites, including MySpace, Xanga, Friendster, Facebook, and others. Curious young people visit the sites every day and post images and personal information about themselves. They can browse and search for others according to age, sexual preference, zip code or school name. They can communicate with one another and then arrange to meet in person. And as you might imagine, the sites are also popular among sexual predators.

We received a phone call a few months ago from an Arizona woman who said that her young daughter, while using a social networking site, was contacted by a man from their neighborhood who was known to her as a registered sex offender. We found the man's web page where he described himself as a kindly lover of poetry, plants and flowers who was seeking female friendship for dating. Fourteen other young people were listed on his profile as friends with whom he had networked through the site. There was no mention on his profile that he is a high-risk registered sex offender in Arizona. Since that time the man's original web page is no longer available at the site, but there is nothing stopping him from re-subscribing to the same site or one of the many other sites under another assumed name. The use of the sites by sexual predators remains a serious threat to the safety of our children.

The problem will likely get worse before it gets better as kids flock to the sites and more communities, schools, libraries and businesses provide unrestricted Internet access through wireless access points that sometimes leave law enforcement investigations at a dead end. My written attachments contain some suggestions for improving the social networking site environment, but in the interest of saving time I do not wish to review them all now.

I would like to talk about an item of importance to my investigative colleagues nationwide. Last week I sent a survey to Internet crimes against children (ICAC) investigators at all of our nationwide affiliates throughout the United States. The survey asked one question: What law could be created or revised to best assist the investigators who work cases involving Internet crimes against children? The most frequent response involved data storage by Internet service providers and the retrieval of data from Internet service providers. What our people are telling us is that investigators need ISP's to retain subscriber and content information so that when legal process in the form of a subpoena or search warrant are served, there is data remaining with the ISP that will help the investigator find the offender.

Most ISP organizations are operated by conscientious and professional business people who are horrified by Internet crimes against children. Some ISP's have graciously extended themselves to help investigators. Some reluctant ISP's will only assist to the extent that the law mandates them to assist.

Mandating that ISP's retain data is not a privacy violation. Law enforcement only needs the data preserved but not disclosed to us, except in response to legal process.



Internet industry professionals may cite the financial burden of data storage, but consider the potential human cost of not retaining data. For example, when law enforcement is seeking a predator identifiable only by the information associated with his screen name, but the responsible ISP did not preserve the information, the investigation ends while the predator roams free.

Based on the requests of my colleagues I respectfully ask for two improvements to the law:

1. That Internet service providers be mandated to retain information about subscribers for at least one year, with penalties for non-compliance.
2. That Internet service providers be mandated to respond to subpoenas involving crimes against children investigations within one week of receiving a subpoena, and more quickly under exigent circumstances where a child is missing.

I will conclude by saying that investigators need your help in order to navigate those dark alleys of the Internet where they work diligently to help protect children. I recognize that turning the Internet control dial comes with a cost, but failing to turn the dial carries a greater human cost to our young people.

Thank you again.

#### **Supplemental Materials to the Testimony of Dr. Kardasz**

##### **Internet Social Networking Sites**

Recent disturbing incidents involving Internet crimes against children have been prominent in the media. In some incidents, the crimes have involved suspects and victims who met each other via Internet social networking sites. Social networking sites are places on the Internet where people can meet one another, communicate and interact.

Social networking and communication are normal parts of the human experience. The Internet has become an important venue for people to network and interact. Young people are naturally curious about themselves, about others, and about the world. The sites permit them to reach out to others from around the globe, sometimes with tragic results.

There are many social networking sites. Some of them are listed below:

- Myspace.com
- Facebook.com
- Friendster.com
- Dittytalk.com
- Cozydating.com
- Interracialsingles.net
- Livejournal.com
- Friendsfusion.com
- Intellectconnect.com
- Prisonpenpals.com
- Zogo.com

##### **Why are the sites popular?**

Most of the social networking sites are free and supported by advertisers who hope users will buy products or services advertised on the sites. Young people who are curious and seeking relationships and new experiences visit the sites to find others.

**How do the sites work?**

Any computer with Internet access can be used to permit someone to join a site. Some sites require only that the registrant provide an email address and often there is no verification process to check the truthfulness of any of the information that a registrant provides. Most sites require that users abide by conditions and terms of use meant to thwart improper conduct, but enforcement is often lax. Once a registrant becomes a member, he or she can post personal information, images or other information depending upon the features available at the site. Unless a user chooses to enable privacy options, all the information posted may be visible to all other users of a site.

**What are the dangers?**

Those who misuse the sites may do so in many ways including:

- Luring / enticement – Internet sexual predators and know sex offenders have used social networking sites to locate and lure victims.
- Identity theft – Criminals steal the identities of those who post personal information.
- Cyberbullying / harassment – Agitators post derogatory, hurtful or threatening information about others.
- Stalking – Stalkers can use personal information posted to the sites to locate and pursue victims.
- Fraud schemes – Criminals who wish to defraud others of money or property can locate victims, gain their trust, and then take advantage of that trust for criminal purposes.
- Inappropriate sexual content – Some users post sexually explicit information that is inappropriate for young computer users.

**Prevention**

What can you do to protect yourself from those who misuse social networking sites?

Do's and Don'ts**Don't -**

- post personal images
- post your true full name
- post your home or cellular phone number
- post your true age or date of birth
- post your true home or business address
- post your school name or the grad that you are in
- post your calendar of upcoming events or information about your future whereabouts.

**Do**

- discuss Internet risks with your child
- enter into a safe-computing contract with your child
- enable computer Internet filtering features if they are available from your Internet service
- consider installing monitoring software or keystroke capture devices on your family computer that will help monitor your child's Internet activity
- know each of your child's passwords, screen names and all account information
- put the computer in a family area of the household and do not permit private usage

- report all inappropriate non-criminal behavior to the site through their reporting procedures
- report criminal behavior to the appropriate law enforcement agency including the NCMEC Cybertip line or the Internet Fraud Complaint Center
- contact your legislators and request stronger laws against Internet crime
- contact the corporations who place advertisements on the sites and let them know that their advertising is helping to support inappropriate Internet behavior. Also, let the corporations know that you intend to boycott or discontinue using their product or services because of the behavior they are supporting.
- visit the NCMEC Netsmartz Workshop at <http://www.netsmartz.org> for more information
- remember that every day is Halloween on the Internet. People on the Internet are not always as they first appear.

#### **Making Social Networking Sites Safer**

The following suggestions would make social networking sites safer for users and more law-enforcement friendly.

1. On every social networking site web page, display a clearly visible hyperlink permitting users to easily report misconduct.
2. For new users, make the default settings for viewing and sharing all account information 'private'. This means that new accounts would be automatically set to exclude others and to not share information. The new subscriber would have to actively choose to share account information by checking the appropriate boxes in the account settings section.
3. On every web page, display a link to the national sex offender registry.
4. Proprietors of social networking sites should install filtering software to eliminate users from posting obscene words.
5. Require that all new users enter verifiable credit card information when first subscribing.
6. Require that all subscribers pay a nominal monthly fee.
7. Include a provision in the social networking sites terms of use that notifies users that they have no expectation of privacy with regards to any of the content they post and that law enforcement may obtain any and all of their postings through the use of a subpoena only - without a search warrant.
8. Retain profile information for deleted accounts for 90 days.
9. Remove the browse and search functions that permit users to locate one another.
10. On every social networking site page, display a link to the Internet Crime Complaint Center for incidents of theft or fraud. Their link is [www.ic3.gov](http://www.ic3.gov)
11. Include an admonition on social networking sites profile pages advising users that revealing personal information could lead to identity theft or victimization by offenders who are intent upon harassment, stalking, fraud or identity theft.
12. Preserve changes to user's pages and the Internet protocol address associated with the changes for 90 days.

#### **Selected ICAC Case Studies – Arizona ICAC Task Force**

##### **Milwaukee Boy Found in Phoenix Home of Sex Offender**

From the Arizona Republic, Aug. 23, 2005, Reported by William Hermann

Phoenix police say the experience of the 13-year-old Milwaukee boy they found Monday night in the company of a man they suspect of using the Internet to lure the child to town is one that parents need to take to heart. Phoenix Police Sergeant Kardasz said

Milwaukee police on Aug. 17 had received a missing persons report from the boy's mother. Investigators went into her son's computer and found that he had been communicating regularly with a person using a Phoenix wireless Internet site. "We went to the address of the wireless user and pretty quickly found he was an innocent person whose wireless service was being used by someone else," Kardasz said. "Through investigative work my staff established who was using the wireless connection, we watched his house, and soon the man drove up with the boy in his car."

At about 11:30 p.m. police arrested Vernon Monk, 31. "The suspect had no ID and was using a false name and a fictitious license plate and pretending to be the boy's father to people in the neighborhood," Kardasz said. Monk was arrested for custodial interference and booked into a Maricopa County Jail. Police also learned that there is an outstanding arrest warrant on Monk from Seminole County, Okla., for a sexual offense against a minor. The boy was taken to the county's Juvenile Court Center to stay until his mother could arrange for his return home.

#### **Internet Sexual Predator / Traveler Arrested and Imprisoned**

Offender: David Jackson Donan, w/m, age 61

In September 2003, an investigation began involving an unidentified person using the Internet screen name "Brasshatter." Investigators learned that "Brasshatter" intended to travel via commercial aircraft from Austin, Texas to Phoenix, Arizona for the purpose of meeting a minor to engage in unlawful sexual intercourse. "Brasshatter" was later identified as David Jackson Donan, age 61, with residences in both California and Texas. On October 20, 2003 Donan boarded a commercial aircraft and traveled from Texas to Arizona. To groom and entice his intended victim, he brought several packages of the candy - Skittles. To aid in his intended unlawful sexual acts he brought nine sexual aide devices, KY Jelly, a male sexual enhancement drug, a prescription for Viagra, and a digital camera - all in his carry-on baggage. Donan was arrested without incident upon his arrival at Phoenix Sky Harbor Airport. He made no statements and was booked.

Arizona ICAC investigators and FBI agents in Arizona, California, and Texas worked cooperatively in the subsequent investigation and search of Donan's residences for evidence. They uncovered computer evidence, firearms and other sexual aid devices belonging to Donan. Later forensics examinations of his computer also revealed a collection of child pornography. Computer evidence indicated that Donan had bragged during Internet chat conversations about having victimized children while he had visited Thailand many years ago. Donan waived his right to trial plead guilty to one count of the Federal offense: Travel with intent to engage in a sexual act with a juvenile (Title 18, Part I, Chapter 117, 2423b). Donans' presentence report was not favorable with indications that he had prior "hands-on" offenses with as-yet unidentified victims.

On September 29, 2004, he plead guilty in U.S. Federal District Court (Phoenix). Honorable Earl H. Carroll presided. Judge Carroll sentenced Donan to 7 years, 3 months prison, followed by one year residence in a transitional facility, \$25,000 fine and lifetime supervised release.

#### **International Cooperation Leads to Child Pornography Trafficker**

Offender: Lee McCulloch, w/m, age 26, resident of Gwent, South Wales, U.K.

Occupation: Factory worker, Marital status: single

Arrest Location: Abertillery, Gwent - South Wales, United Kingdom

Charge: Distributing Indecent Photographs of Children (United Kingdom)

Sentence: Eight months prison, Sex offender registration for five years.

Agencies involved: Arizona ICAC Task Force, Phoenix P.D., Phoenix F.B.I., Heddlu Gwent P.D. South Wales, U.K.

In April 2003, an investigator from the Arizona Internet Crimes Against Children Task Force / Phoenix P.D. initiated an investigation into an unidentified child

pornography trafficker. the investigation led to an unknown suspect in the United Kingdom. Working with the FBI and the Heddlu Gwent (UK) Police Department, investigators assembled a case that led to the identification and arrest of 26 year old Lee McCulloch in South Wales, UK. McCulloch, a factory worker, used computers at his home in the United Kingdom to collect and traffic images of child pornography with other nefarious Internet associates.

McCulloch, who is unmarried, was arrested on November 28, 2003. Investigators in the UK developed further information leading to twenty (20) other suspects there with whom McCulloch traded unlawful images of child pornography. On August 26, 2004, McCulloch was sentenced to 8 months in prison in the UK and five years of sex offender registration status.

**David Mojica Santos -Internet Sexual Predator**

Arrest Date/Time: October 8, 2003, 1530 hours.

Offense: Luring a Minor for Sexual Exploitation

On October 8, 2003, David Mojica Santos, age 65, was arrested for luring a minor for sexual exploitation in northwest Phoenix. Santos first came to the attention of law enforcement in July 2003, when he used the Internet to solicit sexual conduct with a minor. Santos traveled from his residence in Mesa to a location in Northwest Phoenix where he intended to meet a minor for sex. He was arrested, booked, and subsequently released on bond. He later plead guilty to the court.

SENTENCING HEARING – STATEMENT OF SGT. KARDASZ

*(The recent trend among judges in Maricopa County is to sometimes sentence such offenders to probation only, with no jail time. Anticipating this, we prepared a detailed statement to the sentencing judge. Here is an excerpt):*

...Your Honor, the innocent children we struggle to protect are unable to appear here today. They are children whose innocence was stolen by Internet sexual predators like this defendant. Most of those children will never come forward due to fear or a misplaced sense of guilt. A few of them, like 13 year old Kasie Woody of Arkansas, and 13 year old Christina Long of Connecticut, were forever silenced by Internet sexual predators. According to reports from the National Center for Missing and Exploited Children, one in five girls and one in ten boys will be sexually victimized before they reach adulthood, and less than 35% of these crimes will ever be reported.

The Internet provides an unparalleled opportunity for criminals to unearth themselves and victimize unwary young people. Research indicates that of the estimated 24 million child Internet users, one in five received a unwanted sexual solicitation, but only one in four told a parent. Curious and innocent youngsters are flocking to the Internet seeking friendship and information but are instead finding sexual deviants and predators. My undercover investigators and I have witnessed no shortage of adults chatting on the Internet with the stated intention of sexually victimizing minors.

Over the past few years our caseload has skyrocketed while our resources have not. Our investigation of this defendant revealed that his Internet chat was not an isolated incident but part of a series of ongoing offenses occurring against multiple victims over an extended period of time. He was not the unfortunate victim of a "sting" caught at the wrong place at the wrong time. He is a practiced Internet sexual predator. Forensics analysis of his computer revealed that he did not spend his idle time enjoying normal retirement hobbies or mentoring his family or community. This former missionary spent his day prowling cyberspace in search of young sexual prey.

We discovered Internet chat conversations he had with four as yet unidentified girls aged fifteen, fourteen and eleven. In each of the chats he quickly turned the conversation to sex and began to manipulate each girl towards meeting him for sex. I am going to read

brief excerpts of the chat conversations the defendant had with various young girls he contacted on the Internet. Much of the language is so sexually graphic that I will not repeat it verbatim.

"Do you like older guys?"

"Have you had sex yet?"

"Are you curious about having sex?"

"Do you think you would like to have sex sometime soon?"

"I wish I was next door to you....and then maybe not. I might rape you." "What city do you live in....I was just wondering if there is a large airport nearby." "You just don't know how badly I want to (expletive deleted) you right now."

And I will stop there your Honor because the conversations deteriorate graphically from there. Your Honor, I have watched defendants in similar circumstances appear in these courtrooms arguing that everything they did was fantasy role-playing and that they were the unfortunate victims of zealous police operations. That's hogwash. Was it fantasy when this defendant drove over 20 miles from Mesa to Northeast Phoenix for the expressed purpose of meeting a minor for sex? Was it fantasy when the defendant brought condoms with him to the meeting? Condoms that he admitted that he does not use with his wife.

Apologists for this defendant may look at his age and surmise that he has little capacity for future offenses - I disagree. This defendant had the physical capacity to proudly display on the Internet, graphic sexual images of himself, captured with a computer web camera and in a variety of poses. In similar cases my colleagues and I have watched defendants receive minimal sentencing by other courts, only to re-offend later.

In one recent case the defendant mocked the court by continuing to solicit minors for sex while the defendant was out on bond only days after his original arrest. In another of our cases, the convicted defendant, while free on probation, immediately began producing, acting in, and trafficking child pornography, including images of himself sexually abusing three young children under shocking and horrifying circumstances.

The Arizona law as it stands permits the court to exercise wide discretion in sentencing this offense. We trust that this court will act in the best interest of our community and send a strong message to this and all other Internet sexual predators. Finally your honor, we request that this court's judgment provide a message of reassurance to the children unable to appear in your courtroom today that their rights are being defended at this, the highest level of County justice.

SENTENCE -

On June 18, 2004, Santos was sentenced before Judge Hotham of the Maricopa County Superior Court. He received ten months jail and lifetime probation.

Contact:

Dr. Frank Kardasz, Sergeant / Project Director

Phoenix P.D. / Arizona ICAC Task Force

620 W. Washington

Phoenix, AZ 85003

Desk: 602 256 3404

Email: frank.kardasz@phoenix.gov

<http://www.kardasz.org>

MR. WHITFIELD. Thank you very much. Our next witness is the Lead Special Agent of the Wyoming Division of Criminal Investigation,

and the Internet Crimes Against Children Task Force. Mr. Waters, you are recognized for 5 minutes.

MR. WATERS. Thank you, Mr. Chairman, Congressman Stupak, and the distinguished members of the subcommittee.

I welcome this opportunity to appear before you, and discuss how the Internet is being used to commit crimes against children, and how the Internet Crimes Against Children Task Force is responding to that threat.

First, I would like to speak to the issue of child pornography. Now, in Wyoming, I am one of four investigators that are handling this. We are the cops on the beat doing this. This isn't about a movie or a picture. This is ongoing sexual abuse of a child. This is not about pornography. These are not baby in the bathtub movies. These are not consenting adults. Let us be clear, these are images that are crime scenes depicting the sexual abuse of children, starting as young as infants. These are not innocent images. These are images depicting the complete destruction of innocence.

I would like to provide you with a little background information about the Internet Crimes Against Children Task Force. The ICAC includes 46 regional task forces, State and local police officers, sheriff's deputies, spending time at the computers, doing the chat, working the crime scenes. Through funding from the Office of the Department of Justice, Office of Juvenile Justice and Delinquency Prevention, we are able to bring these together with a common goal, and we are able to have contacts in each jurisdiction, as these investigations cross boundaries.

We have a strong relationship with our Federal colleagues, and we collectively strive to bring to bear the strengths of each entity, in our mutual goal to protect children. In fact, in Wyoming, the ICAC that I represent, we have been active for 5 years. We work very closely under the authority of the Attorney General, and we present frequently to the United States Attorney for prosecution.

I heard a citation earlier that 25 percent of these cases are being prosecuted federally, 75 percent of these cases were taken to our State prosecutors, our DAs, and we are getting some support. We are getting outstanding support, in fact. We work very closely with them to try and assure that we bring the best tools to bear. We are facing quite a few new challenges.

The ICAC Task Force Program designed a methodology to investigate peer-to-peer file sharing environment. We were seeing a lot of these images showing up during our forensic examinations of computers, originating from peer-to-peer. Five years ago, we were working a lot of paid websites. Now, coming from the peer-to-peer, I started to write software to try and find out how bad this problem was, and we were amazed. In under 24 months, our investigators, there are

about 400 around the world using this software, have identified over 4.4 million transactions involving the trafficking of movies and images depicting the sexual abuse of very young children. I focused on images 8 years old and younger when I designed the system. By country, Germany, 262,000 transactions; Canada, 294,000; the United Kingdom, 305,000; and the United States, 1.9 million transactions in under 24 months. Over a million IP addresses.

These file sharing networks have created an efficiency level unprecedented in previous distribution technologies. In Wyoming, the smallest state by population, we have over 250 search warrants that we could request if manpower permitted. Our investigators are averaging over 70 hours a week very frequently working on these investigations. We are hitting as hard and as fast as we can.

In addition to the ICAC investigative efforts in the peer-to-peer environment, we are proactively working to put ourselves between child predators and the children in our care. We sit in the chat rooms. We pose as little boys, little girls, maybe adults. These are my two youngest. In 2001, my wife sent this to me to work, to put on the wall. I was having a little bit of trouble dealing with some of the bad guys we were facing, and I kept this on the wall. This was our Christmas card, 2001. Next please. On December 31, while I was online posing as a 13-year-old girl, I was contacted by a man who requested to meet me at a nearby mall for sexual acts. He was very descript. I received this picture of him. Look at his eyes. Go back. It is the same man. A week after Christmas, we walked the mall, and watched this individual for two and a half hours, waiting for him, so that we could arrest him in a safe manner, and eventually, we placed him into custody. This is one of two times where my undercover operations have revealed an offender who had exposed contact to my own children.

The investigators in Wyoming are in these rooms, were speaking to these individuals, and were pursuing arrests. Through our undercover chat operations and file trading investigations, the ICAC investigators are executing arrests and search warrants throughout the Nation. These investigations often lead us to homes where children are being physically and sexually abused, often starting at an early age. The most recent one in Wyoming, the abuse was an act of abuse of a four year old, and we had no other leads. The individual had no criminal history, no priors, no other indication until his trafficking of images on the peer-to-peer networks took us into his home, and fortunately, in that case, we were able to rescue the child.

I would like to speak again briefly about the images that we are running into, and this speaks to what Dr. Kardasz spoke. During undercover operations, an ICAC investigator in Florida received a movie



depicting the rape of a 2-year-old child. In accordance with our policy, the movie was sent to the National Center for Missing and Exploited Children. The abuse was so horrific it even shocked the seasoned analysts at the Center. The ICAC investigator received this movie in August of 2005. Drawing on our efforts on the peer-to-peer environment, we were able to look back and trace this movie to a computer in Colorado, where it had been made available for distribution in April of 2005, several months prior to any other known existence on the Internet.

Just as the ICAC investigators thought they were getting close to the potential origin of this movie, all hope was destroyed. The Internet service provider responded to us that they did not maintain records related to this account. Efforts to find this child fell short, and there was nothing that we could do about it. The safety of our children cries out for each of us to take all steps necessary to eliminate this problem. Technology has allowed us to more accurately gauge the scope of the societal problem of child sexual abuse. The Internet is serving as the great connector for people who seek to harm children and take pleasure in watching children being sexually abused. Better cooperation from the Internet service providers would result in us being able to take more children out of the hands of the predators.

MR. WHITFIELD. Conclude, Mr. Waters. Your statement has been fascinating.

MR. WATERS. Mr. Chairman, I thank you for the opportunity to speak, and I will be happy to answer any questions now, or in the future, later.

[The prepared statement of Flint Waters follows:]

PREPARED STATEMENT OF FLINT WATERS, LEAD SPECIAL AGENT, WYOMING DIVISION OF  
CRIMINAL INVESTIGATION, INTERNET CRIMES AGAINST CHILDREN TASK FORCE  
TECHNOLOGY CENTER, UNITED STATES DEPARTMENT OF JUSTICE

Congressman Stupak and distinguished members of the sub-committee, I welcome this opportunity to appear before you to discuss how the Internet is used to commit crimes against children and how the Internet Crimes Against Children Task Force is responding to that threat. Congressman Stupak, you are clearly an advocate for child protection and I commend you and your colleagues for your leadership and initiative.

The Internet Crimes Against Children Task Force (ICAC) shares your concern for the safety of our children and we thank you for bringing attention to this issue.

Child Pornography

This isn't about a movie or picture. This is about the ongoing sexual abuse of a child. This isn't about pornography. These are not images of consenting adults. These are not "baby in the bathtub" movies. Let's be clear, these images are crime scene photos depicting the sexual abuse of children starting as young as infants. These are not innocent images. These are images depicting the complete destruction of innocence.

Who are these children?

The majority of the children depicted in these pictures are sexually abused by someone they should be able to trust, such as a parent or another adult who has legitimate access to the child. And, contrary to popular belief, the majority of children identified in child pornography have been identified by the National Center for Missing and Exploited Children (NCMEC) as American children.

Internet Crimes Against Children Task Force

I would like to provide you with some background information about the Internet Crimes Against Children Task Force. ICAC includes forty-six (46) regional Task Forces working in partnership with the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention. These Task Forces are composed of state and local law enforcement agencies throughout the United States focused on investigation, education and prevention related to the exploitation of children by means of the Internet. The National Task Force has a strong relationship with our federal colleagues and we collectively strive to bring to bear the strengths of each entity in our mutual goal to protect children.

The Wyoming ICAC, which I represent, has been an active participant in the national Task Force program for five years. Our Task Force consists of three state agents operating under the authority of the Attorney General. In Wyoming, we have a close working relationship with the United States Attorney and our Federal partners.

We Are Facing New Challenges

In the last three years we have witnessed a monumental change in the trafficking of material related to the sexual abuse of children.

Three years ago our national efforts identified over 2600 transactions where people were trading images of child sexual abuse via peer-to-peer networks. At that time, the operation was one of the largest proactive Internet investigations ever. We thought we had made a significant impact in the networks used to trade this material. We were mistaken.

Advances in Peer-to-peer file trading has generated a completely new barter system, encouraging people to move from using sexual abuse images to validate their own interests in harming children to spreading the material to as many other people as possible.

The ICAC Task Force program has designed a methodology to investigate the Peer-to-Peer (P2P) file-sharing environment.

In under 24 months, our efforts have identified over 4.4 million transactions involving the trafficking of movies and images depicting the sexual abuse of very young children.

By Country

- |                  |           |
|------------------|-----------|
| • Germany        | 262,000   |
| • Canada         | 294,000   |
| • United Kingdom | 305,000   |
| • United States  | 1,900,000 |

These file-sharing networks have created an efficiency level unprecedented in previous distribution technologies. Utilizing high speed Internet access, millions of computers are linked together allowing fast and easy distribution of child pornography. It should not be surprising to us that child predators in the United States have found a way to leverage the technology to their benefit.

In Wyoming, our small team has over 250 search warrants we could request if manpower were not an issue. Often our investigators average 70 hours a week working these investigations.

In addition to the ICAC investigative efforts in the peer-to-peer environment, we are proactively working to put ourselves between child predators and the children in our care. Highly-trained ICAC investigators across the country are patrolling areas of the Internet where predators are known to lurk and children are vulnerable. Each week, ICAC investigators identify and apprehend criminals who solicit sexual acts with undercover officers posing as children.

Through undercover chat operations and file trading investigations ICAC investigators are executing arrest and search warrants throughout the Nation. These investigations often lead ICAC investigators to homes where children are being physically and sexually abused. These efforts allow ICAC investigators to disrupt the pattern of abuse at an early stage, sometimes before the child is even old enough to reach out for help.

Sadly, this is not always the case. During undercover operations an ICAC investigator in Florida was sent a movie depicting the rape of a two-year-old child. In accordance with ICAC policy the movie was sent to the National Center for Missing and Exploited children. The abuse was so horrific it even shocked the seasoned analysts at the center. The ICAC investigator received the movie in August 2005. Drawing on the previous coordinated efforts of the ICAC investigators we were able to trace the movie to a computer in Colorado where it had been made available for distribution as early as April 2005. This was several months prior to any other known existence on the Internet. Just as ICAC investigators thought they were getting close to the potential origin of the movie all hope was destroyed. The Internet service provider used to trade this movie did not maintain any records related to the use of the account. Efforts to find this child fell short and there was nothing law enforcement could do about it.

The safety of our children cries out for each of us to take all steps necessary to eliminate this problem. Technology has allowed us to more accurately gauge the scope of the societal problem of child sexual abuse. The Internet is serving as the "great connector" for people who seek to harm children and take pleasure in watching children be sexually abused. Better cooperation from ISP's would result in us being able to save more children from the hands of those who want to harm them.

The ICAC experience shows us that technology can allow us to proactively protect our children and identify predators. The ICAC Task Force Program is critical to the overall efforts to protect children and we'll continue to place ourselves between our nation's children and Internet predators. We thank you for your continued support of the ICAC Task Force Program and appreciate your interest in this important issue.

I will be happy to answer any questions related to this issue now or in the future.

MR. WHITFIELD. Thank you very much. Mr. Clark. Mr. Clark is the Deputy Assistant Secretary for U.S. Immigration and Customs, and you are recognized for 5 minutes.

MR. CLARK. Thank you, Chairman Whitfield, Ranking Member Stupak, and distinguished members of the subcommittee.

I had spent quite some time over the last few days writing up an oral statement off my written statement to sort of summarize some of the work and accomplishments ICE has done in the field of child predators Internet investigations. I wanted to talk about why U.S. Customs originally, and ICE now are involved in these investigations, starting

with our traditional and long history working hand in hand with the U.S. Postal Service, when much of the foreign material came into the United States through the mail, how in the '90s we began working these cases through the Internet. I know I was an ASAC out in San Francisco when we did one of the first significant international child predator investigations, and back then, it involved a chat room in which individuals were sharing pictures, videos, and there was, at that time, on demand molestation among the members of the groups.

Just in March of this year in Chicago, Attorney General Gonzalez and Assistant Secretary Myers from ICE conducted a press conference heralding the case we had taken down in Chicago. The technology had improved, but the situation is the same. It was on demand molestations of children by an international group, actually started with the Edmonton Police Service. Toronto Police Service had done some undercover work on it, turned it over to ICE to continue in an undercover capacity, and when all was said and done, we arrested individuals in the United States, Canada, Australia, and Great Britain. Same types of work, just more significant or sophisticated technology.

I wanted to talk about how ICE is using its unique border authorities to actually attack this problem from a transnational, trans-border perspective. There are many good law enforcement agencies here in the United States working it domestically, the ICACs, who we work with very often, my colleagues on the board here, State, Federal, local, across the board, working it domestically, so in an effort to more efficiently use our limited expertise, resources, we focus on the transnational, trans-border violations, in which there are persons or materials in a foreign country coming across to those in the United States.

I also wanted to recognize the excellent work by the non-governmental organizations. From the international perspective, World Vision, whom we work with often. Here, in the United States, the excellent work done by the National Center for Missing and Exploited Children, NCMEC, on which I am a board member, and who we have investigators assigned to their office to help coordinate a lot of the domestic investigations between the ICACs, state and local agencies, and the Federal agencies.

I wanted to highlight that this is a global problem. It is not a U.S. problem. One of the things we are finding in ICE, in working with our foreign colleagues, is how widespread this is, and on a good note, how the attention and the interest of our foreign law enforcement colleagues is on the rise. We are developing better and better relationships with our 56 overseas offices in developing these investigations, and one in particular, Operation Falcon, that we took down a few years ago, but continues to follow up on a number of leads. While in the United States,

we arrested 236 individuals, outside of the United States, over a thousand individuals were arrested based on leads from Operation Falcon, and I believe the government of Australia had its attention raised such that it is beginning to look at changes in its child protection laws as a result of that case.

There were a number of other things about ICE I wanted to talk about, but I changed my oral testimony, because I think it needs to address very briefly the incident that just happened a couple of days ago, in which the Public Affairs Officer of the Department of Homeland Security was arrested, Brian Doyle. That case just happened. I can't comment on the specifics of the incident, but I think it has bearing on this hearing today, and why we are here. The title of today's hearing is "What Parents, Kids, and Congress Need to Know About Child Predators," and I think the allegations in that case are significant.

I think what we need to know is that there is no profile, no profession, no size and shape, age, color, of an individual, no scarlet letter that they wear in public surroundings that indicate who child predators are. It is very unfortunate, teachers, clergymen, law enforcement. It doesn't seem to matter. There is no profession that we could say if they are doing X, you can be assured that they are child predators, or if they are doing Y, you can be assured they won't be child predators. It is an unfortunate situation. We have thousands of law enforcement officers here in the United States dedicated to these types of investigations, and thousands more internationally doing the same.

I think it is important for the public to realize, though, that there will never be enough law enforcement officers to attack this successfully unless families, parents, communities, and the public at large weigh in, and start paying attention to our kids. We can only do so much in law enforcement to attack it from a criminal perspective, but the public and the families and the parents need to listen to their kids. They don't have to tether their kids to their belts. They don't have to follow them in minicams. They don't have to lock them away in houses. They shouldn't get paranoid, but they should listen to their children. They should pay attention to what they are doing. They should pay attention to where they are going, whether it is around the block, in the mall, or on the Internet. That is very, very significant, and that is a message that has to be out to the public. We can do a lot. We are doing more, but we can't be everywhere, in terms of law enforcement, and the public, the families, the communities have to pay attention to this very, very significant problem.

I will pass along on my time. I appreciate the opportunity to be here, and would be pleased to answer any questions.

[The prepared statement of John P. Clark follows:]

PREPARED STATEMENT OF JOHN P. CLARK, DEPUTY ASSISTANT SECRETARY, UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

### **INTRODUCTION**

Chairman Whitfield, Ranking Member Stupak and distinguished Members of the Energy and Commerce Oversight and Investigations Subcommittee, my name is John Clark and I am the Deputy Assistant Secretary of U.S. Immigration and Customs Enforcement (ICE). I appreciate the opportunity to share with you today how ICE is applying its expertise and authorities to protect our children from Internet sexual exploitation.

I am joined here today by my colleague James Plitt, the head of the ICE Cyber Crimes Center. Jim's unit leads our agency's efforts to combat the sexual exploitation of children on the Internet.

### **THE ICE MISSION**

Among the Department of Homeland Security law enforcement agencies, ICE has the most expansive investigative authorities and the largest number of investigators. ICE is the nation's principal investigative agency for violations related to our borders. Our mission is to protect the American people by combating terrorists and other criminals who seek to cross our borders and threaten us here at home. The men and women of ICE accomplish this by investigating and enforcing the nation's immigration and customs laws. Working overseas, along the nation's borders and throughout the nation's interior, ICE agents and officers are demonstrating that our unified immigration and customs authorities are a powerful tool for identifying, disrupting and dismantling criminal organizations that violate our Nation's borders.

Our agents and officers make it harder for potential terrorists and transnational criminal groups to move themselves, their supporters or their weapons across the Nation's borders through traditional human, drug, contraband or financial smuggling networks, routes and methods. Since its creation in March 2003, ICE has employed our authorities and capabilities against threats to our border, homeland and national security within our broad jurisdiction, including the cross border Internet sexual exploitation of our children.

### **PROTECTING CHILDREN**

By virtue of our robust authorities and capabilities for investigating crimes with a border nexus, ICE makes major contributions in the fight against the sexual exploitation of children worldwide, including over the Internet and the importation of physical or electronic representations of child pornography. We focus these ICE efforts under Operation PREDATOR.

Launched by ICE on July 9, 2003, Operation PREDATOR is currently managed and administered by the Cyber Crimes Center, a headquarters unit of ICE's Office of Investigations, which coordinates enforcement efforts against child sex offenders both nationally and internationally. To date, ICE has successfully arrested more than 7,500 child predators. Of these, more than 6,600 (88%) of the arrestees have been non-U.S. citizens, and of those, more than 3,900 (59%) have been deported from the United States.

ICE's Operation PREDATOR endeavors to apprehend and ultimately prosecute a variety of violators including individuals who:

- Engage in the receipt, transfer, distribution, trafficking, sale, facilitation, and production of child pornography in foreign commerce, including use of the Internet;
- Travel internationally for child sex tourism or who facilitate such travel;

- Engage in the human smuggling and trafficking of minors into the United States for illicit sexual purposes (sexual exploitation and/or prostitution) or worksite exploitation, and/or commit any crimes resulting in the harm, injury or death of a minor – *not* including the smuggling of children by parents for family unity reasons;
- Are foreign nationals/aliens who have been convicted of local, state, or federal offenses against minors and are now eligible for removal from the United States; and
- Are criminal aliens who have been previously deported from the United States for such offenses but have re-entered the country illegally.

These five enforcement objectives/goals are integral components of ICE's border security responsibilities and mission, since these criminal activities involving child exploitation often transcend this country's physical borders. The global Internet constitutes a powerful tool for those who prey upon children or profit from that predation. Far more child pornography is now being transmitted globally in an instant in electronic format than ever was distributed in physical form by couriers or packages arriving at international ports of entry or mail facilities.

Operation PREDATOR is a critical element of ICE's strategy for identifying and defeating threats to public safety that arise from our borders. These threats often include foreign nationals who enter or remain in this country illegally and become administrative fugitives or absconders and who may also be child sex offenders. Other threats include criminal business enterprises with business models based upon the smuggling of alien children into this country for sex exploitation or prostitution. Additional threats include U.S. citizens and/or lawful permanent resident aliens who travel to other countries with the intent to engage in "sex tourism" with children. In multiple cases we have seen these individuals actually return to the United States with trophy pictures and videos of their illicit exploits.

To illustrate for the subcommittee our work, I would like to share with you some powerful examples from ICE case files.

#### **OPERATION FALCON**

ICE initiated Operation FALCON in response to the threat to public safety posed by REGPAY, a criminal businesses activity based in Minsk, Belarus which provided third-party billing and credit card aggregating services to Internet child pornography websites. A task force comprised of agents from ICE, IRS, FBI, Postal Inspection Service, and the U.S. Attorney's Office in Newark, New Jersey, launched investigations into individuals and corporations involved in the production and distribution of child pornography via the Internet. Conducted under the auspices of Operation PREDATOR, this revolutionary investigation employed the latest technology to not only target the purchases, but also identify, track, and apprehend the producers and webmasters leading to the seizure of proceeds from this multi-million dollar criminal enterprise. Operation FALCON has yielded approximately 300 arrests in the United States and more than 1,000 arrests overseas. Operation FALCON is a continuing investigation.

Another ICE investigation that illustrates the enormity of the threat to public safety that can be posed by a single individual involved in Internet child pornography is that of a Louisville resident. This individual was indicted by a federal grand jury in the Western District of Kentucky on February 22, 2006, for receiving and possessing child pornography on his computer. Previously, this individual was indicted by a federal grand jury in the Eastern District of Virginia in December 2001, for similar charges involving possession and transportation of child pornography. This prior indictment was based on an investigation conducted by the Naval Criminal Investigative Service (NCIS), and led to the issuance of an arrest warrant for the individual. He had remained a fugitive until

January 31, 2006, when agents from our Resident Agent in Charge Office in Louisville, assisted by NCIS agents and U.S. Marshals, arrested him at his residence. At the time of his arrest, our agents executed a federal search warrant resulting in the seizure of 14 desktop computers, 4 laptop computers, numerous removable hard drives, and computer storage media. Subsequent forensic analysis of the seized items revealed numerous images of child pornography. This violator admitted that his collection of Internet child pornography, which he stored on his computers, approached more than 200,000 still images and hundreds of video files. He also stated that he was “addicted” to child pornography and had a sexual interest in children.

#### **COOPERATIVE EFFORTS**

Because the Internet allows for the instantaneous transmission of massive amounts of child pornography, including live video of real-time molestations, cooperation with our international partners is vital.

ICE has received excellent cooperation from the Danish and Norwegian National Police agencies. Together, we identify and target suspects who receive and transmit child pornography via the Internet using “peer-to-peer” software applications that operate on worldwide file-sharing networks. Examples include the use of the “LimeWire” program on the GNEUTELLA network and the “KaZaA” program on the FASTTRACK network. ICE has a similar ongoing enforcement initiative with the German National Police, which also attempts to identify and target suspects who distribute child pornography on the Internet. Additionally, ICE works closely with INTERPOL and EUROPOL to identify, arrest, and prosecute international violators with a nexus to the United States, in an effort to combat the international distribution of child pornography and the use of the Internet to facilitate child sex tourism.

ICE has partnered with the National Center for Missing and Exploited Children (NCMEC) to investigate tips received from the NCMEC Cybertipline. The Cybertipline receives leads from persons reporting the sexual exploitation of children. I am a member of the board of this unique organization, which has terrific outreach program for parents and their children on its “Netsmartz” Internet website. There, families can review numerous safety tips to help protect children from online child predators.

In addition, ICE works closely with the DOJ-funded Internet Crimes Against Children (ICAC) Task Forces around the country on major child exploitation initiatives involving illicit computer-related child pornography.

One of the major “high tech” tools we are using to assist us with the investigation of child pornography crimes via the Internet is known as the National Child Victim Identification System (NCVIS), which is a cooperative effort among federal, state, local, and foreign law enforcement agencies and civilian entities. The program is managed and administered by our Cyber Crimes Center in Fairfax, Virginia. The primary focus of NCVIS is to help all law enforcement agencies identify victims of child sexual exploitation and to track the transmission and circulation of digital images via Internet websites, Email, Instant Messenger, Newsgroups, and Chat Rooms. NCVIS is a secure computer-based initiative that was conceived as an investigative tool to assist in child exploitation investigations and allows us to analyze specific child pornography images, which have been seized as evidence or otherwise, to determine whether they match already identified child victims or actual child victims depicted in known child pornography magazines. To date, the ICE Cyber Crimes Center has analyzed more than 150,000 images utilizing NCVIS, resulting in the authentication of more than 2,065 images used to facilitate the criminal prosecutions and/or sentencing of child predators. In addition, since its creation, we have enrolled more than 110,000 images of child pornography into NCVIS of which more than 32,000 are of known child victims.

It is also important to note that our Cyber Crimes Center provides extensive technical training in the areas of online investigations and computer forensic analysis to



local, state, and other federal law enforcement agencies, as well as foreign police agencies. Due to the potentially harmful effects of viewing child pornography and, often times, dealing with its young victims, ICE has launched a proactive assessment program in an effort to prevent adverse emotional and psychological effects that may impact an ICE agent's emotional health.

#### **INTERNET PORNOGRAPHY TRENDS**

No matter how successful our efforts are against these terrible crimes and those who commit them, the continuing advance of technology gives potential offenders new opportunities to prey upon children. In fact, these offenders often are at the forefront of technological efforts to trade, share and transmit illicit images in the hope of evading law enforcement detection and capture.

Chief among these avenues are the lesser known peer-to-peer software applications and programs that operate on worldwide file-sharing networks that can be employed to support the transmission of child pornography images and videos. In fact, investigative efforts by ICE and Canadian authorities recently identified a peer-to-peer network that was developed and operated by an organized group of child predators to transmit alleged live video feed of children alleged to be as young as 18 months being sexually molested by members of the group. Other examples of technologies that have been misused by child predators include instant messaging and Internet Relay Chat programs, which facilitate real-time conversations and the exchange of child pornography. Predators can also use these programs to make real-time contact with unwitting child victims. In response to these threats to public safety, ICE has launched several undercover operations designed to identify and apprehend predators before they are able to make contact with our children.

#### **CONCLUSION**

As the Department of Homeland Security's largest investigative agency with unique authorities to protect the American people from threats that arise from our borders, ICE is uniquely equipped to enforce our nation's laws against the threats posed by child predators who employ the Internet as a tool to advance their crimes.

While ICE is a new agency, with newly unified immigration and customs authorities, we continue to aggressively apply our investigative authorities and capabilities to identify and close vulnerabilities in our border and homeland security. At the same time, we are bringing to bear the best of our former agencies' expertise, cultures, and techniques, while building a new federal law enforcement agency that is more effective and efficient than the sum of its parts. In case after case, ICE Special Agents are putting into practice the powerful advantages that flow from our unified authorities, and are putting them to great use on behalf of the American people. The net result is a greater contribution to the Nation's border security, which is a critical element of national security and public safety.

My colleagues at ICE are grateful for the chance to serve the American people and, on their behalf, I thank this subcommittee, its' distinguished members and Congress for the continued support of ICE investigative endeavors.

MR. WHITFIELD. Thank you, Mr. Clark. Mr. William Kezer is the Deputy Chief Inspector, U.S. Postal Inspection Service, and we recognize you for 5 minutes.

MR. KEZER. Good morning. Excuse me. Good morning, Mr. Chairman, distinguished members of the subcommittee. On behalf of the United States Postal Inspection Service, I want to thank you for holding

this hearing, and giving me the opportunity to discuss the subject of child sexual exploitation, and the important role postal inspectors play in combating it.

As one of America's oldest Federal law enforcement agencies, the Postal Inspection Service, founded by Benjamin Franklin, has a long, proud, and successful history of arresting criminals who attacked the Nation's postal system. Approximately 1,900 postal inspectors are stationed throughout the United States, and enforce more than 200 Federal laws regarding crimes that involve the U.S. mail and the postal system.

The Postal Inspection Service has a longstanding reputation as a true leader in the battle against child exploitation. Postal inspectors began investigating child pornography offenses in 1977, long before any other Federal agency addressed this problem. Thousands of offenders have been arrested and convicted under the new Federal laws. In fact, more than 4,800 child molesters and pornographers have been arrested by postal inspectors since the enactment of the Federal Child Protection Act of 1984. In 1997, the Postal Inspection Service began tracking the number of child molesters identified and children rescued in our investigations.

Since 1997, of the more than 2,400 arrests made by postal inspectors, over 800 were child molesters. That is one out of three. Additionally, more than 1,000 children were rescued from further sexual abuse and exploitation. And I might add that 75 percent of our cases are prosecuted at the Federal level.

In carrying out its objective to combat child exploitation, the Postal Inspection Service is fortunate to work closely with the U.S. Department of Justice, the Federal Bureau of Investigation, the Bureau of Immigration and Customs Enforcement, Interpol, the National Center for Missing and Exploited Children, where we have a postal inspector assigned, and the Federally-funded Internet Crimes Against Children Task Forces. postal inspectors play a significant role, not just through the investigations they perform, but in their efforts to raise public awareness about child sexual exploitation.

In May of 2001, the Postal Inspection Service launched a national crime prevention initiative with the National Center for Missing and Exploited Children. The goal of this initiative was to raise public awareness of the online victimization of children. As part of this initiative, a Postal Inspection Service employee designed an eye-catching poster with a powerful message urging all citizens to report suspected child exploitation to the National Center for Missing and Exploited Children's Cyber TipLine. This poster was displayed in 40,000 post

offices nationwide, and was viewed by as many as eight million postal customers on any given day. This poster is displayed here today.

Postal inspectors make presentations and conduct training on child pornography and child exploitation at local, national, and international conferences. Inspectors also make presentations to civic organizations and school associations on topics related to Internet safety. For a small Federal law enforcement agency, the Postal Inspection Service delivers a powerful punch when it comes to investigating those who produce, traffic, and possess child pornography, or otherwise sexually exploit children.

For the past 7 years, postal inspectors were recipients of the National Missing and Exploited Children's Award. The awards ceremony and Congressional breakfast was held right here on Capitol Hill. In 4 of the past 7 years, postal inspectors were awarded top honors by being named Officers of the Year. Mr. Chairman, as you can see, the Postal Inspection Service has been a law enforcement leader in the investigation of child sexual exploitation. The American public can count on our continued commitment to protect our most precious asset, our children. Again, thank you for bringing this important issue forward.

[The prepared statement of William E. Kezer follows:]

PREPARED STATEMENT OF WILLIAM E. KEZER, DEPUTY CHIEF INSPECTOR, UNITED STATES  
POSTAL INSPECTION SERVICE

Good morning, Mr. Chairman, members of the subcommittee. On behalf of the United States Postal Inspection Service, thank you for holding this hearing and giving me the opportunity to discuss the subject of child pornography on the Internet and the significant role Postal Inspectors play in combating it.

I'm William Kezer, Deputy Chief Inspector, for the U.S. Postal Inspection Service. The sexual exploitation of children spans all social and economic classes, and the perpetrators have no regard for the enduring grief and trauma they bring to their victims. The dangers of child pornography and other forms of child sexual exploitation should never be minimized. Through public awareness, vigorous investigations, certain prosecution, and just sentencing, the incidence of this horrible crime can be reduced. Lawmakers and law enforcers, as well as all members of society, have an obligation to help protect children and their families.

**The United States Postal Inspection Service (USPIS)**

As one of America's oldest federal law enforcement agencies, the U.S. Postal Inspection Service founded by Benjamin Franklin, has a long, proud, and successful history of fighting criminals who attack the nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public. As the primary law enforcement arm of the U.S. Postal Service, the USPIS is a specialized, professional organization performing investigative and security functions essential to a stable and sound postal system. As fact-finding and investigative agents, Postal Inspectors are federal law enforcement officers who carry firearms, make arrests, execute federal search warrants, and serve subpoenas. Postal Inspectors work closely with U.S. attorneys, other federal law enforcement agencies, state law enforcement agencies, and local prosecutors

to investigate cases and prepare them for court. Approximately 1900 Postal Inspectors are stationed throughout the United States and enforce more than 200 federal laws regarding crimes that involve the U.S. Mail and postal system.

#### **Early Enforcement Efforts: Obscenity Investigations**

For more than a century, the USPIS has had specific responsibility for investigating the mailing of obscene matter. In the 1860s and 1870s, Special Agents (as Postal Inspectors were called then) had to contend with obscene material exported to the United States by European producers. Special Agent Anthony Comstock, or “Mad Anthony,” as he was known, waged a relentless battle against anyone who used the U.S. Mail in an attempt to corrupt the morals of young people. In 1873 Congress passed the Comstock Act, a forerunner to the existing postal obscenity statute (18 USC Section 1461). In a letter dated June 11, 1875, now in the USPIS archives, Comstock wrote to his superior reporting on an investigation:

*I have the honor to report that yesterday in the city of New York I caused the arrest of one Zephir M. Caille, of 261 West 27<sup>th</sup> St., and doing business opposite 602 Broadway. He is charged with selling obscene pictures, and today waived examination at Tombs Police Court and was committed in default of \$1,000—for trial in Special Sessions court. I seized about 175 pictures in his possession. I have found I had a good case in State court and therefore I took him there instead of waiting to work up a case in United States Court. He is a Frenchman, and I am informed owned a set of 37 different negatives for printing obscene photographs and supplied the trade throughout the country, although ostensibly keeping a stand on Broadway.*

*I have the honor to be  
Very Respectfully Sir:  
Your Obedient Servant*

*Anthony Comstock*

*P.S. this fellow had a clasp knife sharpened as a dirk, but he did not get a chance to use it as I ironed him.*

#### **Protecting Children From Sexual Exploitation: A National Priority**

Through the years, child pornography has been investigated along with obscenity matters; however, it was not until the late 1970s that Congress took action to create federal legislation protecting children from sexual exploitation.

Prior to the late 1970s, most Americans were unaware of the proliferation and commercial distribution of magazines, films, and photographs depicting children in explicit sexual acts. Fortunately, we have begun to come to grips with the horrors of child pornography and to view it as it truly is, a manifestation of aberrant behavior resulting in the sexual abuse and victimization of children.

In 1977 the Protection of Children Against Sexual Exploitation Act became law (18 USC Section 2251-2253). This was the first federal law specifically designed to protect children from commercialized sexual exploitation. It was the culmination of years of effort by Congress, the U.S. Department of Justice (DOJ), concerned members of the public, and the law enforcement community to take action against the pernicious effects of pornography and the sexual exploitation of children. Under this law, a child, or minor, was defined as a person younger than age 16. In the landmark 1982 U.S. Supreme Court case, New York v. Ferber (1982), the Court found that child pornography is “intrinsicly related to the sexual abuse of children. First, the materials produced are a permanent record of circulation. Second, the distribution network for child pornography must be closed if the production of material which requires the sexual exploitation of children is

to be effectively controlled.” The Court ruled that the standards used to determine obscenity in adult pornography case are not applicable to child pornography, and child pornography is not protected under the First Amendment.

On May 21, 1984, seven years after the first federal child pornography statutes were enacted, President Ronald Reagan signed into law the Child Protection Act of 1984. This act amended the original act and created some new statutes, making the federal laws against child pornography even more substantial.

Postal Inspectors began investigating child pornography offenses in 1977, long before any other federal agency addressed the problem. Recognizing that child molesters and pornographers often seek to communicate with one another through what they perceive as the security and anonymity provided by the U.S. Mail, Postal Inspectors quickly established themselves as leaders in the battle against child pornography using “undercover operations” to flush out child pornography dealers who used the mail. Since that time, thousands of offenders have been arrested and convicted under the new federal laws. More than 4,800 child molesters and child pornographers have been arrested by Postal Inspectors since the enactment of the Federal Child Protection Act of 1984.

#### **Advent of the Internet**

Since the advent of publicly available Internet services, the opportunity for exchange and barter involving sexually explicit materials has dramatically increased the amount of child pornography available on line. Child molesters and pornographers frequently communicate in select online newsgroups and facilitate through technology videographic and still images of child sexual abuse, both from existing collections as well as in response to requests for new materials. The increase in the number of victims, as manifested by newer child pornographic images and bolder production techniques, has necessitated an equally innovative investigative response. The Postal Inspection Service has risen to this challenge and continues to ferret out, identify, and arrest offenders who traffick in child pornography videotapes and computer disks, or who otherwise sexually exploit children, through the U.S. Mail. Today, almost all of the child exploitation investigations conducted by Postal Inspectors have a common nexus with the Internet and the U.S. Mail.

Postal Inspectors have established a nationwide network of intelligence incorporating a wide variety of undercover programs designed to identify suspects and develop prosecutable cases. These undercover operations recognize the clandestine nature of their targets and capitalize on the inherent need of offenders to validate their behavior through contact with individuals like themselves. The investigative techniques used in these operations include the placement of contact advertisements in sexually oriented publications; the infiltration of Internet newsgroups and chat rooms; and the use of confidential sources. The computer has proven itself to be an invaluable investigative tool in identifying individuals who are using the mail to traffick in child pornography or otherwise sexually exploit children.

A technique employed by Postal Inspectors as part of conducting their undercover operations is to control the delivery of child pornography to the requestor’s address. Following its delivery, an anticipatory federal search warrant is immediately executed on the suspect’s property. The item just delivered, along with any other relevant evidence, is then seized. On March 21, 2006, in *U.S. v. Grubbs*, the Supreme Court reported its unanimous decision, ruling that anticipatory search warrants are lawful as long as sufficient probable cause exists when the warrant and supporting affidavit are presented to a magistrate.

#### **The Connection between Child Pornography and Child Molestation**

During fiscal year 1997, the USPIS began compiling statistical information on the number of child pornography suspects that were also child molesters. Additionally, the

USPIS began to collect data on the number of child victims identified and rescued from further sexual abuse as a result of investigations conducted by Postal Inspectors. Since 1997, 802 child molesters were identified and stopped, and 1,048 victimized children were rescued. Of the 2,433 individuals arrested by Postal Inspectors since 1997 for using the U.S. Mail and the Internet to sexually exploit children, actual child molesters were identified in one out of three cases.

#### **Interagency Cooperation**

In carrying out its mission to combat child pornography, the USPIS works closely with the DOJ, particularly, DOJ's Child Exploitation and Obscenity Section, the Federal Bureau of Investigation, the Bureau of Immigration and Customs Enforcement, INTERPOL, the National Center for Missing and Exploited Children, and other domestic and international law enforcement agencies. Postal Inspectors across the country have formed working partnerships with the federally funded Internet Crimes Against Children (ICAC) task forces.

The USPIS is an active member of the Attorney General's Federal Agency Task Force on Missing and Exploited Children. A Postal Inspector is assigned full time to the National Center for Missing and Exploited Children, also known as the NCMEC, in Alexandria, Virginia. The National Center's Cyber Tipline reports are regularly reviewed and forwarded to USPIS child pornography specialists in the field for follow-up investigation or referral to another law enforcement agency, as appropriate.

#### **Raising Public Awareness and Other Outreach Initiatives**

Postal Inspectors play a special role not just through the investigations they perform, but in their efforts to raise public awareness about child sexual exploitation. In May 2001 the USPIS launched a national crime prevention initiative with the NCMEC to raise public awareness of the online victimization of children. As part of the initiative, a USPIS employee designed an eye-catching poster with a powerful message urging all citizens to report suspected child exploitation to the NCMEC's Cyber Tip line. It was printed and displayed in 40,000 post offices nationwide where it was viewed by as many as 8 million postal customers on any given day.

The USPIS has co-sponsored, exhibited, and presented at the National Symposium on Child Sexual Abuse, held in Huntsville, Alabama, home of the nation's first Child Advocacy Center founded by U.S. Representative Bud Cramer. In addition, Postal Inspectors have made presentations and conducted training on child exploitation at local, national, and international conferences and through DOJ and NCMEC sponsored training programs. Postal Inspectors regularly make presentations to civic groups and school associations on topics related to Internet safety.

Internationally, the USPIS has played an important role in INTERPOL's Specialist Group on Crimes Against Children since the group's founding in 1991. Postal Inspectors have made presentations and provided training on child exploitation to delegates from countries around the world. In August 1996 the USPIS delegate to the Specialist Group on Crimes Against Children conducted work shops for delegates from more than 120 countries at the first World Congress on the Commercial Exploitation of Children, held in Stockholm, Sweden.

Postal Inspectors are so recognized for their expertise on the subject of child pornography and child exploitation that their views and experience have been published. Much of this testimony, in fact, derives from a treatment written by Postal Inspector Raymond Smith, in the soon to be published book *Medical, Legal, & Social Science*

*Aspects of Child Sexual Exploitation --- A Comprehensive Review of Pornography, Prostitution and Internet Crimes.*<sup>1</sup>

### **Commercial Child Pornography Distributors**

The U.S. Postal Inspection Service was the first federal law enforcement agency to begin aggressively identifying, targeting, and arresting commercial child pornography distributors. Under the 1977 Protection of Children Against Sexual Exploitation Act, only the commercial distribution of child pornography was against the law.

### **Operation Special Delivery**

In May 1996 the U.S. Postal Inspection Service announced the results of Operation Special Delivery, a highly successful, pro-active undercover operation. The operation shut down the largest known commercial child pornography business ever encountered by authorities in the United States up to that time.

The ring-leader of the criminal enterprise, Troy Anthony Frank, doing business as Overseas Male, produced child pornography using young Mexican males, some as young as 7-years of age, in Mexico City and Acapulco, Mexico. The original videotapes were then smuggled into the United States and distributed by mail from San Diego, California, to customers throughout the country. Business records seized during the investigation revealed the company made as much as \$500,000 per year. Before the investigation into the ring-leader Troy Frank concluded, he committed suicide.

As a result of Operation Special Delivery, Postal Inspectors identified a large number of mail-order customers who knowingly purchased child pornography from Troy Frank. Over 130 searches in 36 states in the United States were conducted, leading to the identification of numerous child molesters, pornographers, and the rescue of child victims. Vast quantities of child pornography material were found and destroyed. One hundred offenders were ultimately arrested and prosecuted, among which were members of the clergy, youth leaders, school teachers, police officers, an attorney, a history professor, a medical doctor, and a school counselor.

### **The Landslide Investigation and Operation Avalanche**

There has been no investigation in the history of child pornography comparable to the Landslide investigation and Operation Avalanche. This landmark case was conducted under the direction of the USPIS and illustrates the success that can be achieved when domestic and international law enforcement work together.

In 1999 an alert Postal Inspector in St. Paul, Minnesota, discovered an advertisement on the Internet that had been placed by Landslide Productions, Inc. Further investigation revealed that Landslide Productions based in Ft. Worth, Texas, sold subscriptions to child pornography Web sites. The investigation was assigned to Postal Inspector Robert Adams, now retired, in the Ft Worth USPIS office. Inspector Adams teamed up with Detective Steven Nelson, also now retired, of the Dallas Police Department's Internet Crimes Against Children (ICAC) Task Force, and they launched an undercover investigation into the activities of Landslide Productions. Their work was the beginning of an investigation of such unprecedented magnitude that, even early on in the case, Postal Inspector Adams reported to his higher-ups he "had a lion by the tail."

Owned and operated by Thomas and Janice Reedy, Landslide Productions was a multi-million-dollar child pornography enterprise. Using the screen names of "Houdini"

---

<sup>1</sup> Chapter 24, "The Work of the United States Postal Inspection Service; Combating Child Sexual Exploitation," by Raymond C. Smith, reported in *Medical, Legal & Social Science Aspects of Child Sexual Exploitation – A Comprehensive Review of Pornography, Prostitution and Internet Crimes*, by Richard Estes, Victor Vieth, Sharon Cooper, Angelo Giardino and Nancy Kellogg (St Louis MO: GW Publishing Inc, 2006)

and "Money," the Reedys used their business to advertise and sell prepaid subscriptions to adult and child pornography Web sites to customers from around the world. Landslide Productions was, in fact, a gatekeeper for a number of international Web masters, advertising and marketing child pornography from countries such as Indonesia and Russia.

Initially, the Reedys were bold in their online marketing, using banners such as "Child Porn-Click Here" and "CHILD R@PE." They eventually changed their advertisements to more covert suggestions of the content of the Web site. For \$29.95, an individual could purchase a 1-month subscription to any number of graphic child pornography Web sites. Most customers used credit cards for their purchase; some customers mailed checks, cash, or money orders to Landslide's post office box address in Ft. Worth. The cash flow for Landslide Productions was significant at times, amounting to as much as \$1.4 million per month. Not surprisingly, the Reedys enjoyed the fruits of their labors, living in an upscale community in Fort Worth and driving top-end Mercedes Benzes. The Reedys were living a grand lifestyle at the expense of sexually abused and exploited children.

In September 1999 the investigation conducted in concert with the U.S. Attorney's office for the Northern District of Texas, the Child Exploitation and Obscenity Section (CEOS) of the DOJ, and USPIS National Headquarters, gathered sufficient probable cause to obtain federal search warrants. On September 8 six federal and state agencies executed a series of federal search warrants on the primary business location of Landslide Production, a secondary Landslide office in Dallas, Texas, and the Reedys' personal residence. The simultaneous raids, led by the USPIS, took more than 18 hours to complete. Under the direction of the USPIS's Forensic and Technical Services Division, Digital Evidence Section, careful efforts were taken to seize, secure, and protect the numerous computer systems located within the properties searched. The data extracted from the computer servers would later be known as the "Holy Grail." Among the evidence seized under the scope of the warrants were financial records. One of the operation's Web masters received more than \$98,000 in one month alone for providing child pornography Web sites to its customers.

Through Landslide Productions' network of computer systems and the World Wide Web, the Reedys provided child pornography to thousands of paying customers throughout the world. The success of their endeavor was based on supply and demand. Customer demand escalated, promoting further production as well as demands for newer and more novel material. Real children were sexually abused and their abuse photographed or videotaped to satisfy the needs of a specific clientele.

In April 2000 the Reedys were charged in a Fort Worth U.S. District Court. A federal grand jury returned an 89-count indictment against them, charging conspiracy to advertise and distribute child pornography and possession of child pornography. Plea offers by the prosecutors were declined and the case went to trial. Defense attorneys argued that the Reedys were not aware of the actual content of the various Web sites they advertised; however, evidence obtained from the Reedys' computers revealed otherwise.

During the trial, a detective from the United Kingdom's National Crime Squad summarized the inescapable bottom line issue with regard to child pornography. The detective, by way of illustration, told the story of two children who are well known in the world of child pornography. Helen and Gavin are British children who were sexually abused and exploited by their stepfather. As the detective explained, the children are victimized again and again whenever their pictures are reproduced, sold and further disseminated.

At the conclusion of the case, the jury found the defendants guilty as charged on all counts of the indictment. On August 6, 2001, Thomas Reedy was sentenced to 15 years in federal prison on each of the 89 counts charged. The judge ordered that each 15-year term run consecutive to the previous term for a total of 1335 years. Janice Reedy was



sentenced to a 14-year term. On August 8 Attorney General John Ashcroft and the Chief Postal Inspector held a press event and publicly announced the investigation and results. The sentences were appealed to the U.S. Court of Appeals for the Fifth Circuit. On appeal, Thomas Reedy's sentence was reduced to 180 years—in essence, a life sentence—and Janice's remained the same.

Using intelligence gained from the Landslide investigation, Postal Inspectors launched Operation Avalanche in collaboration with the federally funded ICAC Task Forces, resulting in the arrest of hundreds of offenders here in the United States. Internationally, Postal Inspectors worked with INTERPOL and other law enforcement agencies around the world tracking down more Landslide customers and suppliers. More than 8,000 search warrants to date have been carried out, making this the largest global operation ever undertaken.

No single offender profile could be created for those individuals who purchased child pornography from Landslide's criminal business. Occupations of the offenders included, but were not limited to, attorneys, physicians, firefighters, professional counselors for children, teachers, clergy, and law enforcement officers.

Through Operation Avalanche, vast quantities of child pornography were seized, scores of individuals arrested, and many children rescued from further sexual abuse and exploitation.

On October 23, 2002, President George W. Bush was personally briefed by representatives of the USPIS on the Landslide investigation and Operation Avalanche. Following the briefing, the President addressed a group of law enforcement personnel and child protection advocates gathered at the White House. In his statement, the President made a commitment to the American people: "Anyone who targets a child for harm will be a primary target of law enforcement. That's our commitment. Anyone who takes the life or innocence of a child will be punished to the full extent of the law" (Bush, 2002). The President used Operation Avalanche and the work of the Postal Inspectors as an example of the government's aggressive efforts to combat the sexual exploitation of children.

### **Operation Lost Innocence**

In September 2002 Angel Mariscal, an Ecuadorian national was arrested by the Postal Inspection Service in Miami, Florida. He was charged with distributing child pornography by mail and indicted on conspiracy charges to produce and ship child pornography. The investigation that ensued revealed a horrifying case of sexual abuse, rape, and commercial exploitation of more than 150 child victims, unraveling an international child pornography ring of shocking proportions.

In 1989 Angel Mariscal began conducting a mail order child pornography business. He produced the child pornography outside of the United States, imported it into the United States, and then mailed it to customers who had previously placed orders in response to advertisements or catalogs. The majority of the victims were Cuban and Ecuadorian children between the ages of 9 and 16. The child pornography was personally produced by Mariscal and his accomplices, featuring Mariscal himself as the one who raped and molested the children. When his business dissolved in September 2002, the videotapes he produced sold for as much as \$975. It was later learned that Mariscal was HIV positive.

In December 2002 Mariscal was indicted in the Southern District of Florida on charges of Conspiracy to Produce Child Pornography, Advertising Child Pornography, and Importation of Child Pornography. Based on information provided by Postal Inspectors, law enforcement authorities in Cuba and Ecuador arrested five co-conspirators and identified a number of child victims. Postal Inspectors participated in Mariscal's arrest in Ecuador. He was tried and convicted in April 2004 and sentenced to 100 years in federal prison – in essence, a life sentence.

Although cases like these involving the commercial distribution of child pornography frequently get the most public attention, they are not as common as investigations into non-commercial traffickers. Non-commercial cases involve perpetrators who exchange child pornography with others – unlawfully receiving, distributing, and possessing child pornography for their own personal use and sexual gratification. However, the investigation of non-commercial traffickers often leads Postal Inspectors to the very people who produce child pornography, and ultimately to the identification and recovery of children who have been victimized. Following are significant investigations conducted by Postal Inspectors into non-commercial traffickers of child pornography.

#### **Non-Commercial Traffickers**

**Covington, Kentucky** - In March 2006 Postal Inspectors were notified about a package in the mail that was believed to contain child pornography. The package was addressed to a Covington, Kentucky man. Working with the Covington Police, Postal Inspectors searched the intended recipient's residence and uncovered hundreds of sexually explicit magazines, videos and DVDs of minor males. The man used the U.S. Mail to receive and distribute child pornography, including pictures taken by the subject himself. He was immediately arrested on state charges of disseminating child pornography. Efforts are underway to identify the children depicted in the photographs. Federal prosecution is pending.

**Slinger, Wisconsin** - In February 2006 first-degree homicide charges were filed against a subject who, in a murder-for-hire scheme, conspired to have murdered his 16-year old stepdaughter, whom he allegedly sexually abused for ten years, as well as two others who had witnessed the abuse. The subject came to the attention of Postal Inspectors in June 2005 when he attempted to purchase child pornography from an undercover operation run by Postal Inspectors. His abuse of his stepdaughter came to light in the course of the investigation. The case was worked jointly with the Washington, Wisconsin County Sheriff's Department and Wisconsin Department of Justice (ICAC). The subject faces 60 years imprisonment on each conspiracy charge if convicted. A cash bond of \$500,000 was set.

**Meridian, Mississippi** - In January 2006 a resident of Meridian, Mississippi, was arrested after he traveled to Birmingham, Alabama, intending to have sexual intercourse with what he believed to be an 11-year old girl. The "girl" was actually an undercover Birmingham, Alabama Police Officer working with Postal Inspectors and FBI Special Agents in an online sting operation. The subject corresponded with the undercover officers via the U.S. Mail, sending order forms and payment to the "escort service." The subject was interviewed and subsequently admitted to secretly videotaping children from his church where he was actively involved in youth programs. The children were filmed changing clothes. The investigation is continuing with federal prosecution pending in Alabama and Mississippi.

**Memphis, Tennessee** - In May 2005 a suspect and his "on-line girlfriend" were sentenced in federal court for using the mail and Internet to distribute and receive child pornography. The suspect was sentenced to 15 years in prison and five years' supervised release; his girlfriend received five years in prison and two years' supervised release. Postal Inspectors initiated the investigation when the suspect's wife discovered CDs containing child pornography in their bedroom and a mailing envelope bearing the suspect's name and address. A search warrant was executed on the residence and tens of thousands of child pornography images were discovered on his computer. Several pornographic images of his neighbor's granddaughter were also recovered. The suspect later pled guilty to producing the images and to using the mail and the Internet to distribute and receive child pornography.

**Brimfield, Ohio** – In December 2005 a suspect pled guilty in state court and was sentenced to life in prison for the rape of a child. The suspect was arrested six months earlier on charges of gross sexual imposition and felony rape following an investigation conducted by Postal Inspectors. Evidence seized during a search of the suspect's residence revealed he had received child pornography via the U.S. Mail. The suspect later admitted to three separate instances of sexual conduct with minors. Follow-up investigation led to the identification and interview of one of the victims, a 14-year-old girl who was only 8 years old at the time the molestation began, and the daughter of one of the suspect's co-workers.

**Kirkwood, Illinois** - In January 2006 a Kirkwood, Illinois, man pleaded guilty to a 4-count federal indictment for production of child pornography and receipt of child pornography. The man came to the attention of Postal Inspectors during the course of an undercover investigation. Inspectors determined that the suspect, a 31-year-old, married, father of a pre-school aged son, regularly contacted young girls on the Internet and convinced them to meet him in local parks where they would engage in sexual activity. He also convinced the girls to take sexually explicit photographs of themselves and mail the pictures to him. Three child victims were identified through this investigation. The man is scheduled for sentencing in April 2006

**Redwood City, California** - Postal Inspectors arrested a 41-year-old man in July 2005 for violating federal child pornography laws. The previous January, Customs and Border Protection personnel assigned to the international mail facility in Los Angeles intercepted a number of DVDs containing child pornography that were addressed to the suspect. The DVDs were coming from Thailand. Postal Inspectors obtained and served a federal search warrant on the suspect's home, seizing additional evidence consisting of CD-ROMs, ZIP disks, and his computer. Following a comprehensive review of the evidence, it was determined the suspect possessed in excess of 127,000 child pornography pictures and videos. The National Center for Missing and Exploited Children has positively identified over 400 of the children depicted in the images. The suspect is free on \$100,000 bond pending trial.

#### **The Mighty Efforts of a Small Agency**

For a small federal law enforcement agency, the USPIS deals a mighty blow to those who would use the mail to produce, transmit, or possess child pornography, and who would otherwise sexually exploit children. The expertise of Postal Inspectors is demonstrated by the number of times prosecutors and other law enforcement agencies turn to the Postal Inspection Service for assistance with particularly difficult cases.

In August 2000 a Postal Inspector in Tampa, Florida, was called upon by local law enforcement to assist in a missing child case when it was suspected the child may have been lured away from her home by an individual she met on the Internet. The parents found evidence of correspondence with the suspect in their daughter's bedroom. A forensic examination of the child's computer and other evidence obtained by Postal Inspectors resulted in the identification of the suspect who was believed to be living in Greece. Through coordination with the NCMEC, INTERPOL, the U.S. and Greek embassies, and with the assistance of the FBI in Greece, the suspect was arrested in Athens on February 1, 2001. The 14-year old girl, having been traumatically sexually abused by the suspect, was recovered and reunited with her family. Postal Inspector April Hindin, the lead agent, was recognized for her tremendous work in this case when she was presented the following year on Capitol Hill with the National Missing and Exploited Children's Award.

In addition to Postal Inspector April Hindin's recognition, other Postal Inspectors have received the prestigious National Missing and Exploited Children's Awards for the past seven consecutive years. The awards are given at a Congressional Breakfast and Awards Ceremony in cooperation with the NCMEC, here in Washington D.C. to

investigators who have conducted outstanding investigations in the cases of missing and exploited children. Singled out in 1999, 2001, 2003, and 2004 Postal Inspectors were given top honors by being named Officers of the Year. No other agency has achieved such acclaim.

More than any award or other recognition, however, there is no greater satisfaction for a Postal Inspector than the knowledge they have helped the very people in this world least able to defend themselves. For one Postal Inspector that moment came in 2003 when a former victim wrote:

*When I was a little girl, when I was being photographed and raped, I used to try and send messages with my eyes down the lens, in the hope that one day a "good person" might see and come and help us. It took years for me to realise (sic) that no one was looking at my face. You saw our face. We want you to know, that we know, how hard this must have been for you all and we thank you from the bottom of our hearts for your courage and fortitude. Your actions have changed our lives and changed the future lives of thousands of innocent children who were yet to come. Thank you Thank you Thank you.*

We have come a long way since the first federal child exploitation laws were enacted in 1977, but we still have much further to go. Only through our continuing efforts, both individually and collectively, at all levels of government and private enterprise, can we ensure that children are protected from this type of victimization, and if victimized, that they receive the services and assistance they need, and that their offenders are caught and prosecuted to the full extent of the law. Thank you for the opportunity to share with you the very special contribution that U.S. Postal Inspectors make in the fight against the sexual exploitation of children through the Internet.

MR. WHITFIELD. Thank you, Mr. Kezer, and our next witness is Raymond Smith, who is the Assistant Inspector in Charge for Child Pornography and Adult Obscenity, at the U.S. Postal Inspection Service, and you are recognized for 5 minutes.

MR. SMITH. Thank you, Mr. Chairman. Good morning. And members of the subcommittee. I am very pleased to be here today on this particular topic, because I have devoted a great deal of my career to investigating these types of crimes. I investigated my first child pornography case in 1982, and now I am able to manage our programs at the national level.

People unfamiliar with the work of the Postal Inspection Service often ask why are postal inspectors involved in these things that, today, seem to involve so much of the Internet? The answer is, because along with the Internet, the bad guys are still using the mail. In fact, 98 percent of the cases investigated by postal inspectors today involve the mail as well as the Internet. We have developed a great deal of expertise using the computer and the Internet as an investigative tool to ferret out and identify the offenders who are trafficking in child pornography videotapes, computer disks, or otherwise sexually exploiting children through the mail.

We know how these offenders think, how they operate, and what their psychological needs are. The worst of these offenders exhibit highly compulsive and predictable patterns of behavior. They have a need to validate their behavior with like-minded individuals through communication, not only on the Internet, but also in the mail. Postal inspectors use a wide variety of proactive undercover operations to identify suspects, and develop strong cases for prosecution. In many cases, we employ the use of controlled deliveries by mail, something only postal inspectors can do. Following the controlled delivery, an anticipatory Federal search warrant is executed on the suspect's property, and the child pornography that was just delivered under controlled circumstances is recovered, along with any other relevant evidence associated with the underlying criminal activity.

Coincidentally, on March 21 of this year, in *U.S. v. Grubbs*, a Supreme Court case, it was also a Postal Inspection Service case, the Court came back unanimously upholding the lawfulness and use of anticipatory search warrants. Commercial child pornography dealers have long been targeted by postal inspectors. In 1996, Operation Special Delivery shut down the largest commercial distributor at that time, grossing upwards of \$500,000 a year. After dismantling the business, postal inspectors took it over in an undercover capacity, and targeted their customers across the country, resulting in over 100 successful prosecutions. Many of these individuals had been sexually abusing children.

Perhaps the most celebrated commercial child pornography business operating on the Internet was Landslide Productions, owned and operated by Thomas and Janice Reedy out of Fort Worth, Texas. This company took in upwards of \$1.4 million a month. They were advertising and selling child pornography websites to subscribers around the world. Later to become known as Operation Avalanche, this landmark case was conducted under the direction of the U.S. Postal Inspection Service, in close cooperation with the U.S. Department of Justice Child Exploitation and Obscenity Section, along with the Dallas Texas Police Department Internet Crimes Against Children Task Force. In the end, Thomas Reedy received 180 years in Federal prison, in essence, a life sentence. His wife received 14 years. Postal inspectors then worked with the various Internet Crimes Against Children Task Forces across the country, and arrested hundreds of paying subscribers in the United States, then working through Interpol and with our international partners, over 8,000 searches were conducted around the world, making this the largest global operation ever undertaken. Huge amounts of child pornography were seized, scores of individuals were arrested, and many children were rescued from further sexual abuse.

Although commercial cases like these get the most public attention, it is oftentimes the most typical noncommercial case that identifies child molesters, the producers of this material, and their child victims. Just a couple weeks ago, in Covington, Kentucky, postal inspectors working with Covington PD arrested a man after a package containing DVDs of nude minor males was delivered in error to the Cincinnati Reds ballpark. During a search of the man's home, hundreds of vintage child pornography magazines, videotapes, and DVDs were discovered, along with packaging material for receiving and distributing child pornography through the mail, including pictures apparently taken by himself of kids. Efforts are underway to identify these children, and Federal prosecution has been authorized.

In another case last week, a 15-year veteran of the Huntsville, Alabama Police Department was arrested by postal inspectors on a Federal charge of production of child pornography. This offender, discovered after he traveled to Titus, Texas, to sexually abuse a 14-year-old girl that he met on the Internet, continued to keep her in his confidence, and convinced this girl, after mailing her a package of a sexual aid and a digital camera, to take pictures of herself. The digital memory card from that camera was then mailed back to the police officer in Texas. Over 300 such images were produced by this young child. He is in custody.

Deputy Chief Kezer mentioned the national awards received by postal inspectors, but I must tell you this, more than any other award or recognition, there is nothing greater than knowing that you have helped one of the many, very many people in this world least able to defend themselves. For me, one of those occasions came in 2003, when a former victim learned of our Operation Avalanche, and wrote to me. I would like to read one paragraph from her correspondence: "When I was a little girl, and when I was being photographed and raped, I used to try to send messages with my eyes down the lens, and hope that one day, a good person might see and come to help us. It took years for me to realize no one was looking at my face. You saw our face, and we want you to know that we know how hard this must have been for all of you, and we thank you from the bottom of our hearts for your courage and your fortitude. Your actions have changed the future lives of thousands of innocent children who are yet to come. Thank you, thank you, thank you."

In closing, we have come a long way over the years, but we have still got much further to go. Only through our continuing efforts, both individually and collectively, at all levels of government service, and through private enterprise, can we help ensure that victims and their families get the services and assistance they need and deserve, and that

their offenders will face the swift and righteous justice that we, as a society, demand.

We all have the need here, and the obligation, to make this world a safer place for our kids. Thank you.

MR. WHITFIELD. Well, Mr. Smith, thank you, and thank all of you for your testimony. You have provided some tremendous suggestions for us to consider. You have provided some tremendous insights.

We have two votes on the House floor right this minute, and so what we are going to do is we are going to recess this hearing until 12:15. So, if you all wouldn't mind coming back in at 12:15, we have questions for you.

MR. STUPAK. Mr. Chairman, if I may, let us see, the full chairman is here, Chairman Barton, I see that the Attorney General, Mr. Gonzalez, testified this morning 9:00.

CHAIRMAN BARTON. I have already been down there.

MR. STUPAK. Okay. Good. Just wanted to make sure you are aware of it, because on page 6 and 7 of his testimony, he talks about child pornography on the Internet. It would be great if we could get him up here.

CHAIRMAN BARTON. I have already been down there, and I have a scout down there, so when he gets ready to leave, he has agreed to talk to me. We are going to have a little visit.

MR. STUPAK. Thank you.

CHAIRMAN BARTON. We are ahead of you.

MR. WHITFIELD. We will recess until 12:15.

[Recess.]

MR. WHITFIELD. The hearing will reconvene, and I apologize we are 5 minutes late, but thank you for your patience.

Dr. Kardasz, in your testimony, you talked quite a bit about retaining data on subscriber and content information. You are the one that mentioned that, aren't you?

MR. KARDASZ. Yes, sir.

MR. WHITFIELD. As one of the possible solutions or helpful solutions, would you elaborate on that just a little bit more, and also, what would you anticipate would be the objections to doing that?

MR. KARDASZ. Every computer connected to the Internet is identifiable by what is called an Internet Protocol address, and it is a series of numbers. It is similar to the numbers you have connected to your cell phone. You have got a cell phone number. So, through subpoena powers, we can start to trace that back, and in the cell phone industry, they keep those records for long periods of time, but that is not always the case in the Internet service provider industry. Some providers keep those records, so that we can chase back the offender for longer

periods of time than others. So, as in a case that Special Agent Waters described, if we are trying to track back on an offender, and the subscriber information that is connected to that Internet Protocol address is not available, then we are at a dead end, and I think the objections would be the cost. Now, they are going to say, and I don't disagree with it, that that is a lot of data that they are going to have to retain, and then, the subsequent searches they have to do in response to our subpoenas is going to cost them some manpower, so I think that is what an IP address, and that is the data storage that we need, and I think that is the issue, the cost.

MR. WHITFIELD. And what would be the suggestion on the length of time to retain the data?

MR. KARDASZ. Well, when we get an investigation in, it is not like we always get it in the next day.

MR. WHITFIELD. Right.

MR. KARDASZ. So, sometimes, there is a long period of time that passes before we get it in, it gets up to the investigator's queue, and he is able to work it, and then he is able to get a subpoena out.

MR. WHITFIELD. Right.

MR. KARDASZ. So, I have heard my colleagues bounce around 90 days would be nice, a year would be great, but the longer period of time that it has to be kept, then, the more data overall has to be stored by that Internet service provider, so the more storage capacity they need, the more that might cost them.

MR. WHITFIELD. Now, I assume the entire panel would agree that that would be an invaluable tool, and it would be a positive development. Is that true? So, no one would object to some statutory language, or action to that effect.

What about applying this data retention to cell phone companies that are also providing the ability of a person to exchange images?

MR. KARDASZ. I am not familiar enough with the data retention schedules that cell phone companies have now. I get the sense that they already retain some data, but it would be very applicable to them. Some of those cell phones now, as you know, can also capture pictures. We have had some child pornography cases attached to those folks that are running around with cell phones capturing child pornography on their cell phone cameras.

MR. WHITFIELD. Is there anyone on the panel that would want to make any comment about the cell phone? Okay.

Mr. Waters, in your testimony, I know you showed the slide of the two children with the Santa Claus, and make sure I understand, those children were your children?

MR. WATERS. That is correct, Mr. Chairman. My two youngest.



MR. WHITFIELD. And they went to a local mall, and he was the Santa Claus, and then, you set yourself in a sort of a sting operation, and this is the same fellow. Is that correct?

MR. WATERS. That is correct, Mr. Chairman. My wife took them to the mall shortly after Thanksgiving, got the photos taken, and then, towards the end of December, I was online in a Wyoming chat room, just sitting around, and I was contacted by this same person.

MR. WHITFIELD. Was he convicted, or--

MR. WATERS. Yes, he was.

MR. WHITFIELD. Okay. Dr. Kardasz, you also mentioned something about responding to subpoenas within a certain period of time.

MR. KARDASZ. Yes, sir.

MR. WHITFIELD. Would you elaborate on that?

MR. KARDASZ. Well, Mr. Chairman, depending on which Internet service provider we are working with when we send a subpoena, they respond various lengths of time later. Ideally, we would like to get a response as soon as we can, particularly, in the case where we are working an active Internet sexual predator, for example, we are online, pretending to be a child. All we have is a screen name, so we do a little research on that screen name, and find out which Internet service provider sponsors that screen name. Now, we can subpoena that Internet service provider to say who is this person, Joe Smith at Yahoo!, at AOL, we can subpoena Yahoo! or AOL, and say who is this person? What is the background information behind that subscriber? So, then, depending on which Internet service provider is involved, it takes them different periods of time. If we could get that within--the quicker, the better, obviously, particularly if it is a missing child case that we are working. But if we can turn those subpoenas around within 2 weeks, that would be a beautiful thing.

MR. WHITFIELD. So, would all of you agree that one of the most difficult parts of your job is just trying to determine who the person is on the other line, right, or with the, as the website, or whatever. And so, the data retrieval would be important, the expedited response to subpoenas would be important. Do any of you have any other suggestions of some mechanisms that could be used to help you do your job better? Yes, sir.

MR. SMITH. Mr. Chairman, we have no statutory authority or otherwise authority to get administrative subpoenas. When we enter into an investigation now, and we have an individual's screen name, we must get a Federal grand jury subpoena to serve on that Internet service provider in order to get the account information. A number of years ago, under the last Administration, beginning with Attorney General Janet Reno and it was concluded by Attorney General Ashcroft, the FBI was delegated administrative subpoena authority by the Attorney General.

The authority went to the Attorney General, it was delegated to each individual U.S. Attorney's Office, and they in turn delegated it to the Bureau. Bureau agents can now write the administrative subpoena out quickly, get it out without going for a grand jury subpoena, and get that information back a lot quicker.

The Immigration and Customs Enforcement, they use a tool which I believe is called a customs summons, which is not necessarily designed as an administrative subpoena, but it serves the same purpose lawfully, and they are able to get that information. Postal Inspection Service cannot.

MR. WHITFIELD. So, Postal Inspection is the only agency in law enforcement that would not have the administrative--

MR. SMITH. No, at the Federal level, and I am not sure about Secret Service. I can't comment on that.

MR. WHITFIELD. Now, what is the difference in an administrative subpoena and--

MR. SMITH. It expedites things. Typically, we would have to go and make a phone call to an Assistant United States Attorney. Oftentimes, we get multiple, multiple names or screen names in an investigation. Give you an example. I am going to use the Justin Berry case, and I don't know all the intimate details with that case, but if there were 1,500 names, you have 1,500 screen names that came forward, we might want to know who those people are. What does that screen name resolve back to on the actual account information? Who holds the account, where do they live, et cetera, et cetera. We could conceivably go to a U.S. Attorney's Office, say I need 1,500 grand jury subpoenas, or maybe one, and list out 1,500 names. It just is cumbersome if we have to keep going back and bugging the U.S. Attorney's Office every day of the week to get another grand jury subpoena. With the administrative subpoena, it is a tool that the investigative agency can use to serve. Of course, it is all tracked and recorded, and they have to account for that information to the Justice Department.

MR. WHITFIELD. Yeah. Well, Mr. Swecker would be available to the FBI, correct?

MR. SWECKER. It is available at the supervisory level. It has been delegated down, and he is correct, it gives you the ability to move much faster, you are much more mobile and agile, because probable cause evaporates very quickly in these cases, and you really need to be able to move very quickly and able to get to either the customers or the abusers themselves, so this gives the ability to do that.

MR. WHITFIELD. Do you know if that tool was used in the Justin Berry case, or can you talk about it?

MR. SWECKER. Sir, I would love to talk to you about the case, but I cannot.

MR. WHITFIELD. All right. How many FBI field agents are devoted full time to child pornography, or child molestation cases?

MR. SWECKER. We are funded for 127. We actually have close to 250 agents working just Innocent Images, child abusers on the Internet.

MR. WHITFIELD. 250?

MR. SWECKER. Yes, sir.

MR. WHITFIELD. Now, we are told that there are six FBI special agents working at the Innocent Images National Initiative, that in fact, two slots are not filled. Even with having eight special agents devoted to this work full-time, given the magnitude, do you think that--well, he said 250, but we are told that there are six FBI special agents working on the Innocent Images National Initiative.

MR. SWECKER. There are six at NCMEC, at the National Center for Missing and Exploited Children. It is two agents, four analysts.

MR. WHITFIELD. Okay. But we are told that two slots are not filled. Is that correct?

MR. SWECKER. They are in the process of being filled. There is normal rotation in and out.

MR. WHITFIELD. Okay. Okay. Now, do you all feel that the financial services industry could do more to assist law enforcement in these cases, and if so, how do you think they could be more effective in what they are doing? How could they assist you more? Mr. Swecker.

MR. SWECKER. I watched Ernie Allen's testimony yesterday, and I think those types of initiatives, where you get cooperation from these PayPals and credit card companies and financial clearinghouses that enable the payments, some of them, right now, it is voluntary cooperation, if there is some method of ensuring that they will be cooperative. Some are more cooperative than others.

MR. WHITFIELD. Yeah. Mr. Plitt, do you have any comment on that?

MR. PLITT. We agree. We assist with those cases, and of course, our concern is that much of the money flows overseas. We are looking at the trans-border side of it. So, any international cooperation from the credit card companies, financial services companies in other countries, is what we target, and we also invite.

MR. WHITFIELD. And what about digital currencies?

MR. PLITT. Digital currencies. In the past, I would say eighteen months, digital currencies have started to appear in these cases, and they are absolutely important. They allow the free, unmonitored movement of money between countries, and to various Internet services. The currency

area is something we have been looking at for a while now, and they are occurring in these child exploitation cases.

MR. WHITFIELD. It seems to me the one impediment to effective prosecution in these cases is we have so many agencies across so many jurisdictions, and it must require a lot of coordination, and working with each other, and teamwork. You must all be frustrated by the complexity of prosecuting. Would that be accurate?

MR. SWECKER. If I may. There is plenty of work for everybody. And I worked drugs for a good part of my career, saw a lot of overlap and duplication. We are not seeing that in this area. I think everybody recognizes the importance of it, and I think it is better to have a good number of agencies working it. The National Center has been a very good clearinghouse for this type of activity. NCMEC has been very effective in that area, because we all have analysts out there. We all have investigators out there.

MR. WHITFIELD. Well, I know that many law enforcement agencies have jurisdictional disputes, but hopefully, this is one area, as you said, where there can be more cooperation and less concern about jurisdictional protections. I am assuming that is the way you all feel about it.

All right. My time has expired, so I will recognize Mr. Stupak.

MR. STUPAK. Thank you, Mr. Chairman.

Mr. Swecker, back in '99, Congress passed a law that required Internet service providers to report any knowledge the ISPs may have of child pornography to the Cyber TipLine, which is run by the National Center for Missing and Exploited Children, and then, they must forward that report to law enforcement agencies, and that is 42 USC § 13032, and we have fines in there for failing to report and all this. But this law did not require the service providers to monitor, to actively monitor their networks, but still, if they came across it, they were supposed to report it.

Tuesday, we learned from Mr. Allen that this law has never been implemented, because the Justice Department said they refused to issue the guidelines, or take any steps to implement it. The guidelines were drafted, we understand, in late 2000 under the Clinton Administration. Attorney General Ashcroft, for some reason, did not want to implement it. Any reason why?

MR. SWECKER. Sir, I am not sure. It would be a great tool. We see that success in the bank secrecy area, with the banks making referrals through the SAR process. This would certainly be a help to us.

MR. STUPAK. Were you aware of the law?

MR. SWECKER. I am aware of it, but I--

MR. STUPAK. Have you attempted to use it?

MR. SWECKER. Well, we don't have any guidelines or regs to implement it yet, so we haven't been able to use it.

MR. WHITFIELD. If I may interrupt. Mr. Swecker, would you talk to the appropriate people at Justice, and ask them to give a formal response to Mr. Stupak's question on that issue?

MR. STUPAK. Because it has been almost 7 years?

MR. SWECKER. Yes.

MR. STUPAK. And I think you mentioned, Doctor, about the ISPs, how important they could be to Internet service providers to helping us, here is a law that Congress did in '99, it is not even implemented.

MR. KARDASZ. Well, Congressman, one important thing that happened as a result of that law is that we got a flood of child pornography investigations that overwhelmed us, that came from some of the responsible ISPs that, when they were finding child pornography on their servers, they were reporting those to us, and we are still getting those investigations in today. So, part of that law is being implemented by those ISPs who have chosen to abide by it.

MR. STUPAK. Sure. Mr. Swecker, you mentioned--oh, Mr. Smith, you had a comment? I am sorry.

MR. SMITH. Just to follow up on that, with that law that requires ISPs to report violations to the National Center, that is the Cyber TipLine II part of the National Center, the I being the public. And as I understand it, the larger ISPs do, in fact, report the information, but hundreds and hundreds of small ones, if not thousands, do not, and then, there is no enforcement provision. There is no penalty associated with non-reporting.

MR. STUPAK. Well, there is a civil penalty up to \$100,000.

MR. SMITH. Okay. I don't know if it has ever been pursued.

MR. STUPAK. Well, testimony is showing that there are like 215 of the ISPs voluntarily report this stuff, but there are thousands upon thousands of thousands out there, and that is not even counting the wireless that we are starting to see more and more of now. So, I mean, it has got to be a phenomenal problem, but we are trying to design laws that will help you out, but when they sit for 7 years, and no, the first we learned about it was Tuesday, that there was a problem with it, according to the Attorney General, so that is why the full Chairman and everyone else wanted someone here to answer his questions.

Mr. Swecker, you mentioned the Justin Berry case. Is Justice in lead on that case? Who is the lead agency?

MR. SWECKER. We are the investigators, and we are the lead investigative agency on that.

MR. STUPAK. Who would be the lead person in charge of that?

MR. SWECKER. Within our agency, there are case agents around the country. Arnold Bell coordinates the investigation from our headquarters. He is the Unit Chief of the Innocent Images Unit.

MR. STUPAK. Right, Mr. Bell, who we asked for today.

MR. SWECKER. I would say, sir, that we are trying very hard not to jeopardize any future prosecution. I think there is logic in not commenting.

MR. STUPAK. And I don't think this committee has ever jeopardized one of your investigations, but I know Justin Berry and everyone else would just like to know what the heck you are doing. You got a very big black eye here Tuesday, and it is getting bigger by the minute, but you just keep saying well, we can't answer these questions. No one has asked any inappropriate questions, and I am sure if it was an inappropriate question which would jeopardize the investigation, the person, Mr. Bell or others, would say I can't answer that. We will answer in closed session. So don't give us that line.

You indicated there were 250 agents that work on child pornography in Justice?

MR. SWECKER. Within the FBI.

MR. STUPAK. Within the FBI. So you have 250 agents assigned to doing child pornography, or do you just have agents who, from time to time, may work on child pornography.

MR. SWECKER. That is actual agents working the system.

MR. STUPAK. Which their main emphasis would be child pornography.

MR. SWECKER. Sole emphasis.

MR. STUPAK. Okay. Mr. Swecker, how about forfeiture statutes. I think ICE has used them. Has Justice ever used forfeiture statutes to get the assets of these individuals? Have you ever used that mechanism?

MR. SWECKER. We have. I don't have any numbers for you.

MR. STUPAK. You are familiar with them with drug cases, then, right?

MR. SWECKER. Absolutely, and white collar cases as well.

MR. STUPAK. Any reason why they could not be used here? Is there anything we have to do to change the law to make sure you could use them in child pornography?

MR. SWECKER. I think we have the forfeiture tools available to us.

MR. STUPAK. Okay.

MR. SWECKER. That was one of the things that came into being very early on.

MR. STUPAK. Okay. Let me go back to the Berry case for a minute. If the FBI has an agreement, there is an understanding out there, it is my understanding, to provide all images to the National Center for Missing

and Exploited Children, but Missing and Exploited Children said they have never received anything. So, CEOS, then, probably has nothing from the Berry case. And the Berry case has been sitting for over, I think, 71 days now, if I count. So, what is going with that, then? I mean, if National Center has not received the information, then CEOS wouldn't have received the information. It seems like it is bottled up in Justice. Is that right?

MR. SWECKER. Well, again, let me just talk generically, if I may.

MR. STUPAK. Sure.

MR. SWECKER. When we get this volume of images in any case, we have to review it, each one of them, and filter out regular pornography, as opposed to child pornography. What we forward over, it has to be viewed, and some agent has to get on the screen, or print it out, and look at the images, and then, it goes over.

MR. STUPAK. Right.

MR. SWECKER. That is as far as I can go with that response.

MR. STUPAK. Okay. Well, if you have got 250 agents exclusively doing it, I think someone could get to it in 71 days, I would think. Seven months, I am sorry, 7 months. I said--can't read my own writing--7 months. So, there is no reason for it. And I can understand why Mr. Berry is frustrated.

In our testimony Tuesday, I think it was, the reporter from the New York Times indicated that credit cards are really the center of this, sort of money. Have you done anything to try to crack down on credit cards, transactions that are used in child pornography?

MR. SWECKER. Well, we can only address these credit card cases in the context of a case. I mean, if we go beyond that, we are not regulators, as we know, but we do find quite, I mean, this is a chokepoint for these types of cases. It is a good place to get your leads, and it is good place to center, but I will say that we get thousands and thousands and thousands of these credit card companies. The volume is overwhelming.

MR. STUPAK. Well, with credit cards, we see with the Internet pharmacy illegal sales. We see it with drug masking chemicals and devices for drug testing, and we see it with child pornography. Do you have any recommendations on what Congress should be doing to try to crack down on credit cards being used in an illegal manner like this?

MR. SWECKER. Sir, I would have to defer to main Justice on any of those legislative solutions.

MR. STUPAK. Mr. Plitt, if I may, you testified that ICE, your main areas are border, and then, of course, international, to help.

MR. PLITT. Yes, trans-border.

MR. STUPAK. So, like on the Berry case, did you assist there, since there is a tie in to Mexico?

MR. PLITT. No, I believe that, if I recall correctly, the ICE link to the Berry case came through the back door, if you will. Another ICE arrest occurred, and the individual indicated that he had purchased, I believe, access to Mr. Berry's site, so once that had occurred, we stepped back, because another agency was handling this case, the Bureau. There was one arrest, led to a second arrest. The second arrest was linked to Mr. Berry.

MR. STUPAK. Okay. So, all right. Dr. Kardasz, if I can, this law we have been talking about a little bit, 13032, where Internet providers, have you tried to access or use that law much? The Federal law, the one I have been speaking 42 USC § 13032, which Internet providers are supposed to contact you?

MR. KARDASZ. No.

MR. STUPAK. I am sorry, they contact National Center.

MR. KARDASZ. No, the way that that law has come to me is just that the images--

MR. STUPAK. Comes--

MR. KARDASZ. --that law have come back to me, and I don't work to enforce that law in any way.

MR. STUPAK. So, you are asking that these ISPs retain their information for 1 year?

MR. KARDASZ. That would be ideal, sir.

MR. STUPAK. Okay. And then, do you have anything like--in Arizona, is that where you are working, right?

MR. KARDASZ. Yes, sir.

MR. STUPAK. Do you have anything like an administrative subpoena that Mr. Smith spoke of, that allows you to move rapidly?

MR. KARDASZ. We do. It is very helpful.

MR. STUPAK. What do they call it out there?

MR. KARDASZ. Administrative subpoena, I believe. But what it allows my investigators to do is to write up a subpoena at their desk. The county attorney has authorized them to phone him, or contact him by email, tell the county attorney that they have an ongoing felony investigation, give them a little bit of background on what is going on, and then the investigator can fax the subpoena off to the Internet service provider, receive the information back from the Internet service provider, which saves the investigator from having to go find a grand jury, or some other legal authority, to get the subpoena authorized. So, that is the manner in which it speeds up our work.

MR. STUPAK. Well, I guess in the bill we are marking up, what we call a markup, I did an amendment to try to get the phone companies and



cables and others to develop new technologies to try to prevent child pornography. Hopefully, that will help you in your work. Technology as a free market system can come up with, hopefully, that will assist you.

And one more, if I may, Mr. Chairman. Mr. Plitt, you indicated that ICE was familiar with the Justin Berry case because of the arrest that was made. Did CEOS ask ICE about Justin Berry at all?

MR. PLITT. I don't believe they did.

MR. STUPAK. Okay. Thank you.

MR. WHITFIELD. Thank you, Mr. Stupak. At this time, we recognize the gentleman from Rhode Island, Mr. Bass.

MR. BASS. When Members of Congress from Kentucky look to the Northeast, they see New England as one State. I actually represent New Hampshire, but it is the same to you, sir.

MR. WHITFIELD. Thank you for reminding me.

MR. BASS. Mr. Waters, I was struck by your testimony, in which you said there were 4.4 million images worldwide, and 1.9 million images which appear to be domestic, and I am assuming that is because the source is a domestic address.

Do you have a way of telling how many hits are occurring on these websites? And this isn't a question just for you, but for anybody. Let us assume the data here is that you have two million images, in the United States. That is your testimony. I would appreciate comment from anybody here.

Anybody have any idea how many hits there are on these--first of all, how many websites are there, and how many hits are there on them? So, what is the size of the community?

MR. WATERS. Representative, the images that I spoke about, those are 1.9 million transactions, where people were offering to traffic in those images. Now, the 1.9 million, I can trace to IP addresses in the United States.

MR. BASS. So, the 1.9 million are the hits.

MR. WATERS. That is correct.

MR. BASS. Okay. I am just trying to get--transaction means that you ask for something on the Internet, or receive something on the Internet, and so, there were 1.9 million individual requests or receipts for information involving a picture of some child on the Internet, or a message, or something, right?

MR. WATERS. That is correct. This deals with, and this particular investigation, a very small set of movies depicting very young victims, very horrendous activity, when the investigator types in, using the software and searches for those, that is the number of download candidates that have been identified over that 24-month period. We have turned a corner somewhat in this area. It is now easier to download, and

faster to download 20 minute, 30 minute movies depicting these activities from these file sharing networks than from the websites.

MR. BASS. Peer-to-peer you are talking about now.

MR. WATERS. That is correct.

MR. BASS. And you have developed software to do what?

MR. WATERS. The software allows the investigators to regionalize their efforts, while contributing to the global network. So, the way it is set up, an investigator types in a search term consistent with these hardcore movies. He receives a list of download candidates for those movies, seven or eight thousand at a time. By submitting that list to servers in Wyoming, ICAC servers, he is given back a list that says of those, these nine are in your State, and then, he can focus his investigative efforts on those nine. But in the background, all of those are submitted to the central server, so from every other State, the investigators, be it FBI, ICE, ICAC, can connect to that server and receive the list of who saw what where.

MR. BASS. Can you just review, how many sites are there, domestically, that provide Internet for child pornography, roughly? Do you know?

MR. WATERS. Well, these move beyond the typical definition of a website. These are actually computers in people's homes, and there are millions. We have identified in this case, just using that series, over a million, 1.4 million unique IP addresses.

MR. BASS. What do you mean series? You are talking about a specific movie or something like that?

MR. WATERS. A subset of movies related to these victims.

MR. BASS. So, it doesn't even start to address the whole breadth of all the pictures that may exist. This isn't the whole scheme. This is just one program, so to speak.

MR. WATERS. Correct. This is just a subset, where I picked very young and very typically violent images of young males and young females. Like I said, these are typically under 8 years old, just in that set. We started out with about two hundred images and movies.

MR. BASS. And you got 1.9 million individuals that accessed that. How many pornographic, child pornography websites are there domestically? Did you answer that question, or does anybody know? Nobody has any idea, do they?

MR. WATERS. I don't think we know, sir. One characteristic you will see is that oftentimes, these websites will come up very quickly, go down very quickly. The site managers tend to do that, simply because it hides the ownership of the site. So, it is oftentimes difficult to estimate exactly how many there are.

MR. BASS. That leads me to another question. Is there technology being developed on the other side of this to deter you? Is that a sophisticated, active industry in itself, to deter your investigation?

MR. WATERS. It is. Of course, they seek to hide their identities.

MR. BASS. Nothing new there.

MR. WATERS. Yeah. Right. And the technology that they are going to employ is technology that is already out there. They very probably don't have any research and development activities to develop their own technology. They are using what is available. And peer-to-peer is a great example, because peer-to-peer is now more frequently used. It is easier to use, and of course, the users are becoming more sophisticated, as generations go on.

MR. BASS. How many rescues do you achieve in a given period?

MR. PLITT. Rescues are--

MR. BASS. Use your mic, please. Your mic is off.

MR. PLITT. ICE tries to specialize in the trans-border cases. The rescues occur at the local level, so I would refer to the ICACs on those.

MR. BASS. You two gentlemen from the Postal Inspection Service, how many of your child pornography cases involve the Internet?

MR. SMITH. Today, about 98 percent.

MR. BASS. Ninety eight percent? Give me an example--

MR. SMITH. One aspect of the Internet or the other. Let me give you an example.

MR. BASS. Okay.

MR. SMITH. This case that I just referenced, where the child was victimized in Texas. That started on the Internet, because the bad guy, the police officer in Alabama, contacted the child in Texas over the Internet, traveled to Texas, sexually abused her, and then returned to Alabama. They then communicated through the mail after that. He mailed her a package, which the mother discovered. That is how this case came to light. In the package was a vibrator, a digital camera, and a seven page, handwritten letter giving her specific instructions what to do. That is a violation of Federal law. It is a 15-year felony, just the mailing of the camera, if you--any communication facility to induce, coerce, or entice a minor to engage in that type of behavior. It is a 15-year hit. That is one example.

In chat rooms, targets hook up with the children, bad guys start talking to the kids, and then, they want to go to the telephone. They will mail the kids calling cards. Let us talk dirty on the telephone. Oftentimes, we will have a commercial site, which may distribute product through the mail. You have the newsgroups out there, where the bad guys all hook up with each other, or in the chat rooms, and then, they

end up mailing disks, DVDs, things of that nature, back and forth, although the initial contact is on the Internet.

MR. BASS. So, it is safe to say that the Internet has changed the nature of your investigations dramatically.

MR. SMITH. Dramatically.

MR. BASS. Yes, sir.

MR. KEZER. What you have to understand is the reason that percentage is so high is because those are the cases that we are targeting. Although we are working on the Internet, we are trying to identify cases that have the mail involved. That is our mission.

MR. BASS. One last question. Hypothetically, if there was one thing that Congress could do that is not financial, because we don't have jurisdiction over financial services, it is not judicial, because we can't deal with subpoenas here, but it had to do with interstate commerce and telecommunications, to assist you A, in conducting your, doing your job, or B, suppressing the problem, what would you suggest we do?

Anybody can comment. And we have got 1 minute and 20 seconds, so there is no rush.

MR. KEZER. Sir. I don't know who would be responsible for it, but someone had made the comment earlier that law enforcement can't do it all. It is absolutely essential that a comprehensive public education prevention initiative be developed, long term, nationally, and if at all possible, internationally. It is absolutely essential to curb this tide.

MR. BASS. Anybody else?

MR. PLITT. Yeah, I would like to second that. We see so many good initiatives, NGOs, that are trying to do the right thing, it is just that it is difficult for the person at the center of the problem, the child of the parent, to know where to go. So, a coordinated effort, which is education, which is outreach, even victim assistance, would be absolutely fantastic.

MR. BASS. Well, education is also not within our jurisdiction. The only suggestion I have heard all morning has been mandating that ISPs store their addresses longer. Any other suggestions besides that? Because if this hearing is going to lead to anything, it is going to have to lead to some sort of, if there is a legislative initiative necessary, what role would the Internet and telecommunications play in that solution? Any of you gentlemen follow that?

MR. WATERS. Well, I think one other area that might be valuable to us is if we can work more with industry, if there is some way that we can facilitate the corporations being able to come forward with solutions for us. There is a lot of--

MR. BASS. Corporations--what do you mean by that?

MR. WATERS. Like Microsoft, for example. As a good example, we have been working with them on tools to establish de-confliction mechanisms, to allow us to share this information, and get data faster to other law enforcement agencies. We need a serious partnership with business, as well, if that helps.

MR. BASS. My time has expired, Mr. Chairman.

MR. WHITFIELD. Thank you, Mr. Bass. Mr. Smith, there is just one question, and we will go on to Ms. DeGette. In this Texas case, what was the age of the victim in that case?

MR. SMITH. Fourteen years old.

MR. WHITFIELD. Fourteen, okay.

MR. BASS. One more thing, if I may, Mr. Chairman. Mr. Waters, the slide that you showed us, Santa Claus and all that, could you provide that for the record?

MR. WATERS. I have, sir, yes.

MR. BASS. Okay, good.

MR. WHITFIELD. Ms. DeGette, you are recognized for 10 minutes.

MS. DEGETTE. Thank you, Mr. Chairman.

I want to try to get a sense of the scope of this issue. As I understand it, the U.S. Postal Service has 35 agents working specifically on this issue. Is that correct?

MR. KEZER. Thirty-five.

MS. DEGETTE. And what about, Mr. Clark, what about ICE? How many agents are working from your agency?

MR. CLARK. I would have to defer to Mr. Plitt, who runs our Cyber Center, and basically, coordinates our national program.

MS. DEGETTE. Mr. Plitt.

MR. PLITT. Yes, the total would be about 140. That is about 90 agents in the field. On top of that would be another, let us say 30 or so doing the actual technical forensics, on computers, who are not necessarily the case agents. And then, between 10 to 12 at Cyber Headquarters.

MS. DEGETTE. Okay. And Mr. Swecker, the FBI, I think, has about 250 agents working on this. Is that right?

MR. SWECKER. That number fluctuates. It is 250 on the street working the cases. There is another group at headquarters in the Cyber Division, you might add 20 or 30 agents to that, and those that are at the Center.

MS. DEGETTE. And Dr. Kardasz, ICAC, how many agents from your agency are working on this issue?

MR. KARDASZ. We have four in the Phoenix Police Department, but we are networked through memorandums of understanding with about

44, 45 other local, State, and county agencies throughout the State of Arizona.

MS. DEGETTE. So, you are mainly working with local law enforcement agencies.

MR. KARDASZ. No--yes, ma'am, but we also work nationwide with the other 46 regional task forces throughout the United States.

MS. DEGETTE. Okay.

MR. KARDASZ. Each of them has groups like mine.

MS. DEGETTE. Representatives from all these agencies, do you all think that you have enough people working on this issue?

MR. KARDASZ. No, ma'am.

MS. DEGETTE. Do you, Mr. Swecker?

MR. SWECKER. We can always use more.

MS. DEGETTE. Yeah. Mr. Plitt.

MR. PLITT. If we tripled our staff, we would still have significant leads.

MS. DEGETTE. Yeah. And Mr. Smith, or Mr. Kezer, whoever.

MR. KEZER. I don't know if there is a law enforcement agency that doesn't believe that they could use more resources.

MS. DEGETTE. Well, I mean, the reason I am asking the--I know my Denver Police Department, they want more agents, too. They always want me to get Federal money for them, but the thing is, in this situation with this type of cybercrime that is going on, it has exploded, it seems to me. No one would disagree, would you? So, we have got, I heard today, 4.4 million images, 1.4 million users, according to someone's testimony. These other countries around the world have maybe 300,000 or something like that. If someone can tell me, how many pending Federal cases do we have right now, involving exploitation of kids on the Internet, sexual exploitation? Does anyone know? Mr. Swecker.

MR. SWECKER. I know we have an inventory of about 2,500, and then you have heard of thousands of other investigations on the part of the Task Forces.

MS. DEGETTE. How many cases are pending? How many criminal investigations have been filed?

MR. SWECKER. You would have to aggregate them all up with all the agencies--

MS. DEGETTE. Thousands?

MR. SWECKER. Thousands.

MS. DEGETTE. Okay. But we could potentially have many more thousands, if we had enough investigators, right? It seems to me that--I know this isn't in the purview of our committee, and that has stymied you guys a little bit, but it seems to me, Mr. Chairman, we should really work with the appropriators and the agencies, just to try to get them more

resources to fight this, because I started my life out as a criminal defense lawyer, and for crimes like this, and we saw it happen in this country, when child porn was going out through the mail. When you started enforcing it, child porn went down, right? I don't know who can answer that. Mr. Swecker.

MR. SWECKER. It did go down.

MS. DEGETTE. It did go down. These are the types of crimes, if you said to these perpetrators, you are going to go to jail for 15 years, it wouldn't deter all of them. There are still criminals out there. But if they knew that they would be caught and prosecuted, it would sure help, wouldn't it?

MR. KEZER. Certainly.

MS. DEGETTE. Yeah. I have a couple questions for Dr. Kardasz, and you testified, I thought, very helpfully about some actual proposed solutions. You said that the ISPs should retain the information on the subscribers for a year, and that they should have to respond to subpoenas within a week or faster, if it is an emergency, correct?

MR. KARDASZ. Yes, ma'am.

MS. DEGETTE. Well, my question is what is happening right now? Can you give me some examples where failure to maintain data has hurt or killed investigations?

MR. KARDASZ. Yes, and I think Flint Waters talked about--

MS. DEGETTE. He did give an example.

MR. KARDASZ. There are other cases like that out there, that because the particular Internet service provider didn't retain the data, the investigation just dead ends.

MS. DEGETTE. How often would you say that happens?

MR. KARDASZ. Well, it is hard to put a number on that, and I don't want to give you a bad number.

MS. DEGETTE. No.

MR. KARDASZ. Periodically.

MS. DEGETTE. Okay. And do you have an opinion why these ISPs fail to maintain this information?

MR. KARDASZ. My sense is that it costs them money to do that. It is not that they are evil. It is not that they are trying to protect these folks. But data storage takes a box with storage capacity in it, and it starts to fill up, and that costs money. Retrieving that data takes somebody to go in, takes their time to go in and type in the information that they need, and return that information to law enforcement. So, it is a tie-up of their personnel and their resources. It is a cost issue for them, I think.

MS. DEGETTE. How often do we have these ISPs refusing to respond to subpoenas in a timely fashion?

MR. KARDASZ. I can't respond to well from Arizona, because it really hasn't been an issue there with--

MS. DEGETTE. Has it been--

MR. KARDASZ. --the ISPs that we have worked with.

MS. DEGETTE. Anyone else have an opinion on that? Yes, Mr. Waters.

MR. WATERS. Yes, ma'am. In some jurisdictions, it is as high as 40 percent.

MS. DEGETTE. Wow.

MR. WATERS. Where they either don't respond, or they say they do not have the records.

MS. DEGETTE. And have there been efforts made to make these folks voluntarily comply?

MR. WATERS. Yes, there have. We have met with ISPs. We have also had some meetings facilitated by the National Center for Missing and Exploited Children to help, and some ISPs are becoming very cooperative and helping us.

MS. DEGETTE. Can you tell me which ISPs are particularly uncooperative? Look, these people are enabling the raping of our children in this country. I don't have any sympathy for them.

MR. WATERS. The ISP that would not respond in the case in Colorado, where we were trying to track down that 2-year-old child was Comcast.

MS. DEGETTE. Comcast. Okay. And what about some other ones that are uncooperative?

MR. WATERS. In Wyoming, we are actually having excellent support. I mean, Bresnan, AOL, they are all working very hard for us. So, that is the only one that comes to mind.

MS. DEGETTE. Anyone else have some particular offenders you want to identify? And if people would like to do this privately, we need to know, because we talk to these folks. Yeah, so if you could supplement the record on that, that would be swell.

Let me ask all of you, just one last question. We have over 2 minutes, so we have more than ample time for even what Mr. Bass was asking. What can be done to improve cooperation on these issues between law enforcement agencies? Let us start with you, Mr. Swecker.

MR. SWECKER. If you are talking about between law enforcement agencies.

MS. DEGETTE. Yes, sir.

MR. SWECKER. I think there is good cooperation as it is. We have the State task forces, the ICACs. They are very well networked. We have the National Center, which is sort of a clearinghouse, and makes many referrals to the State and Federal task forces. I would go out on a



limb, and say this is really a bright spot in law enforcement, in that I don't think they are out there stepping on each other, and then, when they do, I think there is a recognition we need to come together and work them jointly.

MS. DEGETTE. Mr. Plitt.

MR. PLITT. Yeah, I think all the agencies certainly represented here work together, and I think that you also see that over the past several years, they have blossomed in their application of the resources that focus on this problem. It is almost time, perhaps, to think about some areas of specialization.

ICE, for instance, tries to specialize in the trans-border area. The reason we do that is to effectively apply the limited resources that we have. Just a thought.

MR. SWECKER. May I back up for one second?

MS. DEGETTE. Yes, sir.

MR. SWECKER. One of the chokepoints is forensic examinations, and I would venture to say that each State ought to have at least a statewide forensic lab, if not regional labs, and because that is an area where you get a pretty good backlog.

MS. DEGETTE. What about prosecutions?

MR. SWECKER. Well, you can't get a prosecution until you get that evidence--

MS. DEGETTE. Right.

MR. SWECKER. --out of the computer, the ISP. Right.

MS. DEGETTE. So, that is part of--yeah. Okay. Dr. Kardasz.

MR. KARDASZ. I am very happy with the interagency cooperation I have had with all my law enforcement brothers and sisters. I can't throw anybody under the bus on that.

MS. DEGETTE. Mr. Waters.

MR. WATERS. We have had excellent support. It is coordinated through our United States Attorney's Office, and we don't have any issue with folks not coming to the table.

MS. DEGETTE. Mr. Clark is nodding in agreement, it looks like.

MR. CLARK. That is right. I am in agreement with Mr. Plitt, basically, on his answer.

MS. DEGETTE. Mr. Kezer.

MR. KEZER. I would have to concur. The investigation of these cases is a specialized field, and quite honestly, most of the investigators know each other, or are familiar. They go to training together. We couldn't get the work done unless we were cooperating. So I would concur. It is very good.

MS. DEGETTE. And Mr. Smith, do you agree?

MR. SMITH. I do agree, because we all bring, as a unique agency, each of us are different. We all have different jurisdiction and different authorities. We all bring something different to the table, and we all take different investigative approaches to identify the bad guys.

MS. DEGETTE. So, what it really sounds like to me, then, is the bottlenecks are the forensic labs, the numbers of investigators we have, and bottlenecks with the ISPs getting information to you in a timely fashion, so you can investigate and find these perpetrators.

Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you, Ms. DeGette, and at this time, we recognize Ms. Blackburn for 10 minutes.

MRS. BLACKBURN. Thank you, Mr. Chairman. And thank you all for your patience, for being here with us today, and for caring so deeply about the issue. It is evident that you all care about your work deeply.

Mr. Waters and Dr. Kardasz, each of you mentioned the activity, talked a little bit about it by country, and I think Mr. Waters, your testimony, you give by country what you have identified, and of course, we see the transactions for the U.S. as a much higher number than Germany, Canada, or the UK.

MR. WATERS. That is correct, ma'am.

MRS. BLACKBURN. Okay. Now, I would like to get inside that number just a little bit, and then, I think it maybe was Mr. Clark, with your testimony, you talked about ICE has successfully arrested more than 7,500 child predators. Of these, 6,600 or 88 percent of the arrestees have been non-U.S. citizens, and more than 59 percent of those have been deported from the U.S.

So, my question to you is this. Why the U.S.? Are we a magnet for this? Is there something that we are doing, or not doing, that would be pulling people that are not citizens here, and finding them involved in this activity, the number of websites is there--you want to get inside those numbers a little bit for me, either of you?

MR. CLARK. First of all, the numbers are in terms of the removals. That brings in our immigration capabilities to the fore. It is not our Internet investigations, per se, but it is resident aliens who have been here, would otherwise be legal, but have committed child exploitation crimes, which makes them an illegal, and it allows us to remove them from the United States. So, that is part of those statistics there.

In terms of the U.S. versus elsewhere, I would say one is probably greater Internet capability, more common in the United States than elsewhere. I would say probably greater recognition in the United States, law enforcement and the public, and greater use of the Internet. But again, in my earlier statement, I do think that the international community is rapidly growing aware of the issue, and I would refer to

the Australian government, in terms of following the Falcon arrests in that country, looking to see what they can do, in terms of their laws and regulations, in terms of child exploitation. So, I think it is probably just something we have paid more attention to, have more capability of looking at, unfortunately, bad people have more access to and can use. But I don't think this is a cultural or a U.S. problem at all. I think it is a global problem.

MRS. BLACKBURN. Okay. Mr. Waters, anything to add to that?

MR. WATERS. I would add the numbers that I represented are from an operation where we identified primarily movies, large movies, and they tend to traffic more over high speed Internet connectivity, and so, a high saturation of broadband Internet leads to more individuals being able to participate in that trafficking. But we have clearly identified a large number globally, and we have trained Interpol in how to use it, and they are now actively searching as well.

MRS. BLACKBURN. Okay. Mr. Clark, I wanted to come back to you. Tell me why 3,900 of the 6,600 non-U.S. citizens who were arrested were deported instead of prosecuted.

MR. CLARK. I am not certain I would say they weren't prosecuted. I would have to--I am not certain the numbers, 3,900. What would often happen is, in some cases, they have been prosecuted and released. We have gone back out, and taken them administratively, and removed them, based upon the fact that their resident status or legal status, under the immigration authority, is no longer there, so there might have been prior criminal arrests and sentences served.

MRS. BLACKBURN. Okay. If you would, then, look back at that number one more time in your testimony, and then, kind of clarify that for us, I think that would be great. I would appreciate that.

Let us see, Mr. Waters, in your testimony, you talked about a situation where an agent witnessed the rape of a child taking place. I think that is your testimony, and what I want to ask you is, when you get information that there is something taking place, how often do you get that quickly enough to go in and act, and how often have you been able to remove children from those situations when you get the information timely?

MR. WATERS. I think a two-part answer there. We typically react just as fast as possible. We have had several cases where, because--

MRS. BLACKBURN. Well, is that hours, days?

MR. WATERS. Sometimes, it is hours.

MRS. BLACKBURN. Hours.

MR. WATERS. I have had cases where I have gotten on a plane and flown to Houston that day, and--

MRS. BLACKBURN. Okay.

MR. WATERS. And worked the case. We have had several where we respond immediately. Depending on the type of material that we are receiving, sometimes, the circumstances dictate that we wait until we get a response from a service provider, to tell us where this person is at. Sometimes, we have to wait to get records from there, trying to, to give us a physical address. So, occasionally, we are restrained by the logistics of the companies to tell us where these offenders are. But we typically get on them as fast as possible.

MRS. BLACKBURN. Any idea of the actual number of children that you all have pulled out and removed?

MR. WATERS. I can speak just to the last couple of months. Maybe the last 6 months, we have had two out of Wyoming, we are a fairly small State. In our operation, we have had quite a few around the country. We just had one, one of these peer-to-peer cases led to an offender in San Diego who was working in a hospital, and was actively molesting four to five kids a week, coming into these wards, a respiratory therapist. And in that case, they were able to take him out of a situation where, of the 50 kids on the ward, quite a few of these he was being able to molest.

MRS. BLACKBURN. So, if the ISP providers, if they are going to give you the information, that is going to help you to respond quickly.

MR. WATERS. Absolutely.

MRS. BLACKBURN. What I am hearing is, as Ms. DeGette was saying, many times that is your bottleneck.

MR. WATERS. That is correct.

MRS. BLACKBURN. That is what slows you up.

MR. WATERS. Yes, ma'am.

MRS. BLACKBURN. Okay. Now, out of the ones that you have been able to respond quickly to over the past couple of months, what number were you hampered from responding in a timely--could you have gotten in there and done your work?

MR. WATERS. Well, it is difficult to say.

MRS. BLACKBURN. Okay.

MR. WATERS. I would have to draw a conclusion based on information I didn't get, so I don't know how many of the records that failed to come back would have led us to a child in danger. But one is far too many.

MRS. BLACKBURN. Okay. In talking about your work with other agencies, are all of you satisfied with the interaction that you are getting from the Department of Justice?

MR. WATERS. If I can speak to that, we are very satisfied with the support that we are getting. In Wyoming, the United States Attorneys call our office to see if we have any cases we need help with. If they

don't hear from us in a week or two, we get a call, and they want to know how we are doing.

MRS. BLACKBURN. Okay.

MR. KARDASZ. May I respond to that?

MRS. BLACKBURN. Yes, you may.

MR. KARDASZ. The OJJDP grants that we work under are very helpful, and the coordination that is done at the administrative level of the OJJDP really helps us locals to put our programs together, and then work with all the other Federal agencies.

MRS. BLACKBURN. Okay. All right. And I think, Mr. Chairman, I will yield back.

MR. WHITFIELD. Thank you, Mrs. Blackburn, and at this time, I will recognize Mr. Inslee for 10 minutes.

MR. INSLEE. Thank you. Mr. Waters, you mentioned something like 1.9 million images through the peer-to-peer system, and did that, at least in your first review, did each one of those cases, at least on a prima facie basis, could constitute a crime in and of itself, the retention of, receipt of those images?

MR. WATERS. Yes, sir.

MR. INSLEE. So, we had 1.9 million potential crimes. How many of those have been prosecuted?

MR. WATERS. I don't know nationally how many. I can speak to those that have reported back to me. I know they did a sweep of about 40 in New Jersey, they did 70 in North Carolina. We have done 40 or 45 in Wyoming. I only know the ones that get back to me, and let me know how it has gone.

MR. INSLEE. So, that is about 165 out of 1.9 million. The 1.9 million may not be separate individuals. There might be multiple same people.

MR. WATERS. Yes. That is correct.

MR. INSLEE. So, let us cut it in half, and say 800,000. So, out of the, say, 800,000, we have had 165 prosecutions, and my constituents are going to ask the obvious question, so I will ask it. Why so little with that enormous floodtide? Is it a resource issue, and if so, could you describe how we could help you in that regard?

MR. WATERS. Well, it is absolutely a resource issue. We are hitting them as fast and as hard as we can. One of the biggest things that we run into, again, are delays or lack of records. So we have an IP address. We can identify that there is an offense, but we may not be able to identify an offender. But by sheer numbers, it is just, we have more than I have the man-hours to send guys out on.

MR. INSLEE. What could you usefully use, as far as increased resources, what could you efficiently use to pursue these 1.9 million

incidents, do you think? A doubling, a tripling of your resources? What do you think?

MR. WATERS. Well, I think a tripling, we would still be falling behind. As it stands right now, I am bringing in about six, seven new leads in Wyoming a week. We are currently able to hit one search warrant every week or every 2 weeks, so even if we triple, we are still falling behind, as we are finding these leads.

MR. INSLEE. So, I have this sense that if there were oh, bank robberies where you had 1.9 million bank robberies, but only 165 prosecutions, there would be a very large hue and cry to solve this problem, and that we would have resources to you to get that done. Do you kind of share that view? I get this sense that somehow, this has not received the priority that at least I think most of us here would believe that it should. Do you have any sense of that?

MR. WATERS. I share that view, and I thank you for drawing attention to that, because we have been yelling at every rooftop we can get on.

MR. INSLEE. So, let me ask some of the Federal personnel here, start with Mr. Swecker, for instance. I have a sense, I think you testified there was a 2,050 percent increase in images in one of these databases in the last 10 years. What increase in resources would you estimate there has been, if any, in the last 10 years, to this problem Federally from Federal agencies, all told, or at least from yours?

MR. SWECKER. Well, we went from zero to 250. We actually have-- that is a little lesser number than we had over the last couple of years, because we, truthfully, have had to divert some over to terrorism. But we had to borrow those 250, or reprogram those 250 from our Criminal Division. So, where all that goes, to say that there is always room for more resources, I agree. We could put a thousand FBI agents, and thousands more officers on it, and we wouldn't put a dent in that number that you just gave.

MR. INSLEE. And what does this year's budget do to help in that regard? Do you have any idea?

MR. SWECKER. We have no enhancements for this--well, we got 22, I think we got 12 agents and ten analysts. We got 22 positions.

MR. INSLEE. So, in the current budget, passed by this Congress, we have 1.9 million potential crimes, and we have got no increase in resources to deal with that, even though we could, at least in one agency, triple it, and use it efficiently. That is a fair statement.

MR. SWECKER. We have zero enhancements for '07.

MR. INSLEE. Okay. I may note, that is not your gentlemen's responsibility. It is ours at this table, just so the responsibility is in the right location here.

MR. SWECKER. I would also go back to the forensic laboratories, too, because I think those are critical.

MR. INSLEE. Mr. Waters, in the peer-to-peer situation, does the problem with ISP records exist in that context, or is that a different situation?

MR. WATERS. It exists very much in that context. In fact, it is most exaggerated, I think, in the context where we are reliant on the IP address to find the offender.

MR. INSLEE. Okay. I want to ask you about foreign prosecutions, where there is a person outside the United States, when they are sitting at a computer that is involved in this, what is our situation? The father of a victim who testified here last week was apparently, asserted was involved while in Mexico. What options exist for us, what handicaps do we have in that kind of context? And I will ask that to anyone in the panel who wants to take that on.

MR. PLITT. ICE was in that situation very frequently. We do have some remedies. We have quite a few countries that are, for lack of a better term, waking up, strengthening their laws, if they have older ones, they are adding laws, if they don't have it. I think that in the next few days, a report will be released, out of NCMEC, I think, that will indicate that--and it will surprise the panel here--few countries actually have child exploitation laws on the books already, very few. Nevertheless, the governments that we work with, they want to help us in these cases as much as they can. They are concerned about children, of course. They are also concerned about their national reputations, and quite frequently, we will have the law enforcement agencies from those countries work to get us the evidence that we need, and in some cases, extradite.

MR. INSLEE. But is your understanding that we--I mean, do we have jurisdiction in a case where a person is sitting in Mexico, and is abusing through the Internet inciting, exploiting a child, do we not have criminal jurisdiction to assert to extradite that person, assuming that we have the resources to do it, and the case to do it?

MR. PLITT. Assuming we have the resources, yes, we would. A very good example is the child sex tourism cases, where an individual is traveling out of the country to have sex with a child. If that individual is a U.S. citizen, that individual, upon return, or still in the country where the act occurred, is subject to U.S. prosecution.

MR. INSLEE. Given the assertions by Mr. Berry, it is hard for us to understand, given that, why there hasn't been a prosecution, in Mr. Berry's case, of this individual who was in Mexico, allegedly exploiting him, I am having--understand who is his father, so it is not an identification issue. What possible reason for there not for, that to be at least started on the prosecutorial trail?

MR. PLITT. I don't know. Again, that case wasn't brought before ICE. ICE had a linkage to it, simply because it had arrested another individual that had dealt with Berry, and then that was moved to another agency, I believe the FBI.

MR. INSLEE. Mr. Swecker, do you have any insights on that, on what possible reason there would be for not pursuing that?

MR. SWECKER. Well, let me just resort to talking generically about the international investigations. It is really hit or miss on an international level. Eastern Europe is a problem, mainly from a training aspect, and the aspect of not necessarily having the laws to address it, and there is a need for some international training in this area. There is a need for some strengthening of the laws in these areas, and then, they will not render their own citizens. As a general rule, they won't render their own citizens back to the U.S.

MR. INSLEE. Well, let me just sort of interrupt you a second. I have only got a little bit of time, but if you have got an American citizen in Mexico, who is clearly identified as the father of the victim, who has these assertions, under American law, using American resources, using American tools, if you will, why could we not pursue that without necessarily depending on the investigatory resources of Mexico?

MR. SWECKER. We could, if there were charges filed, there is--you have to have charges filed. You can put a Red Notice out through Interpol.

MR. INSLEE. And I yield to Ms. DeGette.

MS. DEGETTE. Thank you. Well, from what we understand, the Department of Justice refused to take jurisdiction on the case. Is that correct, Mr. Swecker?

MR. SWECKER. I have pretty strict instructions not to discuss that case.

MS. DEGETTE. Mr. Plitt.

MR. PLITT. Don't know. We are not--

MS. DEGETTE. Well, but jurisdiction has been declined. Why can't you discuss it? It is not a case under investigation or prosecution.

MR. SWECKER. Well, there is always the potential for prosecution in that case.

MS. DEGETTE. Who would know? When we bring the Attorney General in, will he know?

MR. SWECKER. I would defer to main Justice.

MR. STUPAK. Well, Mr. Berry is here in this room. Can any of you give him any reassurance that someone is honestly looking at his case? It has been 7 months, 1,500 names, websites, credit cards, everything he provided you guys.

MS. DEGETTE. Testimony.



MR. STUPAK. Testimony.

MR. SWECKER. This case is being aggressively investigated.

MR. STUPAK. That doesn't do anything for Mr. Berry or for any of us up here.

MR. SWECKER. I would defer to them, as to whether they are satisfied.

MR. INSLEE. I just want to speak. I am a former prosecutor, and feel very strongly about the integrity and success of prosecutorial efforts, and this has been a huge black eye for the country, and a lot of doubt created, so I think all of us have an obligation to get with the task at hand. Part of that includes cooperating with this panel, which I hope you will spread that message, to the extent you can convince people, to figure out how to solve these problems. I think that is very important.

My time is up. Thank you.

MR. WHITFIELD. Thank you, Mr. Inslee. At this time, we recognize the Chairman of the full committee, Mr. Barton.

CHAIRMAN BARTON. Thank you, Mr. Chairman.

I don't think I am going to take 10 minutes. And if this ground has been plowed while I was gone, I apologize, but Mr. Swecker, where are you in the chain of command at the FBI?

MR. SWECKER. I am the Acting Executive Assistant Director for Law Enforcement Services, which puts me directly over both Cyber and Criminal Divisions, directly in the chain of command on these violations.

CHAIRMAN BARTON. And who do you report to?

MR. SWECKER. I report to the Deputy Director.

CHAIRMAN BARTON. Who reports to?

MR. SWECKER. To the Director.

CHAIRMAN BARTON. Director. So, you are third down from the Director, and you are in the operational chain of command. You are not a staff assistant.

MR. SWECKER. I am directly accountable for anything, all things cyber.

CHAIRMAN BARTON. Okay. Does the name, and if I am mispronounce it, I apologize, Raul Roldan mean anything to you?

MR. SWECKER. Raul Roldan is one of our section chiefs.

CHAIRMAN BARTON. And he reports to you?

MR. SWECKER. He reports to a Deputy Assistant Director, who reports to an Assistant Director, who reports to me.

CHAIRMAN BARTON. So, he is three down from you?

MR. SWECKER. Yes.

CHAIRMAN BARTON. Now, why could he appear on CNN today, but he couldn't appear before this subcommittee?

MR. SWECKER. Well, I wasn't involved in that decision, but my understanding is that he did not comment on this investigation whatsoever. He was talking generically about crimes against children on the Internet.

CHAIRMAN BARTON. I didn't ask that question. My question is, we specifically asked for him. We are not upset that we have you. You are at least a line officer, which is an upgrade from the main Justice Department, but the specific person that we asked for, they flatly refused to have him testify.

I want to know why.

MR. SWECKER. I think there was concern that he would end up commenting on this case, and there were strict instructions not to comment on this case.

CHAIRMAN BARTON. Well, I want you to tell the Director, because I am going to tell him or ask him, if this gentleman doesn't testify voluntarily, he will testify under subpoena.

MR. SWECKER. Yes, sir. I will pass that on.

CHAIRMAN BARTON. And I mean, that is not a threat, that is a fact. So--

MR. SWECKER. I understand.

CHAIRMAN BARTON. I am fed up with being told by my friends, we have a taped message on the cell phone, or one of our committees, that the Justice Department wasn't going to testify, period. We are going to change that. And I thank you for coming. I do have some general questions.

For my first question, and I don't know if I direct it to you, or our postal people, are the laws for transmission of Internet child pornography the same as transmission of pornography, child pornography through the mail? Is it the same law?

MR. SMITH. There is a number of statutes, but it is primarily the same one, 18 USC § 2252, that is our bread and butter statute that we charge probably in 90 percent of the cases. That involves the unlawful receipt or distribution of any child abuse images, child pornography, that travels interstate, foreign commerce, over computers or via mail.

CHAIRMAN BARTON. But it is basically the same.

MR. SMITH. Same statute covers them all.

CHAIRMAN BARTON. Do we need a special statute specifically for child pornography on the Internet, as opposed to through the physical mail? Would that be helpful, or is that unnecessary?

MR. SMITH. No. I think we have adequate legislation there.

CHAIRMAN BARTON. Okay. Is it illegal for an adult in the United States to possess child pornography, the possession is illegal in itself? Okay. Mr. Waters, who is one of our undercover agents here, in order to

prosecute a case, and I am talking generically, do you have to watch a perpetrator commit an act over the Internet as an eyewitness, or do you have to just have knowledge of it, from the child who was abused in the act?

MR. WATERS. We do not typically have to watch it.

CHAIRMAN BARTON. You don't.

MR. WATERS. No, sir.

CHAIRMAN BARTON. So, what is the burden of proof? What is the standard of proof to prosecute?

MR. WATERS. Well, depending on the type of act, we still have the same burden to prove beyond a reasonable doubt what occurred, but frequently, we get this information from the victims that were involved, from the forensic analysis of the computer. Some of these individuals even turn on their own webcam and film themselves while they are committing the crime. So, usually, it is a combination of testimonial and physical evidence that allows us to overcome that burden.

CHAIRMAN BARTON. And do you agree or disagree that we don't need any strengthening of the laws in this area?

MR. WATERS. I don't know of any strengthening of the laws, federally, that--

CHAIRMAN BARTON. You don't think it is necessary.

MR. WATERS. I believe we have adequate legislation.

CHAIRMAN BARTON. Okay. Okay. Well, Mr. Clark testified that law enforcement can't do it alone, and I agree with that. We expect you folks to help us enforce it, but every one of us up here, I believe, is a parent, and in my case, a parent and a grandparent, and we have to be involved, too, and the community has to be involved. And I want to thank you, Mr. Waters, for your testimony, and some of the displays that you put up.

How did you get picked to be here, since you are from Wyoming, just out of curiosity?

MR. WATERS. I believe I got picked because I work on the technical side. I spent a few years as a systems programmer, and so, when the ICAC Task Force runs into a technical challenge, I co-chair the Technology Committee, so at the--

CHAIRMAN BARTON. Are you in Wyoming or here?

MR. WATERS. Cheyenne.

CHAIRMAN BARTON. So, you had to fly in from Wyoming to be here.

MR. WATERS. Yes, sir.

CHAIRMAN BARTON. Did anybody in the agency pressure you not to testify? Did you volunteer to testify? I mean, I am glad you were here, because you are very credible and very committed, but it is just odd we

can't get them to come from four blocks away, and yet, they can fly you in from Wyoming.

MR. WATERS. Well, no one pressured me not to testify. I am here because of the program and working with OJP, Office of Justice Programs. They helped fund a lot of the work that we are doing, and they asked, and I said I would be honored.

CHAIRMAN BARTON. Okay. And Mr. Swecker, I need to give you a chance to stand on your soapbox a little bit, since I have. Is there anything that the Congress is not doing, that we should be doing, to help the FBI prosecute these criminals?

MR. SWECKER. Well, we think we have the laws that we need. I think I would resort back to Mr. Stupak's point, or Congressman Stupak's point, about mandatory referrals. We probably need to get that going. In the banking industry, we know that it has been tremendously successful in getting suspicious banking transactions referred to us.

I would also, again, just beat the drum for the forensic laboratories, because again, that is a chokepoint when it comes to the forensic analysis. We have the laws, but we need the training. We need to export the training to the State and local level as a much faster pace, and get the resources out there to the State and local officers where they need it.

CHAIRMAN BARTON. I am not disputing what you just said, but I am confused a little bit. Child pornography is obvious. What is forensic about that? What kind of a laboratory do you need to dissect if you have a picture of a minor child engaged in a sexual act with an adult, that that is a crime?

MR. SWECKER. It is getting to the picture. It is pulling it out of the hard drive, or identifying the ISP, identifying the specific addresses, of which there would be thousands, and pulling all that information out of the computer. That is what we are calling a forensic analysis.

CHAIRMAN BARTON. I see. Okay. Thank you. Thank you, Mr. Chairman.

MR. WHITFIELD. Thank you. I do want to reiterate, you all did indicate, though, that it would be helpful if we had the mandatory data storage for a period of time, and that, as you said, to clarify, the Internet service provider providing the tip to the Cyber TipLine, though those are two areas that we definitely could do something about within our jurisdiction.

MS. DEGETTE. Mr. Chairman, also responding to the subpoenas within--

MR. WHITFIELD. And responding to the subpoenas. At this time, we recognize Mr. Walden for 10 minutes.

MR. WALDEN. Thank you, Mr. Chairman, and I want to follow up a bit on the Chairman's comments.

As I understand it, under 42 USC § 13032, ISPs are required to report all child pornography images to NCMEC, correct? Isn't that-- whoever is the certified expert here? I want to clarify that the position of law enforcement here, that you would like all ISPs to have to both register and report in known child pornography, to the Cyber Hotline, and it is my understanding there are only like 215 ISPs that are registered, and there must be thousands out there. Can any of you, or whoever feels comfortable, comment about that, and what progress needs to be made there, and what we could do to help along those lines? Okay. Somebody must have an answer here. There are only 215 registered, there are thousands out there. What enforcement capability do you have?

MR. SMITH. The largest ISPs, I believe, are in compliance, from what I have learned in my conversations with Ernie Allen and John Rabin over at the National Center, but there are many, many smaller ISPs that either aren't aware of the law, or they are ignoring the law, whatever the case may be.

MR. WALDEN. All right. Thank you. Mr. Swecker, you are in charge of all things cyber, you said. This must fall under your jurisdiction.

MR. SWECKER. It does. I think there is some confusion on the part of the industry as to the content of what they are supposed to refer.

MR. WALDEN. Okay.

MR. SWECKER. They are looking for a safe harbor, I think, that immunizes them against lawsuits for making the referral, plus I don't think they know whether they are able to send the images across.

MR. WALDEN. Sure.

MR. SWECKER. So, I think there needs to be some more specific--

MR. WALDEN. Who comes up--you said, I think, that you don't really need any new laws to work in this area, so whose responsibility is it to clarify this? Do you need clarifying language from the Congress? Do you issue directives and rulemakings?

MR. SWECKER. That goes to the Legislative Affairs Offices of both Justice and the FBI, and I think they could, we could give you some more details on that.

MR. WALDEN. That would be helpful, because it just strikes me, if we have got the law in place, and you say it is, it is really functionally useless if it is not being enforced because there is confusion. And I know you all have your hands full, clearly, and probably literally, in some of these areas, and so, I guess the question is what do we do to help, and how do we get it clarified? If ISPs don't know they are supposed to register, there should be a mechanism set up to help on that, and then, to clarify this issue. Because I know we had testimony from the gentleman from the New York Times that he had to work with an

attorney, be very careful as he did his investigation, not to run afoul of the law by going to a site clicking the wrong time runs you afoul of the law.

And Mr. Swecker, I want to go to you, because you work in this area. Tell me just generically, if you have a child victim of pornography, and some predator has abused some child, and it is going on, what sort of knowledge do you need as a prosecutor?

MR. SWECKER. To elicit the evidence from the victim, or--

MR. WALDEN. To elicit the evidence from the victim, to pursue the case, how urgently do you get involved?

MR. SWECKER. It is very urgent. These have to be handled with a lot of care. Victim/witness specialists need to get involved very early on. Child interview specialists need to get involved. We need to find the website. We need to find the person that is actually abusing the child, and so that is what we are trying to elicit from the child.

MR. WALDEN. And so, you would bring the child in immediately, I would assume. You would interview them. You would set up--if they came in and said not only has this just happened to me, I know it is going on to somebody else at this moment. Tell me how the FBI responds.

MR. SWECKER. We need to get as much information as we can out of the child, as to the identity and the location of the person that is doing the abuse.

MR. WALDEN. And so, once you do that, let us say you get IP addresses, then do you turn that over to some sector within the FBI?

MR. SWECKER. Well, the first step is to get the website, you work on the Internet addresses that are accessing the website. Our focus really is on the abusers before we go to the customers. It is on the website administrators. It is on the financiers. To draw an analogy, would be we don't necessarily go after the drug users. We immediately go after the abusers. Those would be analogous to a distributor.

MR. WALDEN. Okay. All right.

MR. SWECKER. The person who is actually producing the pornographic material. That means a child is being abused. That is where you want to go first. Find the person who is actually abusing.

MR. WALDEN. And if you know of an abuse, if you are told there is an abuse going on. We have heard some testimony here and elsewhere, that literally, some of these perpetrators use the camera on themselves, in real time, you could watch on the Internet, abuse going on. Tell me what the FBI does, or the Department of Justice does, if I walked in today, and said I just was flipping through the Internet, and came across this. Here is the address. It is happening as we speak.

MR. SWECKER. Well, in that instance, I mean, I don't know if we could move quickly enough to get them while they were in the act. I

mean, that has happened on occasion. You have been lucky enough, or you have been able to set up a situation where somebody was actually on the website, and actually either accessing or producing that type of material.

MR. WALDEN. But if a child presented himself or herself to one of your officers, if I came to you and said I just came from the credit union, and there is a guy with a gun in there in the face of the teller, tell me what happens.

MR. SWECKER. Well, we could, as quickly as we could, we would intervene.

MR. WALDEN. If I come to you today, and say on the Internet right now, at this address, this is going on. Tell me what happens.

MR. SWECKER. Probably the quickest way to get to it is to pose undercover, and try to attempt to get access while that person is on, and that may be one of the quickest ways, when you have a proactive situation like that, to get very quickly to the person.

MR. WALDEN. You are going to move proactively.

MR. SWECKER. Right.

MR. WALDEN. Right away, even if it means sacrificing evidence, I would assume.

MR. SWECKER. You still have to find the location where they are doing this from.

MR. WALDEN. Sure.

MR. SWECKER. It could be a library. It could be an Internet cafe.

MR. WALDEN. Let us say the child presents herself, and says here is the IP address. This is the same person that molested me. Here is the name. Here is the address. It is going on now.

MR. SWECKER. We would attempt to get a search warrant, and go out at that real time. And I will defer to these other investigators, who are actually on the street, to respond as well.

MR. WALDEN. If you knew Bad Santa was operating in the mall.

MR. WATERS. I am going into his living room. If he is at home, and it is active.

MR. WALDEN. You are going right now, aren't you?

MR. WATERS. I am going right now. I am calling the ISP, finding out where it is at, and we are going to be in the door.

MR. WALDEN. All right.

MR. WATERS. If we are not close enough, we will get ahold of the local PD, and they will be in the door.

MR. WALDEN. So, does that happen in a matter of weeks, days, hours, minutes?

MR. WATERS. It varies based on the case.

MR. WALDEN. Sure.

MR. WATERS. But if I have credible information right then, I have had cases where I call the ISP, and they give me an answer now.

MR. WALDEN. Is that right?

MR. WATERS. We get an answer, there is an emergency clause that allows us to get that, and we go.

MR. WALDEN. And you go. Okay. Let me go to the issue of affidavits. Unlike some of my colleagues, I am neither an attorney nor have I ever been a prosecutor. And usually, in my town meetings, when I say I am not an attorney, there is a little ripple of applause. No offense to attorneys.

Explain to me on affidavits in criminal cases, circumstances where victims' names are released. Explain for me affidavits, they get unsealed, victim's names are put out in the public. Is that sort of normal operation? The court says keep this sealed, and then, it becomes unsealed.

MR. SWECKER. Well, affidavits in this type of case are often sealed, but they can't stay sealed forever. Eventually, particularly when you start the judicial process.

MR. WALDEN. You have a right to--

MR. SWECKER. They have a right to confront the witness against them.

MR. WALDEN. Sure.

MR. SWECKER. And at some point, the affidavit is unsealed. I mean, you can get a search warrant on confidential information, to protect the identity. You don't necessarily have to name the person. It depends on how much corroboration you have.

MR. WALDEN. If an affidavit is accidentally unsealed, which I assume occurs from time to time, clerical error, and the victim tries to get it, and asks for it to be sealed again, what obligation does the Government have to ensure that that victim's identity or whatever, if it is allowed to be resealed, that the affidavit gets resealed?

MR. SWECKER. I know what you are referring to, and I am trying--I will try to answer your question without getting into--

MR. WALDEN. You are trying to dodge it. I understand that. I haven't named names.

MR. SWECKER. --specific facts. But the first step would be to notify the person, and offer protection. That would be the first investigative step. The rest of it would be up to a prosecutor to resealed the affidavit.

MR. WALDEN. What should--if it is supposed to be resealed, what sort of timeline should a victim anticipate for that resealed to occur?

MR. SWECKER. I would have to defer to the prosecutors on that, as to what a reasonable time--



MR. WALDEN. Who is a prosecutor here who has ever been through one of these? Have you ever, sir, from the great State of Wyoming? You are an investigator.

MR. WATERS. Strictly an investigator.

MR. WALDEN. Have you ever heard of this sort of circumstance?

MR. WATERS. We work in a different model. We don't typically put victims' names in our affidavits.

MR. WALDEN. Really?

MR. WHITFIELD. This is when we should have Mr. Mercer back. We released him this morning, but he is the U.S. Attorney for Montana.

MR. WALDEN. Yeah, but--well, Wyoming is near Montana. Which is are we getting closer to Washington? I don't know. One final question, if I might, Mr. Chairman.

There has some concern been expressed about extraterritorial application of the law, because in some cases, some of this child pornography is actually being put on the Internet in a foreign country, but it is received in this country because of the global nature of the Internet. Is that an area where the law needs to be changed, or can be changed? Is that an area that precludes your ability to engage in enforcement? Let us say if somebody were in, oh, Canada, or maybe Mexico, and transmitting this sort of pornography. Can you go after it?

MR. CLARK. I would say our laws are satisfactory. Oftentimes, the foreign laws aren't as satisfactory, but we do have relatively good cooperation on a number of fronts with foreign governments, as far as working those types of cases.

MR. WALDEN. One final question. Digital currency, this is sort of new to me. Can you explain? I understand that is sort of the new underground way to engage in payments without fingerprints, if you will. Digital currency. Is this an area we need to explore more?

MR. PLITT. Yes, it probably is. Digital currency is simply the situation where an individual put money on the Internet. You can do that through any brick and mortar location. I will give you an example in a second, but when the money is put on the Internet account, then the money can be used on the Internet to buy access to legitimate sites, to child exploitation sites, to buy items off of the Internet, regular merchandise. It can also be taken off the Internet through another brick and mortar location somewhere else in the world. Currently, it is not regulated. A simple example I would give is that we had one investigation where memberships were being purchased with e-currency, and a lot of the e-currency documents, if you will, were charged with money in Australia.

MR. WALDEN. Okay.

MR. PLITT. To the tune of approximately \$30 million a year.

MR. WALDEN. So this could get completely around the Bank Secrecy, or whatever those--what is the law they have to follow in a bank?

MR. PLITT. Bank Secrecy Act.

MR. WALDEN. Yeah, if \$10,000 in cash or more. So you just do it in a foreign country, put it in, pull it out somewhere else.

MR. PLITT. Yes, and to date, though, the services, the companies that provide the service, have been very, very cooperative with us to track that, yeah.

MR. WALDEN. All right. Well, if you have specific suggestions in this area, I would certainly like to work with you on it.

MR. PLITT. Very good. If I could, one other response.

MR. WALDEN. Sure.

MR. PLITT. Since I have the mic. You were asking about victim/witness issues. One to keep in mind is one that is very, very complex, and that is the child sex tourism cases, where the individual was traveling to another country to have sex with a child. The logistics of bringing the child back, if necessary to testify, parents, guardians, et cetera, is one that is coming up in these cases. Just another comment.

MR. WHITFIELD. Thank you, Mr. Walden.

I think Mr. Walden's line of questioning encapsulates the concerns of many members of this committee about the investigation we heard the testimony of on Tuesday, and that is why we do want to pursue further meetings with Justice, maybe in executive session, because I heard you speaking, Mr. Swecker, of victim/witness specialists, and I am assuming that that is a person who assists the victim, and in the testimony of our hearing on Tuesday, in our meetings with the victim, I never heard that any victim/witness specialist was assigned in that case. And then, we know that evidence was given of child victims, and they were being abused in a real time manner, and action was not taken, and so, we have walked away from these hearings quite puzzled, because it appears that in that instance, the victim of the crime was being treated more as a perpetrator of the crime, and so, I think that is really kind of underlying the sentiment of the committee, and that is something that we need to get into.

But I want to thank all of you for your testimony. We appreciate your efforts to continue to bring these perpetrators to justice, and with that, this panel is dismissed.

Now, at this time, we will call the third panel, which consists of one person, and that is Mr. Grier Weeks, who is the Executive Director of PROTECT, from Ashville, North Carolina.

Mr. Weeks, thank you very much for being with us, for your patience. As you know, this is an Oversight and Investigations hearing.

We take testimony under oath. Do you have any difficulty with testifying under oath? And I assume you do not need a lawyer with you. So, if you would stand, and raise your right hand.

[Witness sworn.]

MR. WHITFIELD. You are sworn in now, and you are recognized for 5 minutes for your opening statement. Turn your microphone on.

MR. WEEKS. Is that better?

MR. WHITFIELD. Yeah.

**STATEMENT OF GRIER WEEKS, EXECUTIVE DIRECTOR,  
NATIONAL ASSOCIATION TO PROTECT CHILDREN**

MR. WEEKS. Thank you. I am Grier Weeks, Executive Director of the National Association to Protect Children, also known as PROTECT. We are a national membership association dedicated to just one simple issue, which is child abuse, child protection. We have members now in 50 States and 10 countries.

One of the things we do the most is go around the country to various State houses, and work on State legislation. And one of the greatest problems we see is a spectacular national failure to take these issues seriously at the State level.

I will condense my remarks here, because I know you know at this point the nature of child pornography, and don't need that characterized again. I would say that as you go back out among your colleagues, and hear this material referred to as kiddy porn, or trivialized in that way, you will be reminded of what we are up against.

Two years ago, law enforcement agents in my home State of North Carolina, arrested a criminal, Brian Schellenberger, who was convicted of producing child pornography, and distributing the images over the Internet. Photos showed a 6-year-old girl was kept in a cage, beaten, sexually tortured, and urinated and defecated on. The criminal penalty for being an accomplice to that crime, for possessing those images in North Carolina, is a felony, is the exact same felony penalty you would get for operating a bingo game without a license or cockfighting. In California, the penalty is a misdemeanor, distributing it to others is a misdemeanor, using a child to distribute it to others is a misdemeanor. And under California law, even manufacturing such a despicable product is a minor felony with no minimum prison sentence. In Colorado, Oregon, North Dakota, possession of these brutal images of children being raped and humiliated is a misdemeanor. In Iowa, it is an aggravated misdemeanor, the equivalent of livestock abuse. If you compare the risk/gain ratio for trafficking in a product like this, to the risk/gain ratio for those who traffic in cocaine, you will instantly

understand why our national weakness on this issue has attracted so many new predators.

Nationwide, an estimated 96 percent of those arrested for child pornography possession are convicted, but fewer than 60 percent are ever incarcerated. Of those convicted solely of child pornography possession, fewer than one in three serves more than a year in jail. This is despite the fact that child pornography, like narcotics, is illegal contraband in and of itself, and easily prosecutable. Let me just add that in the State of Wisconsin, a WITI investigative reporter did a painstaking investigation of how child pornography possession cases were handled in his State, searched every single one of them down, and found that 75 percent of the perpetrators did no time in prison whatsoever.

PROTECT's first point is this. Unless and until the States are made to treat "simple possession" of child pornography as the egregious felony it is, and unless the funding is made available to aggressively investigate and prosecute possession of child pornography, Federal efforts will be hopelessly diluted. Let me give you some examples.

Instead of Federal resources being a multiplier of State efforts, as you would hope they would be, the lack of appropriate legislation and resources is actually discouraging the States from prosecuting these cases. Until States get serious, U.S. prosecutors will continue to pick up the slack for local prosecutors, who have grown dependent upon the Federal government to prosecute their criminals for them. I think all of the prosecutors you talk to will attest to that.

Internet Crimes Against Children Task Forces, the ICACs you have heard so much about, will continue to provide training and technical assistance to frontline law enforcement agents who are so unsupported by their own States that they often have backlogs of hard drives waiting to be analyzed, many of them containing evidence that could save a child immediately.

And the mass, and this is the most important issue here, the mass of domestic criminal conspirators who create and feed the insatiable demand that you have heard about will remain at large as limited Federal resources are triaged and focused on chasing after the major cases of commercial manufacturers and distributors.

PROTECT's second point is that the Federal government also must get serious. We are losing this war, and I don't think we have heard that enough today. We are drowning. I think it is obvious to everybody that was here that we are not supporting our troops on the frontlines. Recent estimates of the size of the exploding global criminal market in child pornography are in the multibillion-dollar range. You have heard \$20 billion numerous times. Yet, there really is no objective measure whereby we can say we are serious about this.

The FBI's Innocent Images National Initiative is funded at a level of about \$10 million a year. That is chump change. By comparison, HUD recently announced it was awarding more than that to build 86 new elderly apartment units in Connecticut. It is a wonderful thing, but this is to put it in perspective. They spent almost seven times the Innocent Images budget just on homelessness in Ohio. The Administration has proposed 20 times the entire Innocent Images budget for abstinence-only education programs. Another example, the Department of Justice's Internet Crimes Against Children Task Force program received about \$14.5 million in FY 2006. That is less than one-fifth the amount proposed for the new initiative to help prisoners reintegrate into society. Last year's budget included \$211 million for the Department of Interior to do high priority brush removal. That is compared to \$14.5 million.

The law enforcement officers that came here today, and that come here every year, to testify on this issue, can't get up here and tell you that. You heard one say he wouldn't, if he had his budget tripled, he would still be behind. But I honestly don't know how we can look him in the eyes, asking them to do probably the most unthinkable job on the planet, and this is what we put into it.

The radical increase in child pornography we see today is the direct result of failing to match our rhetoric about children with the resources needed to fight this war, and we will hear a lot of rhetoric this month. It is Child Abuse Prevention Month. Our third and final point is simply that you heard a lot of experts with a lot of expertise, and I think that after these hearings, they would be very eager to give you very specific policy proposals, hopefully more than you have heard today. But the expertise, really, that is needed here, is your expertise, and I mean that in a meaningful way. It is your expertise that is needed. How do we make this an urgent, serious issue, because nobody else you have heard from knows how to do that.

Finally, I would like to just address a few loose ends that I heard mentioned, and I knew you were looking for policy proposals, and I would like to address a few of them. On the issue of Federal penalties, the Federal penalty for possession of child pornography is a minimum of a fine. So, I do think there is a problem there. The issue is not what is the maximum. The issue is what is the minimum.

On forfeiture, I would strongly encourage you to look into that much more seriously. There is much more that could be done, and it is an extremely--has a lot of potential, because any time you can give law enforcement that much more motivation to get out there and do their jobs, and also, to benefit the efforts of law enforcement, it is very important.

On telecommunications type of issues, we hear from the industry that although there is the issue of reporting child pornography, there is a separate issue, and that is the filtering, essentially, that they would do to detect it in the first place. And we got a comment the other day from one of the major industry leaders, saying that they essentially could turn up that filter, tighten it up, enhance it, and completely blow law enforcement out of the water. And I think there was a realization, all the way around, that you want referrals, we will give you referrals kind of thing.

This is a huge problem. We need them to find more, but we also need to be ready to get it. There is also an issue, I would strongly urge you to talk to industry. What they can do that legislation may not be able to do, and certainly not law enforcement, is tell us what is next. This is truly staggering. The latest that I have heard is wireless Bluetooth technology being used to transfer child pornography where perpetrators gather in a park, and just while they are standing there, watching the pigeons, they are transferring child pornography to each other. My guess is at my age and my limited technological expertise, that is not even the beginning of it, and unless we are hearing from them about what is coming next, 10 years down the line, we are really losing.

I would also mention to you another thing you may want to follow up on, that we are hearing from industry, and that is that many of these perpetrators are actually cataloging children. These images have a monetary value, but that value goes up tremendously when there is a name and address attached to it, and the latest thing that we are hearing is that people are actually putting those names, addresses, elementary schools, and identifying information with these photos, and selling them, and cataloging them.

Finally, just to respond to one other thing. Well, let me talk about two other things. One is that one of the witnesses on this last panel mentioned that, if you find the abuser, that is where you want to go first. I would say to you that is where you want to go first, if you have extremely limited resources. And this is the problem. We cannot just focus on manufacturing. It would be like legalizing heroin, and saying we are going to go get them in Afghanistan where they are growing the poppies. If we do not get serious about the--

MS. DEGETTE. Can I interrupt you for a minute?

MR. WEEKS. Yes, ma'am.

MS. DEGETTE. Because I see Justin leaving, and I have been meaning to thank him, Mr. Chairman. I apologize to interrupt the witness, but I just want to thank you and your family, and everybody for coming to these hearings, and for bringing this to us. You do not know how much you have helped stop this practice, by coming to us. So, I just want to say thank you, and I hope you can come back to some of the

other hearings that we will have. And I hope you can be there when we pass the legislation that will help put a stop to this.

MR. WHITFIELD. Thank you, Ms. DeGette, and we met with Justin earlier, and we all expressed our appreciation to him, and wish him the very best, and we will stay in touch with him. Sorry, Mr. Weeks.

MR. WEEKS. No, I am glad you stopped.

My final point is simply on international treaties. There was a press conference held this morning that talked about the fact that there were only five nations in the world that had serious laws. I have a little bit a problem with characterizing our laws as all that serious, but the point is a serious one, and that is that we need to recognize this as a human rights issue, and whenever human rights are discussed, the exploitation of children should be discussed, and I think you can advance the effort there.

Thank you very much.

[The prepared statement of Grier Weeks follows:]

PREPARED STATEMENT OF GRIER WEEKS, EXECUTIVE DIRECTOR, NATIONAL ASSOCIATION  
TO PROTECT CHILDREN

Chairman Whitfield, Congressman Stupak and distinguished members of the Subcommittee, I am Grier Weeks, the Executive Director of the National Association to Protect Children, generally known as PROTECT. PROTECT is a grassroots membership organization focused exclusively on child protection issues. We have members in all 50 states, and we pride ourselves on being one of the most nonpartisan organizations in America.

As PROTECT works in state legislatures, one of the greatest problems we see is our national failure to aggressively respond to child pornography and the use of the internet for both dissemination of such material and direct exploitation of individual children.

People have argued for decades about what child pornography *is*, yet there has been virtually no attention paid to what it is *not*. It is our position that understanding what child pornography is *not* is the key to understanding—and actually doing something about—what it is.

A 2005 study funded by Congress studied child pornography possession cases nationwide.<sup>1</sup> In looking at the nature of the images being trafficked on the internet, the study revealed the following:

- 83 percent of possessors had images of children between ages 6 and 12
- 80 percent had images of sexual penetration of children—that is to say, child rape
- 21 percent had images showing “children who were gagged, bound, blindfolded or otherwise enduring sadistic sex.”
- Only 1 percent were in possession solely of images that depicted simple nudity or what researchers termed “softcore” pornography<sup>2</sup>

<sup>1</sup> “Child Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Victimization Study,” National Center for Missing and Exploited Children, Crimes Against Children Research Center, U.S. Department of Justice, 2005.

<sup>2</sup> The study also found that 40 percent of those possessing child pornography were found to have sexually assaulted a child in addition to their child pornography crimes and an additional 15 were

So we begin with the understanding that child pornography is not a “free speech” issue, nor does it have anything to do with definitional arguments over whether a given image is “obscene.” It is a human rights issue of catastrophic proportions.

Two years ago, law enforcement agents in Canada and the U.S. arrested a criminal in my home state of North Carolina. Brian Schellenberger was convicted of producing child pornography and distributing the images over the internet. Photos showed that a six-year old girl was kept in a cage, beaten, sexually tortured and urinated and defecated on.

The criminal penalty for being an accomplice to that crime, for possessing those images in North Carolina, is a felony—the exact *same* felony penalty you would get for operating a Bingo game without a license or Cockfighting.<sup>3</sup>

In California, the penalty is a misdemeanor.<sup>4</sup> Distributing it to others is a misdemeanor.<sup>5</sup> *Using a child* to distribute it is a misdemeanor.<sup>6</sup> Under California law, even manufacturing such a despicable “product” is a minor felony, with no minimum prison sentence.<sup>7</sup>

In Colorado<sup>8</sup>, Oregon<sup>9</sup> and North Dakota<sup>10</sup>, possession of brutal images of children being raped, sodomized and humiliated is a misdemeanor. In Iowa, it’s an “aggravated misdemeanor,” the equivalent of Livestock Abuse.<sup>11</sup>

If you compare the risk-gain ratio for those who traffic in such a “product” to the risk-gain ratio for those who traffic in cocaine, you will instantly understand why our national weakness on this issue has attracted so many new predators.

Nationwide, an estimated 96 percent of those arrested for child pornography possession are convicted. But fewer than 60 percent are ever incarcerated. Of those convicted solely of child pornography possession, fewer than one in three serves more than a year in jail.<sup>12</sup> This is *despite the fact* that child pornography—like narcotics—is illegal contraband in and of itself, and is easily prosecutable.<sup>13</sup>

**PROTECT’s first point is this: Unless and until the States are made to treat “simple possession” of child pornography as the egregious felony it truly is—and unless the funding is made available to aggressively investigate and prosecute possession of child pornography—federal efforts will be hopelessly diluted.**

Instead of federal resources acting as a *multiplier* of state law enforcement efforts, the lack of appropriate legislation and funding is actually discouraging the individual states from protecting our children.

known to have attempted a child sexual assault, a conservative indication of a much larger danger. Thirty-four percent had minor children living in their homes at the time of arrest and an additional 12 percent had direct access to children “through a job or organized youth activity”

<sup>3</sup> North Carolina General Statutes 14-190.17A

<sup>4</sup> California Penal Code 311.11 and 311.3

<sup>5</sup> California Penal Code 311.2 (c)

<sup>6</sup> California Penal Code 311.4 (a)

<sup>7</sup> California Penal Code 311.4 (c)

<sup>8</sup> Colo. Rev. Stat. 18-6-403

<sup>9</sup> Oregon Rev. Stat. 163.687

<sup>10</sup> North Dakota Cent. Code 12.7-27.2-04, “Possession of certain materials prohibited”

<sup>11</sup> Compare Iowa Code 717.1A, “Livestock abuse” to 728.12 (3), “Sexual exploitation of a minor.”

<sup>12</sup> “Child Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Victimization Study,” National Center for Missing and Exploited Children, Crimes Against Children Research Center, U.S. Department of Justice, 2005.

<sup>13</sup> Television station WITI in Wisconsin recently conducted a painstaking investigation of every felony conviction for child pornography possession in their state. They found that 75% resulted in no prison time whatsoever. Reporter Bryan Polcyn requested data from the Wisconsin Supreme Court on all cases charged under state statute 948.12 (1m), “Possession of Child Pornography,” for the years 2003-2005. They then researched the disposition for each case that resulted in a conviction.



Until the states get serious, U.S. prosecutors will continue to pick up the slack for local prosecutors, who have grown dependent upon the federal government to prosecute their criminals for them.<sup>14</sup> Internet Crimes Against Children task forces will continue to provide training and technical assistance to front-line law enforcement agents who are so unsupported by their own states that they often have long backlogs of hard drives waiting to be analyzed, many of them containing evidence that could save a child immediately.<sup>15</sup> And the mass of domestic criminal conspirators who create and feed the insatiable demand for more and more children to be raped on camera will remain at large, as limited federal resources are triaged and focused on chasing after the “major cases” of commercial manufacturers and distributors.

**PROTECT’s second point is that the federal government also must get serious. We are losing this war, and we are not supporting our troops on the front lines.**

Recent estimates of the size of the exploding global criminal market in child pornography are in the multi-billion dollar range.<sup>16</sup> Yet, by no objective measure can we claim to be serious or prepared as a nation about stopping what is being done to these children.

The FBI’s Innocent Images National Initiative is funded at a level of about \$10 million annually. By comparison, the Department of Housing and Urban Development just announced it was awarding more money than the entire Innocent Images budget to build 86 elderly apartment units in Connecticut... and almost 7 times their budget just on the homeless in Ohio.<sup>17</sup> The administration has proposed 20 times the entire Innocent Images budget for abstinence-only education programs through the Department of Health and Human Services.<sup>18</sup>

The Department of Justice’s Internet Crimes Against Children (ICAC) Task Force program received about \$14.5 in FY 2006. That is less than one-fifth the amount proposed for a new initiative to help former prisoners reintegrate into society.<sup>19</sup> Last year’s budget included \$211 million for the Department of the Interior for “high-priority brush removal” and related projects. \$14.5 million doesn’t clear much brush.

The law enforcement officers on the front lines of this war won’t come here and tell you what they honestly think of these priorities. They will be grateful if you simply keep their budgets growing. And while we realize that your committee is not the one responsible for these spending priorities, I don’t know how any of us, as taxpayers, can look these men and women in the eyes.

The radical increase in child pornography we see today is the direct result of failing to match our rhetoric about children with the resources needed to fight this war.

**Our third and final point is that while you have an incredible array of experts at your disposal—all of whom, including PROTECT, are eager to provide specific**

---

<sup>14</sup> Reliance upon federal prosecutors to handle internet child pornography cases is so common throughout the U.S. that many jurisdictions appear to regard child pornography as a “federal crime” or federal problem, further weakening state and local resolve to mount serious campaigns to aggressively investigate and prosecute.

<sup>15</sup> Legislation is currently before the Maine state legislature to increase funding for the state crime lab for investigating child pornography. Local news reports say that backlogs of hard drives, awaiting forensic analysis, are severe. A state cyber crimes agent in the Midwest reported recently that he waited months for a hard drive to be analyzed, only to find that it had graphic photos showing the suspect was sexually assaulting his own child, who lived with him at home. Federal agents also report bottlenecks with computer analysis teams.

<sup>16</sup> National Center for Missing and Exploited Children

<sup>17</sup> HUD Section 202 grant funding announcement, January 5, 2006.

<sup>18</sup> HUD Continuum of Care and Emergency Shelter grant funding announcement, January 25, 2006

<sup>19</sup> Budget of the United States Government, FY 2007

**legislative and policy solutions—the expertise we need most now is the expertise you possess: political leadership.**

On behalf of our members and the millions of Americans who believe that nothing should be a higher priority than protecting children from predators, I ask you for that leadership and I thank you for the opportunity to testify in this important hearing.

MR. WHITFIELD. Mr. Weeks, thank you very much, and tell me, did you form PROTECT yourself, or--

MR. WEEKS. No, actually, several people did. There were a number of very prominent experts around the country, including Jay Howell, who started the National Center for Missing and Exploited Children, who said for the longest time, the only group in this country that didn't seem to have a lobby is abused kids, and that is why we exist.

MR. WHITFIELD. And how old is it?

MR. WEEKS. We are about 3 years old. We have changed the laws in about seven or eight States now, and worked with both Democrats and Republicans.

MR. WHITFIELD. And you are funded by just private donations?

MR. WEEKS. Through our members.

MR. WHITFIELD. Yeah.

MR. WEEKS. Right.

MR. WHITFIELD. Well, thank you for the great work that you are doing. Talking about the penalties for these crimes, and you mentioned in your testimony how there is this great disparity going from State to State, and you mentioned in Iowa, it is a misdemeanor similar to an animal abuse case. Of course, any of these crimes can be prosecuted under Federal law, I am assuming, and I guess it just gets down to a matter of whether or not interstate commerce is involved, and whatever. But I find it laudable that you are trying to increase the penalties at the State level, because we know that the largest percentages of the cases are prosecuted at the State level.

And I was curious, when you lobby for tougher sentences in the State legislatures, what are some of the reasons that you are given for opposing what you are trying to do?

MR. WEEKS. It is pretty awful. I mean, there is a widespread tolerance for this, especially for possession, so-called simple possession. You don't hear that same excuse used for possession of heroin. I think we have heard it all, but we are now days away from getting a major bill introduced in California, which in California, as I failed to mention, there is also a statute for luring a child over the Internet, and for the longest time, there was a vigorous debate going on in committees about whether that should be an infraction or a misdemeanor.

MR. WHITFIELD. Really. And South Carolina, I understand, just recently passed some legislation that would make a person that was twice

convicted of child molestation eligible for the death penalty. Is that correct?

MR. WEEKS. Yes. Let me just say this about that. And we don't have a position on whether someone should be put to death, or go for life, but we have a lot of these laws, often named after dead children, that doesn't do much.

MR. WHITFIELD. Yeah.

MR. WEEKS. South Carolina is my family's home, and I feel entitled to say this, it is a little hard to take, given the fact that South Carolina has a law on the books called assault and battery of a high and aggravated nature, and the vast majority of child sexual abuse seems to be plea bargained down to that.

MR. WHITFIELD. Yeah.

MR. WEEKS. So, you know, it is great to have tough laws on the books, but if you are only using them for that tiny fraction of stranger abusers that gets all the media attention, it doesn't do a whole lot for kids.

MR. WHITFIELD. But I guess the bottom line of this is while you are trying to increase the penalties for possession of pornographic material involving children, most of these child molestation cases regarding children today appear to be more and more aggravated. There appears to be rape involved. There appears to be even torture involved. There appears to be, in some cases, I guess they are holding children against their will. Unfortunately, in some cases, you have parents involved in this.

MR. WEEKS. In the majority of cases.

MR. WHITFIELD. Which is almost unbelievable, but those crimes, if they are being prosecuted on those crimes, I mean, those are quite severe. Would you agree with that?

MR. WEEKS. No. Essentially our studies show that about 4 percent of cases nationwide, of all criminal cases, ever go to a jury. So, start off with the vast, vast majority of them being plea bargained.

MR. WHITFIELD. Okay.

MR. WEEKS. Even a smaller percentage of child sexual abuse cases ever go before a trial. So, we are talking about how are cases plea bargained? They are plea bargained, and there is also charge bargaining that goes in. What is happening now, with a lot of these laws, like Jessica's Law, is that you have these draconian sentences that sound great, but very few people will ever be charged with them, and in fact, these cases are trivialized to a great extent.

Let me mention one thing related to that, though, and Chairman Barton brought this up. For decades, what we have heard is that we would love to prosecute these crimes against children, but they are tough.

We have problems with young witnesses. We have problems with evidence. And it is very tough, and we have to plea bargain. This is the exception. We now have a type of crime where you have hard, cold evidence. And if we don't put people away for that, shame on us.

MR. WHITFIELD. Absolutely. In your testimony, you talked about the case in North Carolina, I believe, and where, the gentleman was keeping a young girl in a cage. Was that his daughter, or--

MR. WEEKS. That was a complicated story. I hesitate to say, because I may be mixing it up with the second one. I am not sure.

MR. WHITFIELD. Do you know what penalty he received for--

MR. WEEKS. He did get, I think, 100 years under the Federal law.

MR. WHITFIELD. So, he was prosecuted by Federal officials.

MR. WEEKS. Right. And again, I want to emphasize, there may be some resistance among ideological conservatives to telling the States what to do, and being heavy-handed about it.

MR. WHITFIELD. Right.

MR. WEEKS. But the flipside of this is, they are using the Commerce Clause to essentially slough this off on the Feds. I mean, we have heard top criminal justice policy people in State legislatures essentially talk about these crimes as if they are a Federal problem, even to the extent where one of the most influential policymakers in a State capital told me, look, if you want us to be prosecuting these, then give us more money for Federal prisoners that we are taking care of. So, there is a real disconnect there, and this is, I would think that the staunchest conservative would be a heavy-handed Federalist on this.

MR. WHITFIELD. Well, I mean, I certainly don't have any problem for ramping up and prosecuting more people at the Federal level on this, and I am sure the rest of us do not. So, thank you for mentioning that.

One other comment I would just like to make. You had mentioned that industry told you that they could increase their filters and blow the law enforcement out of the water. Now, would you elaborate on that a little bit?

MR. WEEKS. Well, yeah, I would love to, and let me say, I think it is fair to say that law enforcement is already blown out of the water.

MR. WHITFIELD. Well, okay.

MR. WEEKS. By any definition.

MR. WHITFIELD. Right.

MR. WEEKS. But essentially, what they were saying is look, we are reporting everything that we are detecting.

MR. WHITFIELD. Yeah.

MR. WEEKS. But they could detect a lot more.

MR. WHITFIELD. Yeah.

MR. WEEKS. And they are the ones that are going to be the most sophisticated at detecting it.

MR. WHITFIELD. Right.

MR. WEEKS. But there is a realization that if they greatly increase their detection abilities overnight, that we won't be able to keep up with them, and that is the problem.

MR. WHITFIELD. So, there are so many violations going on that it would just swamp everybody.

MR. WEEKS. Right. Well, there were several questions today about the gentleman from Wyoming, who said there were over a million IP addresses, and I am not sure everybody got the real story there. The real issue, in my mind, is the number of IP addresses, not the number of images.

MR. WHITFIELD. Right.

MR. WEEKS. We are talking about a million computers.

MR. WHITFIELD. Yeah, unbelievable. Yeah. Well, and you devote full time to this project?

MR. WEEKS. Not just to child pornography, but to the work on child abuse legislation, yes.

MR. WHITFIELD. Yeah. Well, this is such an overwhelming problem, and it is so complex, that is difficult not to become discouraged about it, right?

MR. WEEKS. Yeah, I think everybody, the ones that are looking at this every day are the ones that I worry about, but I think there is a common thread, which is if it doesn't kill you, it just makes you feel like, you know, you are doing the Lord's work, getting up every morning.

MR. WHITFIELD. Yeah. Well, thank you very much for being with us, and at this time, I will recognize Ms. DeGette for questions.

MS. DEGETTE. Thank you, Mr. Weeks.

As I understand it, right now, the folks who testified earlier, the Federal prosecutions really take place involving cases where there is some use, there is either international trafficking, or there is some use of the U.S. mail. Is that correct?

MR. WEEKS. I think that is fair to say, yeah.

MS. DEGETTE. Because of the way the Federal statutes are, to prosecute--

MR. WEEKS. They are looking at getting the best bang for their buck, and they are looking at interrupting commercial networks and things like that.

MS. DEGETTE. Right. Well, there is no Federal statute that makes it a crime to possess these materials unless there is some involvement of the Commerce Clause, correct?

MR. WEEKS. Right.

MS. DEGETTE. So, it would have to be interstate.

MR. WEEKS. And if the Internet is involved, of course, that is a given.

MS. DEGETTE. Well, I mean, yes and no. It would be, as someone who has been in, who has done criminal work before, I mean, if you have got a situation where you have got a case where someone was doing these horrible crimes within a State, and transferring it within a State, while technically, you have got the Commerce Clause involved, because it is the Internet, from a law enforcement standpoint, it is really going to be hard to prosecute that by Federal authorities, right?

MR. WEEKS. Right. Right.

MS. DEGETTE. That is why we need tough State laws and Federal laws, right?

MR. WEEKS. That is one reason.

MS. DEGETTE. Yeah.

MR. WEEKS. Another, though, is simply that unless the Federal government wants to increase its force by, you know, by fifty, it is going to have to work with the States, and create incentives for the States to do their share. And a related issue, too, is that a study done, it was commissioned by Congress, came out last year on people that possess child pornography found that 40 percent of them were conclusively known to have also sexually abused children directly, and another 15 percent were known to have tried to lure. So, you have 55 percent, representing a much larger percent, no doubt, that had actually molested children. If we don't have on the ground, local expertise and resources to fight this, what is going to happen is, every time that little 5-year-old-girl goes to school, and discloses that she is being molested at home, that guy may have child pornography. It is a very high likelihood that he has child pornography on his computer. Now, are we going to put together a case that involves dragging that girl through the wringer in court, and many prosecutors will just dismiss it out of hand, because she is too young, or are we going to actually go and get that hard drive, and that is the issue. We are losing the ability to protect children in our local communities every day.

MS. DEGETTE. Right. Well, and I am not trying to disagree with you in any way. I think we agree. What we need is tougher enforcement of Federal laws and State laws and resources at all levels, and coordination. And frankly, from listening to the second panel, I was a little encouraged in this hearing, that at least the levels of authorities seem to be coordinating. I mean, the problem is not, and the Chairman will tell you, we see a lot of situations where the agencies can't even coordinate with each other. So, the good news is, at least they have the mechanisms to coordinate. Do you agree with that?

MR. WEEKS. I have to take their word for that.

MS. DEGETTE. Yeah. And so, really, what we need is strong laws and resources, to help them carry out their charge, correct? You need to answer in words.

MR. WEEKS. Yes, yes. Excuse me.

MS. DEGETTE. Thanks. Now, so, with that in mind, are there Federal statutes that you think we can strengthen, as well as the State laws?

MR. WEEKS. I think that the penalties for possession need to be increased. Since Federal, since the guidelines were deemed advisory only, that is a loophole now. I think that most of the cases you hear about are not getting probation, because they are just essentially cherry picking at this point, but that is a loophole that is a serious issue. I think that forfeiture is another major issue that should be looked at. International treaties. I wish I was more of a telecommunications expert for you.

MS. DEGETTE. Yeah. Okay. Well, but you think we have the adequate laws on the books to prosecute, to federally prosecute cases, even when mail is not involved or international situations. Do you think we can prosecute these cases, simply because they are done on the Internet?

MR. WEEKS. I think we can prosecute them all day long and all night, yeah.

MS. DEGETTE. All right. I was appalled to hear that Colorado is one of the States that just classifies this as a misdemeanor, and I would imagine that States like Colorado and other States that classify it like this have not really looked at their laws vis-a-vis the increase, as the Chairman said the increasing violence and depravity of these Internet communications and the horrible abuse for the children. Would that be your sense as well, working in these things?

MR. WEEKS. I am conflicted about that, and I will tell you why. I have a real hard time believing there are as many people left in this country, especially in positions of leadership, who are that clueless about the nature of child pornography. I just don't believe it. I think, it would be interesting to find out in your State, and other States like that, what has transpired in recent sessions, whether or not they have tried to increase the penalty. Often, what it is, is unfortunately, is prosecutors who just want so much discretion that they resist mandatory minimums and increased penalties. But there is also--

MS. DEGETTE. Well, part of what happened, and I will tell you, I was in the State legislature in Colorado in the early to mid '90s. During those years, we basically tripled, sometimes quadrupled the sentences for the existing felonies in the State. And so, for example, where you had a

crime where it might be an 8 year maximum penalty, it suddenly went up to 36 years, and then, you had the mandatory minimum sentences put in, and in many cases, those increases were warranted. Some of the maximum penalties for different felonies were too low. In other cases, there was no judgment. It was just a rush to increase the penalties.

Well, then, what happened, of course, in the late 1990s, in the past few years, the prisons and the criminal justice systems have become completely overloaded in States like my State and other States. So, I think the legislatures have now been loath to increase the penalties of other crimes because they don't have any place to put the perpetrators, which is a tragedy, because what is happening is the perpetrators for these horrible crimes that are affecting younger and younger children are going away with a slap on the wrist, while other people, who have committed crimes that are not crimes against people, economic crimes and other kinds of crimes, are sitting in prison for 38 years, and that just seems insane to me.

MR. WEEKS. Yes.

MS. DEGETTE. And you agree.

MR. WEEKS. I agree.

MS. DEGETTE. And so, I imagine that is part of the explanation of what has happened here. But I will tell you this. I intend to call up my Senate President and House Majority Leader, who are personal friends of mine, and see if they can't get a late bill introduced next week to fix this in Colorado.

MR. WEEKS. Please, and when you do, please make sure it is tougher than felony cockfighting, as it is in my State, because making it a felony in and of itself is not enough. But thank you.

MS. DEGETTE. Well, making it a felony, I mean, in a State like Colorado, and you have to look at the different States, in a State like Colorado, making it a felony helps, because of the penalty structure.

MR. WEEKS. Absolutely.

MS. DEGETTE. And just one last question. I don't know if you heard me ask the last panel, but for a crime like child pornography, maybe not for the hardcore perpetrators who, as you say, are rapists and child abusers, but for people who possess it, it would seem to me that tougher penalties at the State level and at the Federal level would begin to deter these crimes, because simple possession of it, if someone knew they were going to prison for a long time, that might make them think twice. For the people who are perpetrating these horrible crimes, they are a different story, and they need to be locked up for even longer, but wouldn't you agree, just if someone knew that there was a certainty that they could be arrested and prosecuted and go to jail, that would really reduce the amount of possession.



MR. WEEKS. I absolutely agree. I think to a large extent, it is the certainty of being caught and prosecuted that is the most important thing, and that is not there.

MS. DEGETTE. Right. Well, thank you very much, and thank you, Mr. Chairman.

MR. WEEKS. Thank you.

MR. WHITFIELD. Thank you, Ms. DeGette, and that concludes today's hearing, but before we adjourn, without objection, I want to ask that the slides shown during the hearing by Mr. Flint Waters be entered into the record. The slides from the Immigration and Customs Enforcement, the Regpay article from the Wall Street Journal, and then Chapter 26 from Dr. Cooper's book, and then, the record will be open for 30 days for any additional information that may come in.

[The information follows:]





**superdad38's profile** Last Updated: December 26, 2001

<b>My Email</b> <i>Private</i>	<b>Basics</b> Yahoo! ID: <b>superdad38</b> Real Name: <b>[REDACTED]</b> Location: <b>Cheyenne</b> Age: <b>38</b> Marital Status: <b>Single And Looking</b> Gender: <b>Male</b> Occupation: <b>I have one!!!!</b>  <small>Offline Send me a message</small>	<b>ADVERTISEMENT</b>  <b>Managing your money is easy.</b> Find out how.
<b>On Yahoo!</b> <b>Add to friend list</b> · <a href="#">Messenger</a> <b>View my briefcase</b> · <a href="#">Briefcase</a>	<b>Favorite Quote</b> "If it feels good..... DO IT!!!!" <b>Links</b> <small>Create your own home page at GeoCities!</small> · Home Page: <i>No home page specified</i> · Cool Link: <i>No cool link specified</i>	

◆ Arrested: Dec 31, 2001 – Cheyenne, Wyoming



**U.S. Immigration  
and Customs  
Enforcement**

**Cyber Crimes Center  
(C3)**

**11320 Random Hills Road  
Suite 400  
Fairfax, Virginia 22030  
703-293-8005**

**Cyber Crimes?**

**The electronic introduction, into US Commerce,  
of prohibited items via the internet, or the illegal  
introduction of prohibited "tangible" items  
facilitated by the internet.**

**Also applies to illegal exports**

**No real borders - only cyber borders. Nothing is  
required to clear Customs.**



February 23, 2006

### Illegal Use of Internet

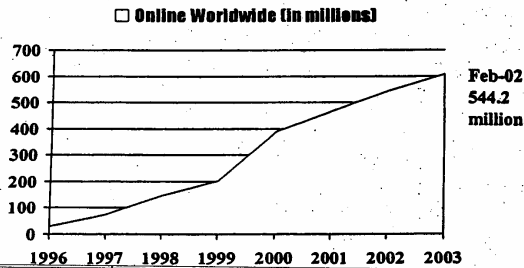
#### Why ?

- Efficient Communications
- Secure Communications - Encryption
- Digital "Merchandise" can Transverse Borders Without Inspection
- Migration of legitimate business to "the Net"
- Marketing Power of the Internet



February 23, 2006

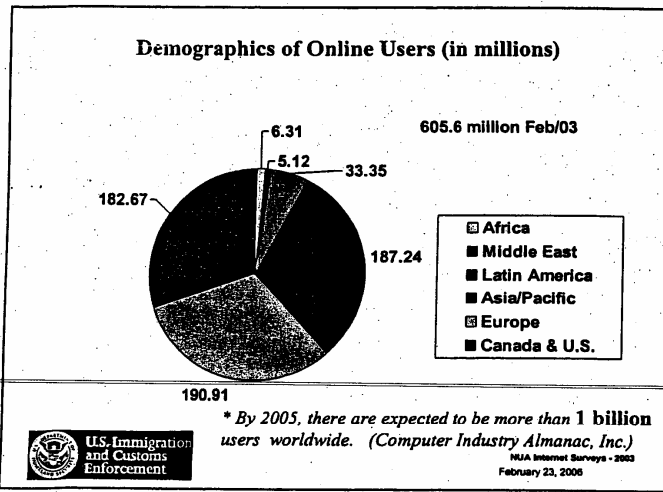
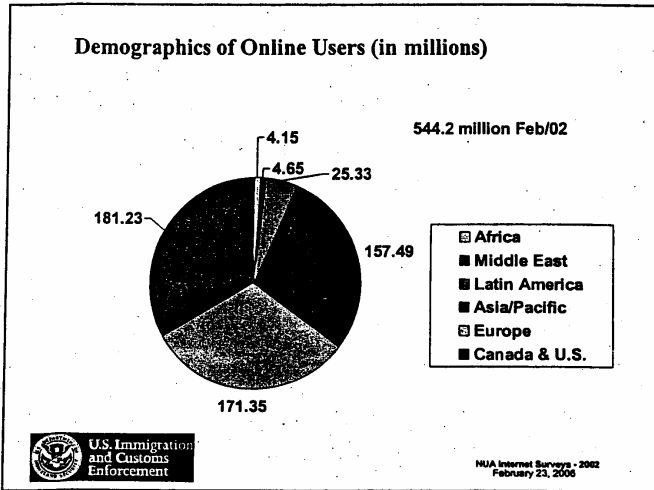
### Online Growth



\* In 2002, it was projected that the 2003, online worldwide users would be over 600 million.



February 23, 2006  
New Market Surveys - 2002



## **Immigration and Customs Enforcement (ICE) Cyber Crimes Center (C3)**

Co-location of investigators, analysts, computer specialists and computer forensic specialists to combat Cyber Crimes

### **Mission**

Develop & refer case leads  
Provide investigative coordination & oversight  
Training: Internet 101, Computer Forensics



February 23, 2006

## **Immigration and Customs Enforcement Cyber Crimes Center**

**Child Exploitation Section (CES)**

**Cyber Crimes Section (CCS)**

**Computer Forensics Section (CFS)**



February 23, 2006

## Child Exploitation Section


### **Child Exploitation Section**

The U.S. Immigration and Customs Enforcement office dedicated to investigating transborder criminal activity on the Internet, has a unit specifically dedicated to investigating the exploitation of children.



February 23, 2006

<b>Staffing / Responsibilities</b>	Operation Predator Internet Programs
<b>Staffing</b>	Commercial Web Sites
1 Section Chief	Peer To Peer
8 Special Agents	Digital Child Exploitation
3 Analysts	Undercover Operations
3 S/A Vacancies	Child Sex Tourism
	NCMEC
	NCVIS
	VGT
	Internet Monitoring
<b>Other Responsibilities</b>	
• Case Referral	
• Field Training	
• Investigative Guidance	
• Oversight of U/C Ops.	

 February 23, 2006

## Child Sex Tourism


**Title 18 USC 2423 (B)**

Travel in foreign commerce for the purpose of engaging in sex with a minor

International travel by Pedophiles is on the rise  
Internet facilitating this increase

Primary areas of concern:  
Latin America, Eastern Europe, and Southeast Asia

---

 February 23, 2006



## **Child Sex Trafficking**

### **Title 18 USC 1591**

Recruiting, enticing, providing, harboring, transporting or obtaining minors for commercial sex acts while engaged in Interstate commerce, using force, fraud or coercion.

May result in imprisonment for any term of years or for life, or both.



February 23, 2006

## **Child Pornography**

### **Title 18 USC 2251**

**Manufacturing/Production**

### **Title 18 USC 2252:**

**Possession**

**Trafficking (Distribution/Receipt)**



February 23, 2006

**Immigration and Customs Enforcement  
Cyber Crimes Center**

**Sources of Information**

**National Center for Missing and Exploited Children:  
Cyber Tip Line  
Tips from ISP's  
Referrals from US and foreign LE  
Proactive Undercover Operations**



February 23, 2006

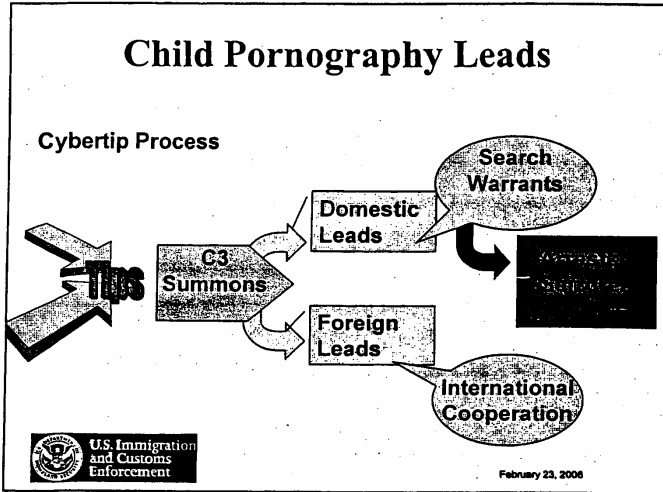
**NCMEC**



- Three special agents are assigned full-time
- ICE provides yearly funding to NCMEC
- Member of Board of Directors
- C3 investigates "Tips" referred to NCMEC by general public and ISPs, (domestic and International)



February 23, 2006



### NCMEC

National Center for Missing & Exploited Children

*FY2002 STATS*

4,406 CyberTips referred by NCMEC to C3  
49 Viable leads referred to field

*FY2003 STATS*

5,151 CyberTips referred by NCMEC to C3  
51 Viable leads referred to field

---

**U.S. Immigration and Customs Enforcement**

February 23, 2006

**NCMEC**

National Center for Missing & Exploited Children

***FY2004 STATS***

**15,952 CyberTips referred by NCMEC to C3  
160 Viable leads referred to field**

***FY2005 STATS***

**20,000+ CyberTips referred by NCMEC to C3  
115 Viable leads referred to field  
776 Leads referred via VPN**



February 23, 2006

**Operation Predator**

**Launched by DHS Secretary Ridge on July 9, 2003**

**The goal of the operation is to identify child predators, prosecute them and force them out of the country if they are subject to deportation.**

**“One in five girls and one in ten boys in the US are sexually victimized before the age of 18.” (quote from David Finkelbor - “Current Information on the Scope and Nature of Child Sexual Abuse”, 1994)**



February 23, 2006

### Operation PREDATOR

- Uses the Internet to track sex offenders who prey on children.
- A single web portal to provide public and law enforcement with a single Internet address to access databases of registered US Sex offenders.
- Created the NCVIS, a central system of digital child exploitation images to assist in the arrest and prosecution of child exploiters and the rescue of the child victims.
- Actively pursues the deportation of non-USC's convicted of felonies against children.



February 23, 2006



### Operation Artus



Joint investigation between C3 and the German National Police involving the production and exchange of child pornography (images and movies) over Internet Relay Chat (IRC) channels. Some suspects were members of the previously investigated "Wonderland Club".

53 targets identified in 10 countries  
 37 search warrants simultaneously executed  
 10 search warrants in U. S.  
 8 arrests in U. S.  
 3 suicides



February 23, 2006



## Operation Hamlet



A joint investigation by ICE and the Danish National Police targeting a ring of pedophiles who molested their own children and distributed the images on the Internet.

16 U.S. Search Warrants  
 19 U.S. Arrests  
 12 Foreign Arrests  
 1 Suicide  
 100+ Children Rescued



February 23, 2006



## Operation Blue Orchid



A joint investigation by the U.S. Customs Service and Moscow City Police into the international production and distribution of child pornography videotapes. C3 coordinated the U.S. investigation. "America's Most Wanted" TOP COP awards were issued to the S/A's who coordinated the investigation.


### *Statistics*

18 Federal Search Warrants  
 5 State Search Warrants  
 10 Consent Searches  
 16 Arrests  
 16 Indictments  
 12 Convictions



February 23, 2006

**Operation Kinderschutz**




An operation initiated in 1997 between the BKA and U.S. Immigration and Customs Enforcement wherein child exploitation leads are referred to the field for investigation.

*FY2002 STATS*

- 138 Cases referred to field
- 25 Arrests, 36 Indictments, 28 Convictions, 47 Seizures

*FY2003 STATS*


- 92 Cases referred to field
- 32 Arrests, 31 Indictments, 30 Convictions, 36 Seizures




February 23, 2006

**Operation Mango – Child Sex Tourism**


- Provided “Escorts”, adolescent Mexican boys to engage in sexual activity with visiting pedophiles
- Established by Timothy Joseph Julian in 1998
- Managed by convicted child molester Robert Decker
- Conspiracy involving more than 14 US citizens
- One minor smuggled into the U.S.
- Gained interest and cooperation from the Mexican Government








February 23, 2006

**National Child Victim Identification Program**



**Internet Crimes Against Children**

**NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN**


- Housed at the ICE Cyber Crimes Center (C3)
- Will contain all known and unique child pornographic images
- For the benefit of all law enforcement
- Images contributed by L.E.A.s and NCMEC CyberTipline
- Victim identification information maintained by NCMEC
- NCMEC will provide Victim ID certification for litigation purposes
- Investigative analysis conducted by participating agencies

**Programs**

**Operation Predator: Total arrests: 7,321**  
**US citizens arrested: 852 (Child Exploitation)**  
**Non-US citizens: 6,469 of which 3,900 have been deported**

**Undercover Operations:**  
**Focus on child sex tourism**  
**Servers in 3 foreign countries**  
**International Citizens**

---



February 23, 2006



## Programs continued

**Commercial Web Sites:****Project Falcon:**

**354K transactions resulted in:  
21K domestic targets, 341 arrests, 254 indictments, 241  
convictions, 579 search warrants,**

**12K foreign targets. 17 countries, 12,000 arrests 907 search  
warrants**

**Project Watchdog, (10-2005):**

**cases: 135  
arrests: 6  
leads to be researched 5, 000+**



February 23, 2006

## Program Results Continued:

**Child Sex Tourism (since 2003):**

**32 arrests 23 indictments 16 convictions.  
197 total cases opened  
at present cases open 81**

**NCMEC: International leads (non-VGT):**

**FY 06: 2,488 reviewed, 792 referred to field for action.**

**NCVIS (since 2003):**

**112,422 images enrolled  
260 identified series  
Total Cases: 465,  
Images: 213,502 Videos: 1,575  
Matches: 91.25%,**

**VGT:**

**314 NCMEC leads sent to member countries**



February 23, 2006

### Virtual Global Taskforce (VGT)



The Virtual Global Taskforce (VGT) was created in 2003 as a direct response to lessons learned from investigations into on-line child abuse around the world. It is an international alliance of law enforcement agencies working together to make the Internet a safer place.



February 23, 2006

### Virtual Global Taskforce (VGT)

The mission of the Virtual Global Taskforce is:

- to make the Internet a safer place;
- to identify, locate and help children at risk; and
- to hold perpetrators appropriately to account.



February 23, 2006

### **Virtual Global Taskforce (VGT)**

**The Virtual Global Taskforce is comprised of:**

- Australian Federal Police**
- National Crime Squad (United Kingdom)**
- Royal Canadian Mounted Police**
- Department of Homeland Security (ICE)**
- Interpol**



February 23, 2006

### **Virtual Global Taskforce (VGT)**

**The Virtual Global Taskforce delivers innovative crime prevention and crime reduction initiatives to prevent and deter individuals from committing on-line child abuse.**

**On-line child abuse includes searching for, sharing and downloading images of children being physically and sexually abused and "grooming" children in, for example, chat rooms with the intention of committing sexual abuse both on and off-line.**



February 23, 2006

### **Virtual Global Taskforce (VGT)**

**INITIATIVES:**

**Present:**

**A VGT Website**

**VGT Industry Partnerships**

**Future:**

**A 24/7 On-line Presence**

**A "Most Wanted" Initiative**

**Opening Membership of the Virtual Global Taskforce to  
Other Qualified International Partners**



February 23, 2006

**Questions?**

## THE WALL STREET JOURNAL

### Dangerous Mix: Internet Transforms Child Porn Into Lucrative Criminal Trade --- Company in Belarus Collected Millions From Pedophiles; A Landmark Prosecution --- Agent's Rendezvous in Paris

By Cassell Bryan-Low

2438 words

17 January 2006

The Wall Street Journal

A1

English

(Copyright (c) 2006, Dow Jones & Company, Inc.)

On a Saturday morning in October 2003, federal agents raided the apartment of Chicago pediatrician Howard Marc Watzman. They found two computers with more than 3,000 images of boys and girls as young as 4 years old being sexually exploited. Mr. Watzman was later sentenced to five years in prison for possessing child pornography.

The case is one of more than a thousand stemming from a broad international probe into a company called **Regpay** Co. in the former Soviet republic of Belarus. **Regpay** gathered lurid images and sold them to pedophiles around the world with the help of U.S. companies that collected credit-card payments.

**Regpay** offers a window into how the Internet has transformed what was once a cottage industry into a sophisticated business. The company is at the center of what U.S. law-enforcement officials call the largest Internet child-pornography investigation to date and the first to follow the international financial trail of child-porn sales. The probe has discovered the names of some 40,000 Americans who downloaded child porn and led to more than 1,400 arrests world-wide including about 330 in the U.S. At least three users arrested in the U.S. have committed suicide.

Some estimate the Internet child-pornography business could bring in billions of dollars annually. "It has now become a revenue generator for organized groups," says Ernest Allen, head of the National Center for Missing and Exploited Children, an Alexandria, Va., nonprofit.

U.S. and U.K. child-protection experts estimate that there are thousands of commercial Web sites containing child pornography and as many as 100 new ones pop up each month. They say the children being abused are becoming younger and include toddlers. The potential market is large: As many as one in 1,000 men has a sexual interest in children, estimates Hamish McCulloch, assistant director for trafficking in human beings at Interpol, the international police organization. The problem is less common in women, though not unknown.

In the 1980s, a broad crackdown in the U.S. and other countries largely choked off the flow of child pornography, forcing it out of its traditional niche of sex bookshops and into underground networks of collectors. When the Internet became widespread in the 1990s, it instantly proved popular with pedophiles. There was little risk of prosecution amid a lack of law-enforcement scrutiny.

Child-pornography Web sites draw "people who had never dreamed of indulging in the fantasy" by giving them the perception of anonymity, says Kevin Zuccato, director of the Australian federal police's high-tech crime center. Thanks to better Internet connections, **Regpay's** users were able to download millions of images in just one year, something that "simply wouldn't have been possible" 10 years ago, says Mr. Zuccato, whose team coordinated the arrests of **Regpay** customers in Australia.

The Internet emboldens consumers of child pornography to seek out increasingly graphic material. "I wanted to see more and more abusive pictures," says Chris, a technician for a leisure company, in a video interview used for training purposes by the Lucy Faithfull Foundation, a British child-protection charity.

In the video, Chris says he started off spending a few minutes a week searching for child porn on the Web. Soon he was spending as much time viewing images "as I humanly could," and he even recalls one 24-hour session. Chris served a three-year probationary sentence for possessing child pornography in a case unrelated to **Regpay**. The foundation made the video available on condition that his last name not be used.

At first it was mostly pedophiles themselves who distributed the images circulating on the Internet. But the industry's profit potential has increasingly attracted organized criminals who bring with them business and money-laundering skills.

**Regpay's** president was Yahor Zalatarou, a 27-year-old man with a talent for computers. The son of an engineer and a teacher, Mr. Zalatarou grew up in the Belarus capital of Minsk. He worked with Aliaksandr Boika, 31, who has a background in computer software, and Alexei Buchnev, 28, a translator. All three are now in jail.

U.S. law-enforcement agencies suspect that Mr. Zalatarou had connections to a larger criminal network and say their investigation is continuing. Robert Little, a New Jersey lawyer for Mr. Zalatarou, says there were "levels of hierarchy above him." Mr. Little adds that Mr. Zalatarou denies his bosses were "mafia-related."

The allegations against **Regpay** are detailed in indictments returned by a Newark, N.J., federal grand jury in December 2003 and October 2004.

At first the company was called Trustbill. It changed its name to **Regpay** after receiving two cease-and-desist notices from the Michigan attorney general's office in August and September 2002, according to an affidavit by Internal Revenue Service special agent Maria Reverendo attached to a July 2003 complaint against Messrs. Zalatarou and Boika.

**Regpay** processed payments for more than 50 third-party child-pornography sites, and ran at least five of its own with names like darkfeeling.com, lust-gallery.com and lolittles.com. "All girls are under 14," read the advertising blurb for the lolittles.com site, according to Ms. Reverendo's affidavit. Another site advertised "6,000 high-resolution professional images."

The majority of images of child pornography come from the U.S. or Western Europe, law-enforcement officials say. Abusers typically are family members or someone else known to the victim. The advent of digital cameras and camcorders has fueled an explosion in the material available online. Because pedophiles often are willing to share their images at little or no cost by uploading them to the Internet, it is easy for third parties like **Regpay** to obtain and package content on their own sites.

Lawyers for Messrs. Zalatarou, Boika and Buchnev say their clients weren't involved in making child pornography. Some U.S. law-enforcement officials suspect links between **Regpay** and the producers of some images on its Web sites because Belarus authorities said they found a studio used to make pornographic pictures in the same building as **Regpay's** offices in Minsk. But U.S. authorities say they haven't recovered any child pornography from that studio.

Subscribers paid up to \$75 per month to access **Regpay's** sites and the sites for which it handled payments, says Kevin O'Dowd, an assistant U.S. attorney in Newark and a lead prosecutor on the case. **Regpay** processed about \$8 million in payments from June 2002 to June 2003 and pocketed more than 75% of that, according to U.S. authorities. They believe Mr. Zalatarou personally earned only about \$20,000 to \$50,000 a month, bolstering suspicions that he was part of a larger enterprise.

The key to **Regpay's** business was getting money from the credit cards of subscribers in the U.S., Europe and elsewhere into its own accounts, at least one of which was in Latvia, a former Soviet republic neighboring Belarus. ~~Credit card payments from many customers went first to a small Fort Lauderdale, Fla., company called Connections USA Inc. Connections, which had a legal business in online and telephone dating services, had signed up as a merchant in credit-card networks. Both Visa and MasterCard cooperated in the investigation.~~

Connections forwarded subscriber payments to a **Regpay** account in Latvia, according to the indictments. The money was transferred from a Morgan Stanley account -- apparently the business account for

Connections -- to a Deutsche Bank AG account and from there to Aizkraukles Bank in Riga, Latvia, according to the IRS agent's affidavit.

Altogether Connections helped launder about \$3 million from June 2002 through June 2003 in return for a commission of more than 11% on the funds transferred, according to the indictments.

No banks have been charged in the **Regpay** case. Financial institutions have a duty under U.S. law to know their customers and file reports if they detect suspicious activity, but how much a bank should investigate "is still very much a judgment call," says Karen Petrou, managing partner of Federal Financial Analytics Inc., a research and consulting firm in Washington.

The three banks declined to comment on whether they reported suspicious activity in this case. Morgan Stanley spokesman Hugh Fraser says his institution "performed appropriate diligence on the account" and has been cooperating with law enforcement. A Deutsche Bank spokeswoman declined to comment.

Aizkraukles Bank said in a statement that laws prohibit it from talking about specific clients but that in 2003 it investigated several transactions related to the sale of child pornography online and reported its findings to authorities in Latvia.

Mr. O'Dowd, the assistant U.S. attorney in Newark, declined to comment on whether any bank was a target of investigation. In general, he says, banks "really need to focus on continuing due diligence" but "sometimes the ongoing due diligence isn't there."

**Regpay** also used another U.S. company, LB Systems Inc., run by a Belarussian man living in Los Angeles, to transfer funds to a **Regpay** account in Latvia, according to the indictments.

The U.S. investigation began in early 2003 when undercover federal agents in Newark and Washington began purchasing child pornography from Web sites in an attempt to track down people producing and profiting from the sites. It marked the first time the U.S. government followed the financial trail of online child pornography, according to U.S. Immigration and Customs Enforcement. The effort was conducted by the U.S. attorney's office in Newark in conjunction with IRS agents, postal inspectors and immigration officials.

Credit-card and other records led agents to Connections. In June 2003, federal agents searched Connections' offices and secured cooperation from the company's owner, Arthur P. Levinson. Mr. Levinson later pleaded guilty in Newark federal court to a criminal violation of structuring financial transactions to avoid reporting requirements. His lawyer, Henry Klingeman, says Mr. Levinson didn't know that **Regpay's** business involved child pornography.

Connections and two of its employees pleaded guilty to money laundering or failure to report the offense to law enforcement. Connections forfeited more than \$1.1 million and was dissolved. Mr. Levinson and the two employees await sentencing.

Posing as Mr. Levinson, federal agents began communicating with Mr. Zalatarou, the **Regpay** president, and others at the company via email and phone about payment arrangements. Because the U.S. doesn't have an extradition arrangement with Belarus, U.S. authorities couldn't ask the country to hand over Mr. Zalatarou and his cohorts. The federal agents lured Mr. Zalatarou to France under the pretense of discussing future business opportunities.

An agent met with Mr. Zalatarou and Mr. Buchnev, the translator, at the restaurant of the Hotel Concorde La Fayette in Paris on July 30, 2003. Following the meeting, French police arrested the two men in the hotel's lobby. Two days later, Interpol officers arrested Mr. Boika, the **Regpay** software expert, at a hotel on the northeast coast of Spain, where he was on vacation with his wife. Spain and France have since extradited the three men to the U.S.

Mr. Zalatarou and Mr. Boika both pleaded guilty in February 2005 to money laundering and conspiring to distribute or advertise child pornography. They are in jail in New Jersey awaiting sentencing and face up to 40 and 50 years in prison, respectively. In their native Belarus, penalties for those crimes range from a fine to five years in prison.

Mr. Zalatarou declined to be interviewed. Mr. Little, his lawyer, says he has "accepted his responsibility." Mr. Zalatarou left a wife, Anna, and a 3-year-old daughter behind in Minsk. Ms. Zalatarova, an English teacher, describes Mr. Zalatarou as an "ideal husband and wonderful father" who attended church regularly. She says she "cannot admit the possibility" that he was involved in child pornography.

Mr. Boika, who also has a wife and young child in Belarus, didn't respond to a letter mailed to him in jail. His lawyer in New Jersey, Richard Verde, says Mr. Boika "isn't a bad young man" and "is sorry for what he did."

Mr. Buchnev has pleaded guilty to conspiracy to distribute child pornography. He faces up to 20 years in prison. His lawyer, Maria Noto, says he didn't know **Regpay** was involved with child pornography until the July 2003 meeting in Paris with the undercover agent. He "regrets his involvement, as limited as it was," she says.

Federal agents seized server computers in Texas and Virginia that **Regpay** leased to run its business. The servers yielded credit-card transactions from about 90,000 customers. Almost half were in the U.S., with others as far away as Italy, Hong Kong and New Zealand.

The 330 **Regpay** subscribers arrested in the U.S. include teachers, priests and Boy Scout volunteers. Among them was Richard G. Fleischer, a 37-year-old divorced father of two who worked as a home-delivery manager for a newspaper in Florida. Police raided Mr. Fleischer's Tallahassee, Fla., home in August 2004 and found more than 1,100 images and video clips of child porn.

Mr. Fleischer told officers he knew he was "doing things I didn't need to do" but was "too scared to talk to anybody" about his problem and even cut off his Internet access to try to escape the temptation, police records show. He pleaded guilty in Florida federal court to possession of child pornography in December 2004 and is serving 15 years in prison.

Mr. Watzman, the pediatrician arrested in Chicago, spent an average of about \$1,000 a month purchasing child porn from more than 100 Web sites, according to court filings in his case. He couldn't be reached by phone and didn't respond to a letter mailed to his home. His lawyer, Thomas Durkin, says the 39-year-old Mr. Watzman, "like many people, became addicted to pornography." Mr. Watzman pleaded guilty but is appealing certain elements of his case.

Mr. O'Dowd, the **Regpay** case prosecutor, says the probe dealt a big blow to commercial distribution of child pornography on the Internet, "but it wasn't a kill shot." He says online distributors are switching from credit cards to electronic-currency systems, which leave less of a paper trail. Law-enforcement officials suspect the people to whom Mr. Zalatarou reported continue to operate under a different name.

### Dirty Trail

How some funds flowed from customers to Regpay, a child-pornography distributor, between June 2002 and June 2003.

- ① Customers paid up to \$75 a month by credit card.
- ② Connections USA, a Florida company, processed payments and kept 11% commission.
- ③ Funds flowed through accounts at Morgan Stanley, Deutsche Bank and Latvia's Abzrauktes Bank to Regpay operators in Belarus.

Source: court filings





**Yavor Zalatarou**



**Aliaksandr Boika**

Document J000000020060117e21h0002j

More Like This

**Related Factiva Intelligent Indexing™**

+

## INVESTIGATING INTERNET CHILD EXPLOITATION CASES

Sp Agt Christopher D. Trifiletti

One of the primary reasons many offenders use the Internet to exploit children sexually is because of the expectation of anonymity on the Internet; however, this feeling of anonymity is often false. A good investigator, even an investigator with limited Internet knowledge, can penetrate cyberspace to identify and arrest a suspect.

This chapter provides investigators with the basic knowledge to be a competent first responder to an Internet child sexual exploitation complaint and begin the investigation process. Since this chapter uses many technology-specific terms, **Appendix 26-1** provides a glossary.

An effective response to the growing problem of Internet-based crimes, especially those committed against children, must be a mission rooted in 3 components—enforcement, training, and education. The cooperation of all levels of law enforcement working with civilian groups that have an interest in protecting children has led to a large, and sometimes ambiguous, matrix of law enforcement coordination. However, that children and their families have various resources to protect them from online dangers makes it worth the effort. Enforcement is the most logical and important task for all investigators; however, since the Internet continues to grow and evolve, this medium demands more than enforcement. Proper training of fellow investigators and other members of the criminal justice system, including judges and prosecutors, is necessary. Lastly, members of the education, child advocacy, and health-care communities, as well as (and most important) parents and guardians must be educated about the risks their children face when using the Internet. Such education should allow them to find the proper balance between allowing their children to use the Internet as an important resource and protecting their children from the dangers that can be found on the Internet. (See **Table 26-1** for a representation of the complex matrix that makes up the discovery and investigation of child exploitation on the Internet.)

Though this educational mission may seem daunting, providing simple brochures and other printed materials through existing community and law enforcement programs is an important first step (**Table 26-2**). These printed guides provide important information for parents who are not as knowledgeable about the Internet as their children and who may not obtain this information by other means. The development of a comprehensive public awareness mission, which includes aggressive media coverage of cases, an Internet Service Provider (ISP) liaison, guidance for computer and other private sector companies, and an educational campaign for parents, teachers, and children, is equally important.

**Table 26-1. Investigators and Complainants**

### ONLINE INVESTIGATORS

- Federal Bureau of Investigation (FBI)
- Immigration and Customs Enforcement (ICE)
- US Postal Inspection Service (USPIS)
- Internet Crimes Against Children (ICAC) Task Forces

### LAW ENFORCEMENT COMPLAINANTS

- FBI Offices and Legats
- ICE Field Offices and Attaches
- USPIS Field Offices
- Police Departments

### CIVILIAN COMPLAINANTS

- National Center for Missing & Exploited Children (NCMEC)
- Internet Service Providers (ISPs)
- Child Advocates
- Physicians and Other Healthcare

### CHILDREN AND FAMILIES

**Table 26-2. What Can You Do to Minimize the Chances of an Online Exploiter Victimizing Your Child?**

- Communicate with your child about sexual victimization and potential online danger.
- Spend time with your children online. Have them teach you about their favorite online destinations.
- Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for a sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.
- Use parental controls provided by your ISP and/or blocking software but do not totally rely on them. Though an electronic chat room can be a great place for children to make new friends and discuss various topics of interest, it is also prowled by computer sex offenders. Use of chat rooms, in particular, should be heavily monitored.
- Always maintain access to your child's online account and randomly check his/her e-mail. Be aware that your child could be contacted through the US mail. Be upfront with your child about your access and reasons why.
- Teach your child the responsible use of online resources. There is more to the online experience than chat rooms.
- Find out what computer safeguards are used by your child's school, the public library, and at the homes of your child's friends. These are all places, outside of your normal supervision, where your child could encounter an online predator.
- Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions.
- Instruct your children never to do the following:
  - Arrange a face-to-face meeting with someone they met online
  - Upload (post) pictures of themselves onto the Internet or online service to people they do not personally know
  - Give out identifying information such as their name, home address, school name, or telephone number
  - Download pictures from an unknown source as there could be sexually explicit images
  - Respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing
  - Not to believe that whatever they are told online; it may or may not be true

Adapted from Federal Bureau of Investigation (FBI). *A parent's guide to Internet safety*. FBI Publications Web site. Available at: <http://www.fbi.gov/publications/pguide/pguide.htm>. Accessed August 23, 2004.

Stimulating public interest and involvement is important, but investigators should be familiar with organizations formed by private citizens to help fight child exploitation on the Internet. Though the mission of such groups is admirable, investigators in some countries, including the United States, have encountered difficulties (eg, insufficient information, the improper handling of potential evidence) when working with these groups. Most alarming is the activity of some unauthorized members who go against the principles of the group to conduct their own Internet investigations, thereby opening themselves to potential criminal liability. Sadly, some agencies have seen members of these organizations use their affiliation as a cover or alibi when

being prosecuted for violations of the law. Since background investigations or references are not required of their members, a person with a criminal history or poor morals will usually not be discovered until it is too late. Investigators are reminded to consider this when receiving complaints from the Internet community.

### A NEW AREA TO PATROL

#### IDENTIFYING SUSPECTS AND POTENTIAL CRIME AREAS ON THE INTERNET

Law enforcement personnel should think of the Internet as a new type of community that should be patrolled for crime. This is especially true when comparing an Internet investigation to a more well-known type of criminal investigation (eg, a drug investigation). For example, a drug investigator's typical day is comprised of looking for "bad" people or patrolling "bad" areas. (In this chapter, a "bad" person or area is considered a person or place "predicated" or predisposed to commit a crime.) In most countries, predications about who or what area is bad allow investigators to begin the process of identifying, investigating, and arresting suspects who have become known to law enforcement officials by citizen complaint, forensic evidence, or through undercover techniques, where legally acceptable (Table 26-3).

Table 26-3. Examples of Predication

PREDICATED LOCATION	PREDICATED PERSON
— Chat room name:	— Citizen complaint:
— littlegirlsexchat	— "He is saying sexual things to my son."
— underage_boy_pics	— "He tried to meet my daughter online."
— File names:	— Criminal history:
— lolita	— Registered sex offender and known
— 8yo	suspicious Internet use
— Twinks	
— illegal teen	

Law enforcement officials patrol bad areas to gather intelligence information for future investigations. In Internet investigations, investigators obtain this information by reading material posted on the Internet by potential abusers and by monitoring known, predicated areas that draw potential abusers. The resulting intelligence helps identify the bad people who posted the recovered information. In addition, investigators may predicate suspects from citizen and/or parent complaints. As a result of the sheer volume of information and areas on the Internet, information received from technical and professional sources helps focus the investigators' limited resources as they search for suspects regardless of the way in which these suspects were initially predicated. Since most countries lack laws requiring ISPs to provide information useful to law enforcement officials, such assistance from outside sources helps. As a result of working together, positive, friendly relationships are encouraged between law enforcement officials and information technology employees.

#### PROSECUTION OF SUSPECTS

Regardless of the way a suspect was identified, whenever possible, investigators are urged to prosecute the suspect in the jurisdiction in which he or she resides in order to facilitate the potential identification of other victims. Prosecution in the suspect's place of residence generates the greatest amount of community impact through media and neighborhood attention. Such attention helps increase public awareness about this crime problem and potentially reaches families so that future victimization of this kind may be prevented.

Since the Internet community is global, if a suspect is believed to live in another country, investigators are encouraged to refer these suspects to the appropriate law enforcement agencies. A suspect who commits an offense in North America one moment could easily commit the same type of crime in Europe moments later without changing his or her physical location. Working on international cases or multistate investigations is challenging because of differing laws and investigative procedures; however, the virtual mobility of the Internet offender and the various information and resources necessary to conduct Internet investigations require investigators to work together.

#### INVESTIGATION TASK FORCES

Even when working with a local investigation, investigators must pool their investigative skill and resources, which has led to expansive use of the task force concept. Task forces, which include members of multiple agencies and jurisdictions, ensure the best chance of identifying and arresting offenders and the proper sharing of expensive computer and labor resources as well as the resultant criminal intelligence that develops from the work performed. An effective task force has key resources and members available though sometimes one person may have to perform many of these roles simultaneously, as is the case with a smaller task force (Figure 26-1). Task force members should include the following:

- Coordinators who serve as liaisons between other task force members and law enforcement agencies
- Computer forensics examiners who review the deluge of equipment and media seized from suspects and victims
- Intelligence analysts who interpret the case evidence, digital or otherwise
- Attorneys who are knowledgeable in this area and can readily interpret the rapidly developing area of computer and Internet law
- Child interviewers who are skilled in working with child victims
- Victim and witness specialists who help protect the welfare of child victims and maintain the integrity of the case

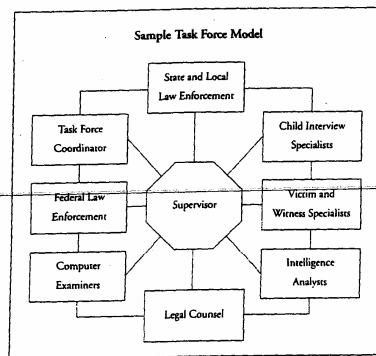
Some investigators may feel helpless to create such a task force; however, the same virtual mobility the offenders seek on the Internet can be used to create a local or regional task force or work group in which the members do not necessarily need to occupy the same office space. Though sensitive case or victim information should *never* be transmitted via the Internet without appropriate security precautions, the use of e-mail and other Internet services for less sensitive information can reduce the need for face-to-face contact, thereby helping to make such virtual work groups effective.

Whether a task force is large or small, local or regional, or real or virtual, most realize that a single group can not handle all of the local complaints received from the public, let alone the national and international Internet child exploitation complaints received.

In an effort to meet these obligations on a national basis, many countries have established centers to serve as national collection points for Internet complaint information.

In the United States, the joint publicly and privately funded National Center for Missing & Exploited Children (NCMEC) serves this function. All NCMEC functions are specific to crimes against children, including the NCMEC's CyberTipline for Internet child exploitation complaints.

Figure 26-1. Various roles in a sample task force.



In other countries, these centers may handle other Internet crimes as well as child exploitation crimes. In some countries, a government agency runs the hotline, and other countries have a private interest group, which cooperates with government officials, monitoring and maintaining the hotline (as is the case with the NCMEC). Whether run by a government agency or a private interest group, information centers can be a useful resource to all investigators. Regardless of the information center's size, the investigators, and especially the first responders, must make the case to save the victimized children.

#### ROLE OF THE INVESTIGATOR

Understanding the basic concepts presented in this chapter will enable investigators to work effectively and efficiently with other cybercrime investigators but will not qualify investigators to work proactively online to seek suspects or perform the computer forensic work necessary for case prosecution. These areas are specific disciplines that require extensive training; an unprepared investigator would do more harm than good. Rather, investigators should use the information provided in this chapter to ask the right questions of suspects, victims, and witnesses and to learn where to find the right information and evidence to begin an investigation.

### INTERNET BASICS

#### TRADER AND TRAVELER CASES

Internet child sexual exploitation complaints typically comprise 2 violations:

1. Complaints about child pornography
2. Complaints about people attempting to meet children via the Internet for sexual exploitation purposes

These crimes are sometimes referred to as *trader* and *traveler* cases, respectively. These terms are admittedly too kind when compared to the ghastly crimes they represent. In fact, many investigators worldwide no longer use the term *child pornography* and instead use the term *child abuse images* since it more accurately describes this crime, which perpetuates the abuse of the child victim long after the images are taken.

While most countries have recognized this and have adopted laws prohibiting the production, transmission, and possession of child pornography (Table 26-4), the use of the Internet to meet children for sex may not, by itself, be a violation in many countries. Even in such countries, however, if the suspect is successful in his or her attempt to meet a child and engages in sexual activity, he or she will be prosecutable under relevant sex offense laws and the potential for Internet evidence can not be overlooked.

#### LOCATING EVIDENCE

If investigators are called to identify a trader or traveler, they must know where to look and how to find the necessary evidence. If the Internet is patrolled as another crime area, as previously suggested, investigators must understand what this Internet "neighborhood" looks like. This can be a bit confusing because no single entity owns or runs the Internet.

The Internet Corporation for Assigned Names and Numbers (ICANN), a multinational organization, performs many of the Internet's managerial functions, such as the assignment of Internet protocol address block assignments and the design and adoption of Internet naming standards, as their name implies. The ICANN took over these functions from the United States-led Internet Assigned Name Authority (IANA). Despite this change, many people believe the Internet remains unduly dominated by the United States. While the ICANN and other Internet managerial bodies typically control key parts of this infrastructure, most widely used services on

Table 26-4. Countries That Submitted Information on Exploitation Laws to Interpol

A	B	C	D	E
— Albania	— Bahamas	— Cambodia	— Denmark	— Ecuador
— Andorra	— Bahrain	— Canada	— Djibouti	— Egypt
— Argentina	— Barbados	— Chile	— Dominican Republic	— El Salvador
— Armenia	— Belarus	— China (Hong Kong)	— Dominica	— Estonia
— Australia	— Belgium	— Colombia		
— Austria	— Bolivia	— Costa Rica		
— Azerbaijan	— Bosnia Herzegovina	— Côte d'Ivoire		
	— Botswana	— Croatia		
	— Brazil	— Cuba		
	— Brunei	— Cyprus		
	— Burundi	— Czech Republic		
F	G	H	I	J
— Fiji	— Georgia	— Honduras	— Iceland	— Jamaica
— Finland	— Germany	— Hungary	— India	— Japan
— France	— Gibraltar		— Indonesia	
	— Greece		— Ireland	
	— Guatemala		— Israel	
	— Guinea		— Italy	
	— Guyana			
K	L	M	M	O
— Kazakhstan	— Latvia	— Macao	— Namibia	— Oman
— Kenya	— Lebanon	— Malta	— Nepal	
	— Lesotho	— Mauritania	— Netherlands	
	— Liechtenstein	— Mauritius	— New Zealand	
	— Lithuania	— Mexico	— Norway	
	— Luxembourg	— Moldova		
		— Monaco		
		— Mongolia		
		— Myanmar		
P	R	S	T	U
— Pakistan	— Romania	— St. Kitts & Nevis	— Tanzania	— Ukraine
— Panama	— Russia	— Senegal	— Thailand	— United Kingdom
— Peru		— Singapore	— Trinidad & Tobago	— United States
— Philippines		— Slovakia	— Tunisia	— Uruguay
— Poland		— Slovenia	— Turkey	— Uzbekistan
— Puerto Rico		— South Africa		
— Portugal		— Spain		
		— Sri Lanka		
		— Swaziland		
		— Sweden		
		— Switzerland		
		— Syria		
V				
— Venezuela				

Specific legislation can be viewed at and table adapted from Legislation of Interpol member states on sexual offences against children. Interpol Web site. Available at: <https://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/Default.asp>. Accessed February 21, 2005.

the Internet follow a commonly accepted protocol that is specific to each service. New protocols are usually first described in Request for Comments (RFC) documents. These RFCs are formal papers that guide the evolution of the Internet upon their acceptance and adoption. The major services currently in public use on the Internet include the following:

- World Wide Web (WWW)
- Internet Relay Chat (IRC)
- Electronic mail (e-mail)
- Usenet newsgroups
- File Transfer Protocol (FTP)
- Web-based chat (WBC)
- Messengers
- Peer-to-peer (P2P) networks

Each of these areas facilitates different types of communication but all can foster child sexual exploitation. To investigators, the major difference between these areas is the information that must be obtained through interviews or physical evidence, which enables a suspect to be located. As the Internet evolves, these services will evolve, and others will be added. As a result, investigators must remain abreast of these changes to conduct investigations properly. To maintain compatibility among computer operating systems on the Internet, all existing and emerging services generally comply with the Transmission Control Protocol (TCP) and/or Internet Protocol (IP). Advanced Internet investigators should have a grasp of these TCP/IP concepts.

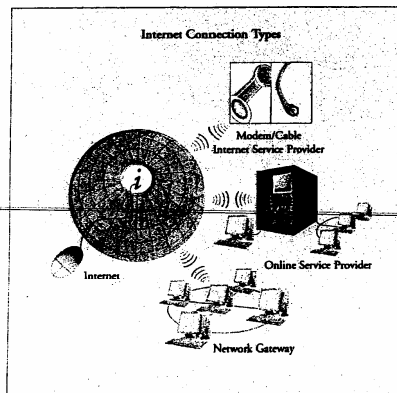
Regardless of the service used, an Internet user must connect to a point-of-presence (POP) and obtain an IP address, which is essentially a unique number that identifies a particular computer to others on the Internet. Users of the Internet primarily connect via one of the following 3 means (Figure 26-2):

1. A modem or cable modem and an ISP
2. An online service provider that allows an Internet connection
3. An Internet gateway provided by a corporate, government, library, education, or other computer network

All of these connection types have seen massive increases in bandwidth in recent years. Increased transmission speeds, resulting from broadband services, such as Digital Subscriber Lines (DSLs) and cable modems, have increased the potential damage that can be done to child victims. Greater numbers of child pornography images and even full-motion video images can be easily transmitted on the Internet, thereby creating permanent records of the child and causing repeated, perpetual victimization.

Fortunately, users of these connection methods, including broadband services, can usually be traced to their origin and identified to stop the abuse. When conducting such investigations, the primary concern is whether Internet records are available to follow the trail from the user's online identity to his or her true identity. Depending on which Internet service is being used, investigators need to obtain different information to begin this identification process (Table 26-5). Not all information is necessary to trace the offender successfully; however,

Figure 26-2. People connect to the Internet through a modem or cable modem and an ISP, an online service provider that allows an Internet connection, or an Internet gateway provided by a computer network.





<p><b>WORLD WIDE WEB (WWW)</b></p> <ul style="list-style-type: none"> <li>— Uniform Resource Locator (URL) (ie, Internet address)</li> <li>— Domain name or Internet Protocol (IP) address</li> <li>— Hosting</li> <li>— Connection</li> <li>— Domain name system (DNS) provider(s)</li> </ul> <p><b>ELECTRONIC MAIL (E-MAIL)</b></p> <ul style="list-style-type: none"> <li>— Complete Internet message headers (ie, full or advanced header, not just basic "To" and "From" lines)</li> </ul> <p><b>FILE TRANSFER PROTOCOL (FTP)</b></p> <ul style="list-style-type: none"> <li>— IP address</li> <li>— Date</li> <li>— Time</li> <li>— Time zone</li> <li>— Nickname</li> <li>— Advertised location, if any</li> </ul> <p><b>MESSENGERS</b></p> <ul style="list-style-type: none"> <li>— Online identity (ie, screen name, identity name, or unique number)</li> <li>— Chat room(s) used</li> </ul>	<p><b>INTERNET RELAY CHAT (IRC)</b></p> <ul style="list-style-type: none"> <li>— IP address</li> <li>— Date</li> <li>— Time</li> <li>— Time zone and/or nickname</li> <li>— Server</li> <li>— Channel(s) used</li> </ul> <p><b>NETWORK NEWS TRANSFER PROTOCOL (NNTP)</b></p> <ul style="list-style-type: none"> <li>— Complete Internet message headers (ie, similar to but different from e-mail headers)</li> <li>— Posting nickname(s) and group(s)</li> </ul> <p><b>PEER-TO-PEER (P2P) NETWORKS</b></p> <ul style="list-style-type: none"> <li>— IP address</li> <li>— Date</li> <li>— Time</li> <li>— Time zone</li> <li>— Network, program, and online identity used</li> </ul> <p><b>WEB-BASED CHAT (WBC)</b></p> <ul style="list-style-type: none"> <li>— Online identity (ie, nickname) used by suspect</li> <li>— Web site(s) and chat room(s) used</li> </ul>
--	--

<ul style="list-style-type: none"> <li>— Pretext calls</li> <li>— Phone records</li> <li>— Interview/Interrogation</li> </ul>	<ul style="list-style-type: none"> <li>— Surveillance</li> <li>— Trap and trace</li> </ul>
---	--

the likelihood of success increases with more complete and accurate information.

Investigators must remember that the computer is an instrument used in this type of crime and not an end in itself. When the identification of a suspect through Internet means alone is unclear or needs further supporting evidence, investigators should rely upon more traditional investigative techniques to help identify the perpetrator behind the keyboard (Table 26-6).

**WORLD WIDE WEB**

The World Wide Web (WWW), or "Web" for short, is most users' introduction to the Internet. In fact, most people perceive that the Web is the entire Internet and remain oblivious to the other services available. The Web is easy to use, which has resulted in a high rate of use among all age groups; however, from an investigator's point of view, the Web can be difficult to master.

The Web is largely comprised of billions of pages of information that provide everything: basic text, images, movies, music, and even software. Usually, multiple pages are organized to form a Web site. Every page and element within the Web site has an Internet address, or Uniform Resource Locator (URL), that defines its location on the Web. By simply following a hyperlink on any page, users can be taken to other locations to view other Web content. This content can easily originate from a country other than that of the user even if the user is unaware. In fact, a single Web page is

often comprised of content from multiple states or countries, thereby complicating Web site investigations.

**HYPERTEXT TRANSFER PROTOCOL**

A knowledgeable Internet user may recognize the commonly used term Hypertext Transfer Protocol (HTTP). Though often listed with a Web page address, HTTP means little to the average user even though HTTP is the essential means by which Web pages are transmitted for viewing. This is probably because the HTTP portion of a Web address does not usually need to be included in a Web browser to find the page and is often omitted. Likewise, the term WWW is often redundant, unnecessary, and unused. The information that flows over HTTP on the WWW includes the Hypertext Markup Language (HTML) programming code and the contents of other files related to the Web site being viewed (Figure 26-3). This code and all files related to the Web site can be useful to investigators as they search for the necessary information to trace the Web site and identify the responsible party.

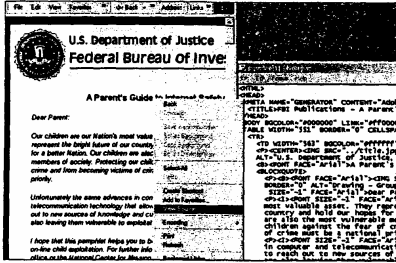


Figure 26-3. Screen capture from the FBI Web site and the related HTML source code.

**PROBLEMS INVESTIGATORS CONFRONT**

Previously, the Web was not widely used for child pornography because of the ease of determining the person(s) responsible for the content. Usually, this determination was not because of the HTML code but because of log files and billing records. Unfortunately, this has changed because of free Web hosting and the complexity of the Web pages themselves. Adding to the confusion is the process of Web page redirection. This redirection may cause an Internet user to be unaware that the Web page address selected for viewing is not the one being viewed. Another problem with Web site investigations is that multiple suspects can be responsible for a single page or site. This is especially true with a type of Internet service known as a virtual community, which is often referred to as a Web club, e-group, or Web community. In a virtual community, single Web sites can contain content posted by multiple members of the club who are usually offered free and unverified memberships. In other words, a single Web page may contain content originating from multiple domestic suspects or even suspects from other countries who have provided little or no true identity information.

**INFORMATION HELPFUL TO INVESTIGATORS**

The minimum information necessary to begin a Web site investigation includes the URL of the site, including the domain name and as much information about the content's actual location as possible. Investigators find a printout of the Web site contents helpful. Ideally, an investigator has a copy of the Web site contents saved to a diskette since the contents can provide useful information in the HTML code and related files. From this information, an Internet investigation specialist can locate the registrant of the domain name, the host of the content, the ISP providing the Internet connection to the content (often the same as the host), and the ISP providing the domain name system (DNS) entry for the Web site (Figure 26-4). Although these components are the keys to a successful Web site investigation, bogus registration information and frequently changing international hosts and connections have been a challenge in many attempts to dismantle child exploitation Web sites. Investigations of virtual communities have been more successful, mostly because the Web site host can provide other information that is useful in tracing the offenders.

Whether for basic Web site investigations or for an investigation of a Web site that hosts a virtual community, an accurate URL must be obtained in a timely fashion, or the investigation will be over before it has begun. The complexity of URLs can seem difficult to investigators, but this need not be the case. In the following examples, an

Figure 26-4. Web site components help investigations by providing keys to identify the creator of a site.

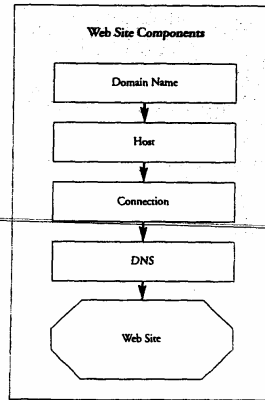


Table 26-7. Generic Top-Level Domains and Their Typical Uses

.biz	Business
.com	Commercial
.edu	US educational institutions
.gov	US government
.info	Informational
.int	Established by treaty
.mil	US military
.net	Internet infrastructure
.org	Nonprofit organizations

*Note: In the case of all but the ".edu," ".gov," ".mil," and ".int" domains, the use of the gTLD is generally at the discretion of the domain's registrant. This means that a Web site registered as ".org" may not be a nonprofit entity, one registered as ".net" may not be an Internet infrastructure component, and so on.*

investigator would be interested in the top-level domain (TLD), that is, "anyisp," as the proper ISP to begin the investigation:

- http://www.anyisp.com
- http://www.anyserver.anyisp.com
- http://clubs.anyisp.com/preteensex
- http://clubs.anyisp.com/html/93000673/73012486/club?target=preteensex

In each of these examples, "anyisp.com" is referred to in the domain name portion of the Internet address, which includes the ".com" portion [also known as the generic top-level domain (gTLD)]. For US domain names, the domain name is always the portion of the address directly before the gTLD and includes the gTLD itself. Current, common gTLDs and their typical uses are listed in Table 26-7.

Since the Internet is a global entity, a method is available to determine a Web site's possible country of origin. A domain can be registered with a country code top-level domain (ccTLD) in which the domain name is augmented with the 2-letter country identifier. For example, "http://www.anyisp.co.uk" would be the Internet address for "anyisp" in the United Kingdom; "anyisp.co.uk" is the ccTLD in this example. Country identifiers may

or may not describe the country of origin, however. Since most Internet registrars do not verify registration information, a domain registrant can often choose to register in a country different than the ccTLD of the Web site's domain. As a result, ccTLDs may not be entirely useful in locating an offender, but a basic knowledge of ccTLDs is often helpful for investigators. Table 26-8 lists examples of country code identifiers.

**INTERNET RELAY CHAT**

Internet Relay Chat (IRC) is accessible to all Internet users although many people may not be aware of this. By using appropriate software, users can connect to an IRC network server (Figure 26-5). Users then become connected to a particular network in which real-time "chats" with other users worldwide can be conducted in a "chat room." Thousands of Internet chat rooms exist. Each is referred to within IRC as a channel.

In addition to providing chat rooms, IRC allows for private conversations and the private exchange of files without the use of e-mail. Through a process known as a *file server (f-serve)*, automated file exchanges can be accomplished.

As with all other Internet services, IRC can be used by legitimate users for legitimate means but can be abused by those seeking to exploit children. Major ISPs allocate server space to IRC and do not attempt to manage the content. As a result, no one owns IRC, and users are free to create whatever channels they wish to meet others, chat, and/or trade files. Unfortunately, IRC is perceived as a nearly risk-free environment for Internet users who believe they are free to do whatever they want, when they want.

For law enforcement officials to identify suspects on IRC, they must obtain a great deal of specific information. First of all, a user's IRC nickname, or the online identity of the user, should be obtained. This information alone is insufficient to determine a user's identity since IRC users can change their nicknames instantly. To be certain about a user's identity, an investigator must have the IP address of the user as well as the date, time, and time zone of the connection. Though such information is usually easily obtained via IRC software, complaining parties rarely have this information. As

Table 26-8. Country Code Identifiers

.au	Australia
.be	Belgium
.ca	Canada
.cc	Cocos (Keeling) Islands
.cr	Costa Rica
.de	Germany
.es	Spain
.fr	France
.ie	Ireland
.jp	Japan
.ky	Cayman Islands
.nl	The Netherlands
.nu	Niue Islands
.py	Paraguay
.ru	Russia
.se	Sweden
.tv	Tuvalu

a result, investigators may need to obtain more general information (eg, IRC network and server to which the suspect was connected, the channel(s) used by the suspect) to locate the suspect. As with all Internet evidence, anything saved to disk will likely be more useful than printed items, so investigators should be sure to obtain disks from complainants and victims whenever possible. Table 26-9 presents a sample of IRC channels and their descriptions, which are created by and available to IRC users.

**ELECTRONIC MAIL**

Electronic mail can be sent from and received within virtually any paid ISP account as well as via many free e-mail services (eg, Yahoo!, Hotmail), which are available to people who have an Internet connection. Although an increasing number of people are using free e-mail services and Web browsers to view their e-mail, this e-mail service is not really a Web function.

As with other Internet services, e-mail operates via its own set of protocols. The common protocols for e-mail are Simple Mail Transmission Protocol (SMTP) for sending e-mail and either Post Office Protocol (POP3) or Internet Message Access Protocol (IMAP) for receiving e-mail. Again, most users are unaware of the technical nature of e-mail; they view e-mail as only an exchange of text and files between the addressed Internet users.

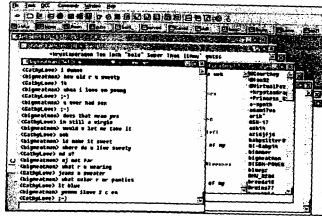


Figure 26-5. Screen capture of a software program that is used to access IRC.

Table 26-9. Sample Internet Relay Chat Channels and Their Descriptions

CHANNEL NAME	DESCRIPTION
#0!!!!!!!!!!!!12yrolsex	[-Roleplay-Cybersex-&-Porno-]
#0!!!!!!!!!!!!preteen101	Welcome to 101—on-topic material
#0!!!!!!!!!!!!preteen00	We're open again, and doing great
#0!!!!!!!!!!!!littlekidsex	WelCome...16yo and younger cum play
#0!!!!!!!!!!!!mom'n'sonsex	#1 Place 4 Moms
#0!!!!!!!!!!!!pedomoms	Men who love women and their kids
#0!!!!!!!!!!!!family_lovers	A Real family love channel
#0!!!!!!!!!!!!dad&daughtersex	Come in and Chat...16+ Fantasy Only
#0!!!!!!!!!!!!preteenrapsex	Roleplay-Cybersex-&-Porno
#0!!!!!!!!!!!!childslavesex	For those that love young slaves
#0!!!!!!!!!!!!forcedfamilysex	Fantasy Sex—Come in and play—16+
#0!!!!!!!!!!!!littleboysexchat	For boys and boy-lovers
#0!!!!!!!!!!!!idgirlsexchat	Where Young Girls get lots of loving
#0!!!!!!!!!!!!childsexchat	Where the kids are sexually active

Note: The exclamation point (or "bang") in the channel names results in these channels being sorted to the top of a computer alphabetized list. Since this is an example, most IRC channels at the top of such a list are related to child sexual exploitation.

that e-mail information that is commonly seen by most users (e-mail "from" information) can be easily altered by using a spoof or remailer. Furthermore, most free e-mail accounts can be created using false user information or no information at all. Currently, e-mail "spam" exploits these vulnerabilities and has become a major scourge of the Internet; e-mail spam goes well beyond the simple annoyance of a clogged inbox. In fact, the use of spam e-mail as a delivery system for online security threats is considered a future threat to the Internet itself.

Tracking spam, which includes tracing messages that offer child pornography, has become incredibly difficult. In contrast, most personally addressed e-mail is easier to trace by using the more reliable information related to e-mail transmission, which is found in the message's header.

If a complainant or investigator has a copy of the message text but not the header information, then the entire message may be obtained if that message remains stored on the mail server of the user's ISP. When in doubt, investigators should contact a properly trained investigator to help save the e-mail message to a disk since a printout alone may be insufficient to trace the message.

Unfortunately, increased public knowledge regarding the ability of law enforcement officials to trace e-mail messages, in addition to the recent use of systems that can monitor e-mail in real time by law enforcement officials, has sparked a growing interest in "secure" e-mail services (eg, Hushmail, SafeMessage, ZipLip). The names of these services clearly indicate they are designed to ensure the privacy of e-mail, thereby complicating the investigator's role. These services are rarely used for child exploitation offenses, however, and most e-mail remains easily traceable if a true copy of the e-mail and the message's header information is obtained.

#### USENET NEWSGROUPS

Usenet newsgroups can be thought of as virtual bulletin boards on which messages containing text and computer files are posted for public exchange. Newsgroups are continuously updated by users worldwide and are usually not monitored by the ISPs that host them. More than 90 000 known newsgroups currently exist. These newsgroups serve legitimate and illegitimate topics. Because of the lack of monitoring and sheer volume of groups and postings, newsgroups are thought of as yet another "risk-free" Internet service for the posting and downloading of child exploitation materials.

Dedicated investigators can be on the winning side of this problem though. Newsgroup postings are maintained at ISPs for a matter of days or weeks and then may become available to download and trace to the user who posted the information, thereby providing valuable information to quick-acting investigators. Many ISPs will not carry some of the most heinous newsgroups; therefore, people interested in such groups must pay for a private newsgroup service. To conduct this type of investigation, investigators who want to fight members of such newsgroups must also pay for this private service.

---

As with other Internet services, posting and downloading content on newsgroups follows a protocol. In the case of newsgroups, the protocol is called Network News Transfer Protocol (NNTP).

As with e-mail, most newsgroup postings can be easily traced by careful analysis of message header information, which can be used to identify the authoring account (Figure 26-6). The analysis of newsgroup headers can be challenging, so investigators are urged to obtain a copy of the posting's complete message header for later analysis. Usually, if information such as the posting host and date, time, and time zone stamp are obtained from saved evidence, the user can be traced; however, various portions of a message header may be forged. For this reason, ISPs may use different portions of a

message header to determine the authoring account. As a result, an investigator's best course of action is to provide the ISP with the entire message header if possible. Even if the suspect posting is no longer available to be downloaded and investigated, knowledge about the poster's online identity, the subject description of the postings, and the newsgroup to which the message is being posted can help locate the suspect. A small sample of child sexual exploitation-related newsgroups available on Usenet is presented in Table 26-10.

**FILE TRANSFER PROTOCOL**

Programs that use File Transfer Protocol (FTP) are still widely used by people who trade child pornography even though newer, more powerful programs exist. Users of any of the previously mentioned services (eg, World Wide Web, IRC, or newsgroups) may encounter Web pages, IRC messages, and newsgroup postings that offer FTP services (Figure 26-7). An FTP advertisement typically includes the IP address of the FTP server in addition to the username (ie, nickname) and password needed to connect to the server.

Like many Internet child exploiters, advertisers of FTP servers almost never charge for their services and are usually individual users operating an FTP program on their home, work, or school computer in an effort to propagate child pornography. Though this effort can require advertisement to others, hundreds and perhaps thousands of servers are probably operating secretly on the Internet at any given time.

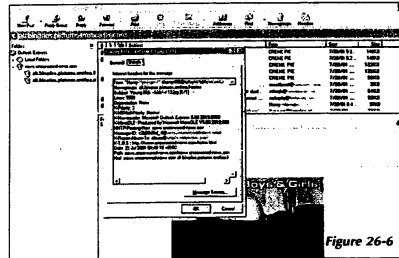


Figure 26-6

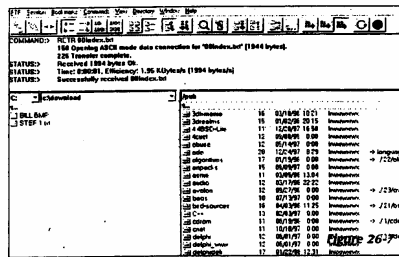


Figure 26-7

**Table 26-10. Newsgroups Related to Child Sexual Exploitation**

Newsgroup names are usually broken into segments that allow users to ascertain some information about the newsgroup's topic. The following provide examples:

- alt.binaries.pictures.erotica.age.13-17
- alt.binaries.pictures.erotica.child
- alt.binaries.pictures.erotica.child.female
- alt.binaries.pictures.erotica.child.male
- alt.binaries.pictures.erotica.lolita
- alt.fan.yarbird
- pedo.binaries.pictures.erotica.pre-teen

Newsgroups with clandestine names as well as privately circulated newsgroups also exist. For the descriptive newsgroups listed above, the following definitions are provided:

- alt alternative
- binaries binary data
- pictures picture files
- erotica erotic or sexual content
- pedo pedophilic content

Figure 26-6. Screen capture of a newsgroup posting with full headers displayed

Figure 26-7. Screen capture of a program that allows the use of FTP.

Once connected to an FTP server, users may upload and download files, including child pornography images. Similar in operation to an f-serve on IRC, FTP servers usually require users to upload images to receive credit to download others.

### WEB-BASED CHAT

In recent years, many users have taken to Web-based chat (WBC), or chat, which functions within a Web browser. WBC is popular because it is easy to use when compared with paid services provided by online service providers (eg, America Online [AOL]) and free services like IRC chat. Chat within a Web browser is accomplished by using small programs (known as *applets* or *scripts*) downloaded by the user to the computer browser. As in IRC, Web-based chat online identities or nicknames are easily changed. Even more challenging for investigators, though, is that the evidence of chat rooms visited and messages sent and received are usually not logged because these chats occur within the Web browser. This means that though IRC and WBC have legitimate uses, some unscrupulous users have flocked to them in particular since a record of their communication is not maintained unless intentionally kept by the sender or receiver. In other words, the computers of many suspects and victims might not show obvious signs of them having used these services.

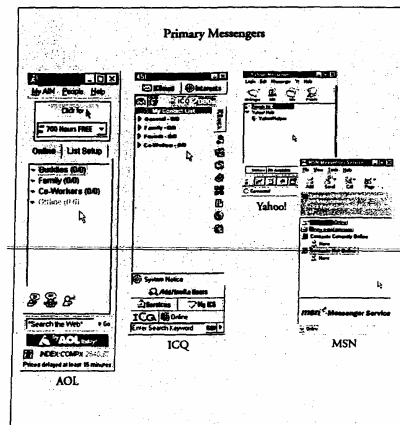
Web-based chat that incorporates Voice over IP (VoIP) further complicates this problem for investigators. As used in a Web browser, VoIP allows users to talk to one another rather than typing their chat. Whether via VoIP or regular chatting, tracing a user of WBC requires knowledge of the nickname or other online identity being used by the user as well as a specific location of the chat since one Web site can host thousands of different chat rooms. Investigators must work quickly on WBC cases because the logs to trace offenders may expire within hours or days if such logs are kept at all.

### MESSENGRERS

Another rapidly growing area of use on the Internet is that of *messengers*, which are free, standalone software programs offering users the ability to instant message one another, create private or multiuser chat rooms, and send messages to and from properly equipped cellular telephones. The most popular of these messengers are ICQ (also known as *I Seek You*), AOL Instant Messenger (AIM), Yahoo! Messenger, and Microsoft Network (MSN) Messenger (Figure 26-8). Millions of people use these products as online Internet "buddy" locators or as a way to find friends to chat with as well as powerful file transfer programs. Most people support some form of voice and video chat or VoIP. Many functions of the messenger programs are being built into Internet-based game software that include real-time chat between worldwide participants. Unfortunately, most parents will not realize the potential harm of such games since their sole understanding of the Internet is that of the Web browser. As a result, this concept will likely prove especially risky for unsupervised children.

The information necessary to locate the user of a WBC or messenger program varies depending on the type of service used. Usually a nickname or other online identity (eg, a unique, identifying number) is sufficient; however, more specific information (eg, e-mail address, IP address) may be available. Investigators should be particularly specific and thorough when dealing with these services since one piece of information may be the difference between identifying or missing a targeted subject.

Figure 26-8. The 4 primary messengers include AOL Instant Messenger, ICQ, Yahoo! Messenger, and MSN Messenger.



## PEER-TO-PEER NETWORKS

Currently, a relatively new variant of Internet programs known as peer-to-peer (P2P) networks are some of the most hotly debated. The term *peer-to-peer network* refers to 2 or more computers directly connected to one another without the aid of a central server. However, P2P has become more widely associated with Internet P2P programs, which make file sharing easy for the masses.

Though most of the media rhetoric concerns on the protection of intellectual property rights and copyright enforcement are outside the scope of this chapter, investigators should be aware that, if left unchecked, no other area on the Internet seems to have as much future damage potential in terms of child pornography.

Programs such as Gnutella, WinMX, eDonkey, Morpheus, and KaZaA that run on the major P2P networks have the potential to propagate child pornography and frustrate even the most highly trained investigator. As parents strive to recognize the new "danger areas" for their children, these programs pose a great problem. This is because most of these programs show only an icon in the system tray on a Windows-based computer. This means that the program icon will show up only in the area near the computer's clock rather than on the taskbar at the bottom center of the screen where most users, including parents, expect to see icons.

When running a P2P program, users are not usually connected to other users via a central network; rather, they are directly connected to one another (hence the term *peer-to-peer*). All users can share files with one another, thereby allowing an unlimited ability to download and upload computer files, including software, music, images, and video. Since users have a direct connection to each other, criminal file transfers (eg, child pornography) are difficult to trace without a direct connection between an investigator downloading and the person uploading these file transfers. Furthermore, since file transfers can occur only when users are connected to the program (unlike a Web site or newsgroup posting that may remain up for days or weeks), the amount of time available to investigators to look into a P2P complaint may be small. Perhaps worst of all, the latest variants of these programs, known as *distributed P2P*, allow a user to simultaneously download a desired file from multiple users, thereby distributing the download among 2 or more computers. Distributed P2P greatly complicates investigations.

The description of this technology makes it seem impossible to investigate. However, successful investigative methods have been developed and are in use. Like most areas mentioned in this chapter, investigators are especially urged to leave active, online investigations of P2P to properly trained investigators. These trained investigators have the best chance of possessing the technical knowledge to solve such cases as well as a proper undercover computer and Internet connection with which to conduct such an investigation. Investigators seeking the ability to conduct P2P investigations should consult a properly trained online investigator who is currently working such cases for guidance in this important, emerging threat area.

The basic information needed to trace an offender includes the P2P network, program, and nickname used by the offender; however, this information can be used only to locate the offender when he or she is online. Additional information (eg, IP address information) can be obtained.

## OTHER FUTURE THREATS

With such a large list of Internet concerns, it is difficult to imagine investigations becoming more difficult, but that seems to be the case. The Internet is rapidly being integrated into all aspects of interpersonal communication. A convergence is occurring, and some services may be contracting or ceasing existence, but more continue to emerge (eg, P2P) and replace these services.



Another reemerging threat is use of VoIP for Web-to-telephone calls. With such calls, one user uses the computer to make a call to another user's telephone. Currently, many Web-based phone call service models are returning after losing their users in the shift from free-usage business models to fee-for-service models. Many users of such services chose not to pay for a service they perceived as free, but the technology has improved and become more reliable. This technology will likely be adopted in the future, thereby increasing the risk to children and hampering investigations.

Yet another concern is the rapid adoption of wireless technology. Improperly installed wireless home and business networks are ripe for unauthorized access and abuse by unintended users. Even a properly installed network is a threat because of the mobility this service provides an offender. The importation of the wireless feature into portable electronics (eg, mobile phones, personal digital assistants) exacerbates this problem.

Noteworthy is the integration of computers and other home media, such as television, music, and photography that combine Internet and other computer functions with a television. In the future, these devices will be potentially harmful since parents will be lulled into a false sense of safety and become more likely to allow children unsupervised Internet access.

#### ONLINE SERVICE PROVIDERS

Though most online service providers provide a connection to the Internet and the use of all other services mentioned in this chapter, an important and notable difference to investigators exists. Online service providers provide self-contained services exclusive to the subscribers. The 2 largest (AOL and MSN) provide services to more than 30 million users in the United States. Usually, online service providers offer the ability to create user "profiles" that may contain either true or false information about the user.

The real advantage to an investigator attempting to locate a suspect on an online service provider is that, unlike so many free services available on the Web (eg, free e-mail), these providers are usually paid services that provide some sort of verified information for investigators to use in locating a suspect. Investigators should be reminded, however, that maintaining the information is the services' prerogative and that few countries have laws requiring that these services maintain records useful to law enforcement officials. Some countries even have laws *preventing* the retention of such information or require the destruction of such information. This means that, as with ISPs, investigators should consider the long-term liaison relationship with online service providers and maintain decorum when dealing with them because a positive relationship may make the difference in developing an effective case.

#### INTERNET PROTOCOL ADDRESS "TRACING"

As previously described, the starting point for many Internet investigations is tracing an IP address or domain name to the responsible registrant. This information is usually available via public databases from organizations known as Regional Internet Registries (RIRs). The 3 major RIRs responsible for registration on the Internet include the following:

1. The American Registry for Internet Numbers (ARIN) is responsible for managing IP address numbers for the Americas and sub-Saharan Africa.
2. The Registrar for Internet Protocols in Europe (RIPE) is responsible for managing IP address numbers for Europe, the Middle East, the northern part of Africa, and parts of Asia.
3. The Asian-Pacific Network Information Center (APNIC) is responsible for managing IP address numbers for the Asian-Pacific region.

Each of these registries has its own Internet Web page for referencing the respective databases, so many investigators find it helpful to use the interface available at <http://www.sampade.org>, which was designed by security expert Steve Blighty. This site was originally set up to trace senders of spam and malicious computer hackers. In addition to a "whois" interface (ie, it identifies registration information provided by the owner of a second-level domain name who registered it with an RIR), this site also provides other tools to Internet investigators and hobbyists alike. A "whois" search performed on this site checks many international registries simultaneously for information about a given domain name or IP address.

Other ways exist to help track Internet information. For example, investigators can use third-party software to obtain IP address tracing and other Internet network information. For more technically minded investigators, some basic commands on a Windows-based computer can provide useful information.

Although locating IP and domain name information may appear easy when using Web sites, software, or even computer commands, investigators are warned that much of the information contained in the registry databases can be bogus and unreliable. Tracing Internet users is one of many technical challenges facing Internet investigators and is a primary reason for obtaining proper training before conducting such investigations.

#### THE IMPORTANCE OF TIME

Perhaps the most critical element and technical challenge of tracing offenders online is time. Just like any other crime, the chronology of events often links a particular suspect to a particular crime in Internet investigations. Investigators can rest assured that because of a system known as *Network Time Protocol (NTP)*, a protocol used to synchronize computer clock times in a network of computers, most of the times provided from ISP logs are usually accurate. This may not be the case, however, when dealing with a victim's or suspect's computer, or even the investigator's own computer. Most times provided by the computer to files (eg, chat logs, image files) are based on the system clock of that computer.

The time of this clock may be set accidentally or intentionally by the user to display an incorrect time. This means that it is critical for investigators to note the time displayed on the computer clock as well as any difference from the accurate, current time as part of a complete investigation (eg, most self-timing cellular telephones display an accurate NTP time). This time correction as well as any correction based on time zone and possibly daylight savings time can be used to compare critical events.

#### OTHER TECHNICAL CHALLENGES

Starting or exiting Windows or any other operating system, or even viewing or printing a computer file, changes the integrity of the evidence. As a result, investigators are cautioned not to tamper with original evidence; rather, investigators are encouraged to use working copies for analysis.

Likewise, a competent team leader and properly trained assistants should lead the search of a premise for computer and other related evidence. If possible, a certified computer examiner should be a part of the search team. Even a "simple" computer search can become complicated by the discovery of a home or business network with more than one computer or a computer connected to other, unexpected or unrecognized devices.

Furthermore, with searches conducted at a place of business or anywhere else that may have other potential, innocent users using the same network should be conducted to obtain the necessary evidence from the suspect's computer while protecting the work and the privacy of the rest of the employees. In this regard, information technology professionals at the suspect's place of employment can often serve as

valuable sources of information and assistance for the search team if those professionals are first ruled out as potential suspects or accomplices in the offense.

No matter what is searched and seized at the scene of a computer search, the evidence must be treated with caution and care. For proper analysis of computer evidence, seizure of the entire suspect computer system and related equipment is usually necessary to maintaining the chain of custody of all the seized items.

While investigators should strive to ensure that all technical matters are handled properly, they should not overlook other clues. Many successful cases have been made or assisted by the findings of such low-tech things as log books or notes containing online identities of the suspect or other victims, account numbers leading to additional evidence, or even printed images or chat logs kept by the suspect for reference or remembrance. Even if the offender does not make these mistakes and enlists the use of high-tech protections (eg, encryption or password protection), investigators should not rely on the hope that they may be able to "crack" or guess a password. Rather, these investigators should obtain the password from the suspect. No matter what the technical competence of the suspect, the most effective way to gain a confession and obtain other necessary information is with a thorough, well-conducted interview of the offender by an investigator familiar with all of the services and technology being used in the offense.

#### VICTIM IDENTIFICATION

During the past several years, an exciting development has been taking place with respect to identifying victims of Internet child pornography. In the past, if the previously described tracing techniques were used to identify a transmitter or possessor of child pornography but failed to identify the creator of the images, most investigators prosecuted the subject at hand and ignored the larger issue of identifying the producer. This worked fine to identify and prosecute many offenders but did little to help the victims being abused in the production of these images. Because of increased international cooperation and the proliferation of digitally produced child abuse images worldwide, many investigators find that it is rewarding to go beyond technical-tracing techniques and undertake the difficult work of using the clues provided in the images themselves.

Though this work can be technical and advanced at times, the work is based on the same 5 questions asked so often in any investigation (Table 26-11). Investigators can often find the answers to these questions in the child abuse images themselves.

The effectiveness of this investigative technique and the use of these clues depend upon several important assumptions. Most importantly, the assumption that national and international sharing of identified victim information will occur. If individual agencies and countries do not share this information, investigators will find themselves spending weeks analyzing the clues in a series of images to trace the offender and/or victim, only to find out that the victim is already safe. Though privacy issues need to be satisfied, all countries should find a law enforcement reason to share limited victim information such as the images themselves, the age of the child in the images, the name of the offender(s), and the circumstances of the abuse. Victim name information is not necessary and adds little or no value to subsequent investigative efforts, so the name should not be released or shared with others.

In the United States, the lead effort in victim identification is the multiagency National Child Victim Identification Program (NCVIP), which is a joint partnership among the Bureau of Immigration and Customs Enforcement (ICE), Federal Bureau of Investigation (FBI), US Postal Inspection Service (USPIS), US Secret Service, state and local police as represented by the Internet Crimes Against Children Task Forces, and the NCMEC, among other agencies. Members of the NCVIP partnership are coordinating their efforts with similar efforts being undertaken worldwide. These

Table 26-11. Primary Investigator Questions That Can Be Answered by Critically Observing an Image

QUESTION	POSSIBLE ANSWERS
Who	offender and victim face, gender, age, scars, marks, tattoos, jewelry
What	objects, logos, products, furniture, rooms
When	date and/or time on files or in images, seasonal clothing, calendars, decorations
Where	wiring, plumbing, language found on products, keyboards, clothing
How	one or more offenders, accomplice, use of self-timer

projects include work being done by the Trafficking in Human Beings Branch of the Interpol General Secretariat in Lyon, France, and a European Commission-sponsored project, which is bringing together representatives of Interpol, Europol, the European Commission, the Group of Eight Nations (G8), member nations, and several other countries known for expertise in victim identification (specifically, Sweden, Denmark, and the Netherlands). All of these efforts seek to build on the experiential knowledge of countries, such as Sweden, whose national police have led victim identification efforts worldwide and serve as the basis for the Interpol and G8 work in this area.

Regardless of the agency conducting the investigation, another important assumption in victim identification is that a sufficient number of images exist to be analyzed. Many of the stand-alone images contain few, if any, of the clues listed in Table 26-11; however, a series of images may develop many clues, especially when these images are reviewed as a related series.

To help relate one series to another, leading law enforcement agencies worldwide are working with state-of-the-art software to conduct automated, visual searches of these images. The combination of this software with the increased international sharing of information has led to a deluge of new cases fit for investigation. To select cases for investigation, many agencies prioritize by considering many factors, which include when the image was captured and whether the child victim(s) is in imminent danger.

The Danish National Police led one of the single most successful cases of victim identification, referred to as Operation Hamlet. Through a combination of technical Internet tracing techniques that used image clues to identify victims, this case identified more than 100 child victims worldwide.

Though the use of image clues and international sharing has increased the success of victim identification efforts, many heinous cases remain unsolved. To combat these cases, investigators in several countries have begun to use the mass media to help identify offenders and, in some countries, child victims. The German Federal Police, Bundeskriminalamt (BKA), is recognized worldwide as the pioneer of this technique. In at least 3 cases in which traditional and Internet tracing investigations failed to identify a child victim, the BKA successfully identified all of the victims by featuring them on a selected national crime television program. In the United States, the FBI has initiated similar efforts with the *America's Most Wanted* television program. With the help of this program, the FBI has had success in identifying the 3 offenders

featured thus far. Further investigations revealed that each of these offenders had committed offenses against multiple child victims.

### THE UNDERCOVER TECHNIQUE

Undercover (UC) operations have become a primary investigative strategy for dealing with Internet crime in countries in which the use of this technique is legally permissible; however, many countries do not allow the investigation of a suspect who lacks proper predisposition to commit a crime. Furthermore, an investigator who knowingly conducts unauthorized UC activity with subjects in countries in which such activity is illegal may be seen as infringing on national sovereignty. The bottom line is that investigators should carefully avoid issues of entrapment and remain cognizant of prevailing laws in the country or countries in which they conduct their investigative activities.

The good news is that if the UC technique can be used, UC officers and agents may pose as anyone on the Internet with relative ease and enjoy the same apparent anonymity craved by the offenders. In terms of child exploitation offenses, this may include posing as a child by standing in place of a would-be victim, proactively identifying suspects, assuming the role of a fellow trader interested in child pornography, or pretending to be a molester with access to children who are available for sex.

For UC investigations, investigators must only use computers set aside for these investigations that can not be traced to government agencies or compromise other computers or networks. All investigators, especially those conducting UC activity, should be keenly aware of the potential harm of a computer virus, Trojan, or worm. The occurrence of these threats, as well as their complexity and potential harm, continues to grow exponentially. At a minimum, online investigators should be proficient in using anti-virus software and a network with a proper firewall or, preferably, a stand-alone computer with a personal firewall. Investigators should be certain that such programs remain current.

One way to help prevent these harmful issues from arising is by understanding the use of a file name extension. Unfortunately, most Windows-based computers do not show file extensions for known file types. Therefore, investigators should learn ways to configure their computers to show all file extensions. Once this is done, investigators should remain aware of the many file name extensions that constitute a "danger list" (eg, .exe, .vbs, .js, .asp, .shs, .scr, .com, .bat, .sys, .ovl, .prg, .mnu).

The problem with identifying programs from this list is that each of these file types has a legitimate purpose but can be used to create harm. When considering whether a particular file may be harmful, investigators should consider the file's source, the context in which the file was found, and any messages or other files associated with the suspect file. In any case, all suspect files, especially those received via the Internet or from suspect evidence, should be scanned for viruses before opening. Whenever possible, a stand-alone computer that is *not* connected to the Internet or to another network should be used to open such files.

---

### OTHER INTERNET CRIME CONCERNS

The world of Internet crime is not just that of child exploitation offenses. Terrorism, computer intrusion and hacking matters, Internet fraud and intellectual property violations, hate crimes and crimes of violence, and many other "traditional" crimes have found their way onto the Internet as well. This has led to great debate within larger agencies as to whether these investigations should be handled by cybercrime task forces, which work all types of computer crimes, or by more specialized teams, which treat the computer merely as a new instrument of the crime. Early experience has shown that both models can be used effectively.

## TYPICAL INTERNET CHILD EXPLOITATION CASES

### Case Study 26-1

In the United States, a 38-year-old civilian military contractor was running an automated file server from his home in an IRC channel named for a child pornography movie series. The subject appeared to be a serious distributor of child pornography because he allowed a massive amount of downloading per user. A UC FBI agent downloaded images of child pornography from the subject, who was found to have configured his computer to use an IP address other than the one assigned to him by his cable modem provider. By working with the network operations center of the cable modem provider, the UC agent was able to determine the true identity of the subject, and the subject's home was searched. The subject was charged with possession, advertising, and distribution of child pornography and was sentenced to 7 years in prison. As a result of his arrest, 2 of his cousins came forward to report that the subject had molested them when he was between 14 and 16 years old and they were between 6 and 8 years old.

### Case Study 26-2

A successful 62-year-old Broadway music director who worked at a summer arts camp for kids was suspected of illicit contact with a minor. The local police department in New Hampshire contacted the FBI and supplied the subject's online identity. A UC FBI agent posed as a 13-year-old boy and sent a message to the subject to establish contact. The subject expressed a desire to meet the "boy," and he traveled to a mall in Maryland to meet the "boy" to have sex. A search executed at the subject's home revealed a victim logbook, which led to dozens of other possible victims. The subject was sentenced to a 41-month prison term.

### Case Study 26-3

A 32-year-old man living in a suburb of Dublin, Ireland, was being monitored in the preteen channels on IRC. An Irish federal police official (or Garda) engaged him in conversation online in IRC after he requested a private chat. During the conversation, which continued over a number of nights, the suspect sent child pornography to the officer. A search of the subject's house revealed a huge collection of child pornography stored on disks kept under the floorboards in his bedroom.

### Case Study 26-4

A 28-picture series showing the sexual abuse of an 8- to 10-year-old girl was detected during a routine Internet search by the computer crime squad of the German Federal Criminal Police Office at Interpol Wiesbaden. Identification of the person responsible for the postings was not possible because of the absence of log files. A shopping bag from a German supermarket was found in the background of some of the pictures, and other useful information was also found within the contents of the image files themselves. A difficult decision was made to publish and show on German television some selected, nonpornographic pictures that showed the abused girl. As a result, the girl and perpetrator were located a week later. The offender was a 25-year-old unmarried educator who specialized in caring for problem children and for individual cases; he did so in the child's home; he also volunteered as a Boy Scout leader. Investigators determined that he had abused 3 children, and he was sentenced to 4 years in prison. One accomplice was also identified.

### Case Study 26-5

A 50-year-old man from Pamplona, Spain, who had police records for child abuse set up e-mail distribution lists for the purpose of distributing information and child pornography images. Even though the lists were in Spanish, English-speaking offenders joined the groups because of the amount of child pornography files available. The suspect was found to be the owner of a video club with child pornography videotapes available from Germany. At first, he used the distribution lists to offer and sell these tapes; however, portions of the movies were later digitized and posted within the groups. The Cuerpo Nacional de Policia first obtained access to the distribution list and then monitored 15 e-mail accounts. The investigation resulted in 8 arrests in Spain, and reports of other offenders were issued to law enforcement officials in the United States, Canada, Argentina, Mexico, Chile, Ecuador, Puerto Rico, Germany, Sweden, Serbia, the Netherlands, the United Kingdom, France, Denmark, Finland, Thailand, the Philippines, Korea, Malaysia, Australia, and New Zealand.

### Case Study 26-6

In the Netherlands, a female Internet user reported to the local police that she had been chatting with a man on ICQ who sent her some child pornography images. He gave her his cell phone number and they arranged to meet each other on the Internet again the next day. The local police informed the Dutch national police which worked with the public prosecutor to trace the owner of the cell phone. The next day a police officer went to the woman's house and waited with the woman until the suspect was online again. At the same

time, the public prosecutor and some police officers waited near the suspect's house. The moment the suspect sent another child pornography picture to the woman's computer, the officers arrested the man in his house since he was caught in the act. The man's computer was still online, and more child pornography pictures were found.

### CONCLUSION

Regardless of the organizational model selected, communication among investigators and the sharing of knowledge and resources is the key to success. For this reason, investigators are cautioned *not* to investigate Internet crimes in isolation. Becoming involved in a task force (or at least seeking regular assistance), becoming trained, and sharing information are all necessary to conduct Internet investigations. Many domestic and international agencies, large and small, have such resources available and welcome contact from other investigators.

### APPENDIX 26-1: GLOSSARY OF INTERNET-RELATED TERMS\*

**American Registry of Internet Numbers (ARIN)**—The organization responsible for the management of Internet Protocol (IP) address numbers for the Americas and sub-Saharan Africa.

**Anti-virus software**—A program that can detect known or potential viruses found on hard drives, on floppy disks, or in Internet traffic.

**Asian-Pacific Network Information Center (APNIC)**—The organization responsible for the management of IP address numbers for the Asia-Pacific region. There are 62 economies within the Asia-Pacific region, from Afghanistan in the Middle East to Pitcairn in the Pacific Ocean.

**Bandwidth**—The potential speed of data transmission on a communication medium.

**Broadband**—A communication medium that provides a wide band of frequencies to transmit information.

**Browser**—A program that allows the user to look at and interact with all the information found on the World Wide Web (WWW).

**Cable modem**—A device that enables the connection of a computer to a cable television line to receive, and possibly transmit, data at higher speeds.

**Channel**—A specific chat group found on Internet Relay Chat (IRC) similar to a chat room on a Web site or an online service provider.

**Chat room**—A Web site or part of a Web site found on an IRC channel or as part of an online service provider. A chat room provides a venue for communities of users with a common interest to communicate in real time.

**Country code top-level domain (ccTLD)**—The top-level domain name of an Internet address that identifies that domain generically as associated with a country. For example, in the domain name, "police.se," Sweden (ie, ".se") is the chosen ccTLD. Some ccTLDs can be inaccurate and misleading.

**Cyberspace**—The global community created by the interconnectedness of people through computers and the Internet.

**Domain name**—The labeling system that locates an organization or other entity on the Internet by a name that corresponds to an IP address. For example, the domain name "www.klpd.nl" locates an Internet address for "klpd.nl," which is the Netherlands National Police Agency at IP address 193.178.243.72.

**Domain name system (DNS)**—The manner in which Internet domain names are located and translated into IP addresses.

\* Adapted from <http://www.whatis.com>.

**Download**—The transmission of a file from one computer system to another, usually smaller computer system.

**Digital Subscriber Line (DSL)**—A broadband information system that brings high-bandwidth capacity to homes and businesses over ordinary telephone lines.

**Electronic mail (e-mail)**—The exchange of messages and sometimes file attachments via the Internet.

**Encryption**—The conversion of data into a form that can not be easily understood by unauthorized people.

**File name extension**—An optional addition to a computer file name that describes the file's format in a suffix that usually consists of 3 characters (eg, .pdf, .doc, .jpg, .mpg, .avi).

**File Transfer Protocol (FTP)**—The IP for downloading and uploading files.

**Firewall**—Hardware or software located at a network gateway server that protects the resources of a private network from users of other networks.

**Gateway**—A network point that acts as an entrance to another network.

**Generic top-level domain (gTLD)**—The top-level domain name of an Internet address that identifies that address generically as associated with some domain class (eg, .com, .net, .org, .gov, .edu, .int, .mil.). For example, in the domain name "www.fbi.gov," ".gov" is the chosen gTLD.

**Header**—In a newsgroup or e-mail message, the header is the portion of a transmission that is sent with the actual message and may identify the sender and other facts about the transmission.

**Host**—Any computer that has full, 2-way access (ie, transmit and receive) to other computers on the Internet.

**Hosting**—The business of housing, serving, and maintaining files for one or more Web sites. Also known as *Web site hosting* and *Web hosting*.

**Hypertext Markup Language (HTML)**—The set of symbols or codes inserted in a file that is intended for display on a Web browser.

**Hypertext Transfer Protocol (HTTP)**—The set of rules for exchanging files on the WWW.

**ICQ**—A program used to notify users when friends and contacts are online on the Internet and allows the sending of messages, files, audio, and video to other users. Also known as *I Seek You*.

**Instant message**—The exchange of real-time messages with chosen friends or co-workers on the Internet.

**Internet**—A worldwide system of computer networks. A network of networks in which users at any one computer can, if they have permission, obtain information or other services from any other computer. Also known as the *Net*.

**Internet Assigned Numbers Authority (IANA)**—The organization under the Internet Architecture Board of the Internet Society that, under a contract from the US government, oversaw the allocation of IP addresses to Internet Service Providers. Partly because the Internet has become a global network, the US government has withdrawn its oversight of the Internet, which was previously contracted to IANA, and has lent support to an organization with global, nongovernment representation. The Internet Corporation for Assigned Names and Numbers (ICANN) has assumed responsibility for the tasks formerly performed by IANA.



**Internet Corporation for Assigned Names and Numbers (ICANN)**—The private, nongovernment, nonprofit corporation with responsibility for the services previously performed by the IANA.

**Internet Message Access Protocol (IMAP)**—A standard protocol for receiving e-mail.

**Internet Protocol (IP)**—The protocol by which data are sent from one computer to another on the Internet.

**Internet Protocol (IP) address**—A 32-bit number, which is usually expressed as 4 decimal numbers. Each decimal number represents 8 bits, which are used to identify senders and receivers of information across the Internet.

**Internet Relay Chat (IRC)**—A system for chatting within stand-alone software or within a Web browser.

**Internet Service Provider (ISP)**—A company that provides individual and corporate access to the Internet and other related services (eg, Web site building, hosting).

**Link**—A selectable connection on a Web page from a word, picture, or other information to another Web page or Internet object.

**Modem**—A device that modulates outgoing digital signals from a computer or other digital device into analog signals for a conventional, copper-twisted pair telephone line and demodulates the incoming analog signal and converts that signal to a digital signal for the digital device.

**Network**—A number of host computers interconnected by communication paths.

**Network News Transport Protocol (NNTP)**—The protocol for managing the messages posted on Usenet newsgroups.

**Network Time Protocol (NTP)**—Protocol used to synchronize computer clock times in a network of computers.

**Newsgroup**—A discussion about a particular subject that consists of messages posted and propagated through Usenet.

**Online service provider**—A service (eg, America Online) that has its own online, independent content rather than connecting users directly with the Internet. Most online service providers provide an Internet connection, in which case these providers function as ISPs as well.

**Password**—A sequence of characters used to determine whether a computer user requesting access to a computer system is an authorized user.

**Peer-to-peer (P2P)**—A communications model in which each party has the same capabilities and either party can send or receive information.

**Personal firewall**—A software application used to protect a single computer from intruders outside the network. Also known as a *desktop firewall*.

**Point-of-presence (POP)**—An access point to the Internet.

**Post Office Protocol (POP3)**—The most recent version of a standard protocol for receiving e-mail.

**Protocol**—A special set of communication rules.

**Redirection**—A technique for moving visitors to a Web page that differs from the address entered or followed by the user.

**Regional Internet Registries (RIRs)**—Entities that provide IP registration services. The 3 current RIRs are the American Registry for Internet Numbers (ARIN), the Registrar for Internet Protocols in Europe (RIPE), and the Asian-Pacific Network Information Center (APNIC).

**Registrar for Internet Protocols in Europe (RIPE)**—The organization responsible for the management of IP address numbers membership in Europe, the Middle East, northern Africa, and parts of Asia.

**Remailer**—An Internet site to which e-mail can be sent for forwarding to an intended destination but conceals the sender's e-mail address.

**Request for Comments (RFC)**—A formal document from the Internet Engineering Task Force (IETF) that resulted from committee drafting and subsequent review by interested parties.

**Server**—A computer program that provides services to other computer programs in the same network or different computers. The computer that the server program runs on is also referred to as a server.

**Simple Mail Transport Protocol (SMTP)**—A protocol primarily used in sending e-mail.

**Spam**—Unsolicited e-mail or other unwanted communications received on the Internet.

**Spoof**—To deceive for the purpose of gaining access to someone else's resources. For example, if a user fakes an Internet address to appear to be a different kind of Internet user, the user is spoofing.

**System tray**—A section of the taskbar in the Microsoft Windows desktop user interface that is used to display the clock and icons of certain programs. Some running programs appear only in the system tray.

**Top-level domain (TLD)**—Identifies the general part of the domain name in an Internet address. A TLD is either a generic TLD (gTLD) (eg, .com for commercial, .edu for educational) or a country code TLD (ccTLD) (eg, .nl for the Netherlands, .ie for Ireland).

**Transmission Control Protocol (TCP)**—A protocol used along with the IP to send data in the form of message units between computers over the Internet.

**Trojan**—A program in which a malicious or harmful code is contained. A Trojan appears to be harmless programming or data so that it can gain control and do damage (eg, ruining a hard disk). A Trojan may be redistributed as part of a virus.

**Uniform Resource Locator (URL)**—The address of a file (ie, resource) that is accessible on the Internet. For example, "http://www.fbi.gov/hq/cid/cac/innocent.htm" describes the Federal Bureau of Investigation's Innocent Images Web page. This URL indicates the page to be accessed with an HTTP (ie, Web browser) application located on a server named "www.fbi.gov." The specific file is in the directories of "/hq/cid/cac" and named "innocent.htm."

**Upload**—Transmission from one, usually smaller, computer to another computer.

**Usenet**—A collection of user-submitted messages about various subjects that are posted to servers on a worldwide network in which each subject collection of posted notes is known as a *newsgroup*.

**Virtual community**—A community of people sharing common interests, ideas, and feelings via the Internet or other collaborative networks.

**Virus**—A program or piece of a program usually disguised as something else, which causes an unexpected and usually undesirable event, usually seeking to contaminate only the host machine.

**Voice over IP (VoIP)**—A protocol for managing the delivery of voice information using the IP.

**Web site**—A collection of Web files regarding a particular subject that includes a beginning file called a *home page*. For example, the Web site for Ireland's National Police Service, An Garda Síochána, has the home page address of "http://gov.ie/garda."

**Whois**—A program that identifies registration information provided by the owner of any second-level domain name who has registered it with a Regional Internet Registry. Whois information can be bogus or incomplete.

**World Wide Web (WWW)**—All the resources and users found on the Internet using the HTTP.

**Worm**—A self-replicating virus that resides in active memory and duplicates itself with the intent of sending itself to other users.

MR. WHITFIELD. But Mr. Weeks, thank you for the great job you are doing.

MR. WEEKS. Thank you.

MR. WHITFIELD. We really appreciate your willingness to come and help us out, and I look forward to working with you in the future.

MR. WEEKS. Thank you, Mr. Chairman.

MR. WHITFIELD. And that adjourns today's hearing.  
[Whereupon, at 2:20 p.m., the subcommittee was adjourned.]

RESPONSE FOR THE RECORD OF WILLIAM E. KEZER, DEPUTY CHIEF INSPECTOR, UNITED STATES POSTAL INSPECTION SERVICE

May 19, 2006

The Honorable Edward Whitfield  
Chairman  
Oversight and Investigations Subcommittee  
of the Energy and Commerce Committee  
U.S. House of Representatives  
Washington, DC 20515-0001

Dear Mr. Chairman:

On April 6, 2006, the U.S. Postal Inspection Service was honored to testify before the Oversight and Investigations Subcommittee concerning its efforts to combat the increasingly, menacing crime of sexual exploitation against children. Despite the overwhelming use of the Internet to perpetuate crimes involving child exploitation, many offenders also utilize the U.S. Mail, in concert with the Internet, to traffic in child pornography or otherwise sexually exploit children. Numerous examples of recent cases investigated by Postal Inspectors with a common nexus to the Internet and the U.S. Mail were provided in our oral and written testimony.

When the U.S. Mail is used in connection with crimes involving the sexual exploitation of children, Postal Inspectors work diligently to identify and track down those responsible for the commission of these heinous crimes. We work closely with the various United States Attorneys and other agencies, such as the National Center for Missing and Exploited Children in order to bring the alleged offenders before the federal judicial system. The Postal Service has and continues to be committed to fighting the war on crime against those individuals who prey on our nation's children. Presently, we have a number of Postal Inspectors assigned full-time to these types of investigations.

Testimony elicited by the Subcommittee revealed several areas in which Congress may aid law enforcement in these types of investigations. These include possible assistance within the jurisdiction of both the House Energy and Commerce and House Judiciary Committees. Assistance suggested by several of the law enforcement witnesses at the April 6<sup>th</sup> hearing included requiring Internet Service Providers (ISPs) to maintain subscriber data for a set time period (i.e., a minimum of 90 days) and to respond promptly to subpoenas seeking subscriber information; providing for additional investigator resources assigned to child exploitation investigations; providing for the means to reduce backlogs in the forensic examination of digital evidence; and, specific to the Postal Inspection Service, providing administrative subpoena authority in the area of child exploitation offenses.

As a result of the hearing, the Postal Inspection Service, along with other agencies, were asked to provide further comment on the benefits of administrative subpoenas as a necessary law enforcement tool. The Postal Inspection Service was invited to formally request this type of investigative authority.

It is our belief the ability to issue administrative subpoenas will greatly assist our efforts against child exploitation. The testimony of several witnesses at the April 6<sup>th</sup> hearing supported the fact administrative subpoenas help accelerate the process of identifying offenders who oftentimes hide behind screen names as well as websites operated by child abusers and pornographers. As you are aware, in 1998 Congress passed *The Child Protection and Sexual Predator Punishment Act of 1998*. Title III, Section 301 of the Act authorized the Attorney General to issue administrative subpoenas in child exploitation cases. This authority is presently codified at 18 U.S.C. §. 3486. **(Exhibit A)** This authority has been delegated to the Federal Bureau of Investigation at the supervisory field level.

The U.S. Postal Inspection Service would benefit from having this investigative tool to aid in its law enforcement efforts against child exploitation. As the Internet has changed the manner in which child pornographers operate, so too, must the law enforcement tools used to investigative and arrest the perpetrators of these crimes adapt to the changing environment.

It appears an amendment would be needed to 18 U.S.C. § 3486 in order to include authority for the Postmaster General to issue administrative subpoenas in criminal investigations involving child exploitation. **(Exhibit B)** If such an amendment is enacted, the Postal Service would then publish regulations authorizing Postal Inspectors in Charge at the field level similar to the process used by the Federal Bureau of Investigation. This amendment would greatly assist federal agencies in the pursuit of those individuals who are sexually abusing and exploiting our children.

The interest and assistance of the Subcommittee on Oversight and Investigations are welcomed and appreciated. If you require any additional information, please contact Deputy Chief Inspector William Kezer at 202-268-8709.

Sincerely,

L. R. Heath  
Chief Postal Inspector

Enclosures

RESPONSE FOR THE RECORD OF FLINT WATERS, LEAD SPECIAL AGENT , WYOMING  
DIVISION OF CRIMINAL INVESTIGATION, INTERNET CRIMES AGAINST CHILDREN TASK  
FORCE TECHNOLOGY CENTER, UNITED STATES DEPARTMENT OF JUSTICE

May 30, 2006

The Honorable Edward Whitfield  
Chairman  
Oversight and Investigations Subcommittee  
of the Energy and Commerce Committee  
U.S. House of Representatives  
Washington, DC 20515-0001

Dear Mr. Chairman:

1. You state in your testimony that a special agent from the Department of Homeland Security worked with your task force. Is this an employee of the Immigration and Customs Enforcement, or some other division?

Special Agent Balliett is an employee with Immigrations and Customs Enforcement. She is assigned to our task force full time and routinely handles cases throughout the region related to the trafficking of child sexual abuse images and Internet child victimization. I can't emphasize enough how the Federal support of our mission makes it possible to protect Wyoming children. This cross-jurisdictional problem has overwhelmed state and local law enforcement. Without the Federal resources we have received, like a special agent from ICE and the ongoing guidance and funding provided from the Office of Justice Programs, we would have failed.

2. Under Wyoming law, if law enforcement has a current IP, e-mail and home address for an Internet user suspected of possessing child pornography, is that sufficient to obtain a search warrant and seize that computer?

If the suspicion of criminal conduct rises to a level of probable cause we can obtain a search warrant to seize the computer.

I will make myself available for any further questions that may arise from this matter.

Respectfully,

Flint Waters,  
Lead Agent, Wyoming ICAC

RESPONSE FOR THE RECORD OF CHRIS SWECKER, ACTING ASSISTANT EXECUTIVE  
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE



**U.S. Department of Justice**  
Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

August 30, 2006

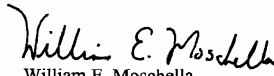
The Honorable Edward Whitfield  
Chairman  
Subcommittee on Oversight and Investigations  
Committee on Energy and Commerce  
United States House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

Please find enclosed the Department of Justice's responses to questions directed to Chris Swecker, Acting Executive Assistant Director of the Federal Bureau of Investigation, following the April 6, 2006, hearing entitled "Sexual Exploitation of Children Over The Internet: What Parents, Kids, and Congress Need to Know About Child Predators."

The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to the submission of these responses. Please do not hesitate to call upon us if we may be of additional assistance.

Sincerely,

  
William E. Moschella  
Assistant Attorney General

Enclosure

cc: The Honorable Bart Stupak  
Ranking Minority Member



**Responses of the Federal Bureau of Investigation  
Based Upon the April 6, 2006 Hearing  
Before the House Committee on Energy and Commerce,  
Subcommittee on Oversight and Investigations  
Regarding "Sexual Exploitation of Children Over the Internet"**

**Questions Posed by Representative Dingell**

**1. Does the Federal Bureau of Investigation (FBI) have any suggestions as to how to ensure that credit card companies, banks, electronic payment and digital currency companies and/or financial clearinghouses that can enable the payments for child pornography will cooperate with law enforcement or private groups to halt their involvement in this illegal trade?**

**Response:**

The FBI's field offices enjoy excellent relationships with the financial institutions and financial services industry members in their jurisdictions. Based on those relationships, financial institutions generally respond voluntarily and quickly to the FBI's requests for information regarding their customers who purchase access to child pornography web sites. Nonetheless, extending administrative subpoena authority to financial institutions and financial services entities in child pornography investigations (this authority is already available to obtain electronic communication service or remote computing service records in these cases) would improve the FBI's ability to address these crimes quickly and effectively. The FBI additionally suggests consideration of the following measures, which would enhance the efficiency and productivity of these criminal investigations:

- Requiring financial institutions to accept electronic service of process and to provide their responsive information in an electronic format would expedite the process and reduce the opportunity for data entry errors.
- Requiring financial institutions to authenticate a user's information before charging the individual's account or credit card would serve two purposes: it would reduce loss due to identity theft and it would enable the FBI to more quickly identify the proper subject of an investigation.
- Requiring electronic currency companies to maintain customer information and to provide this information to law enforcement in appropriate circumstances would allow quicker identification of offenders.

**2. Has the FBI made any attempt to encourage the thousands of small Internet service providers to join voluntarily with the larger ones to report any suspected child pornography on their systems?**

**Response:**

The FBI interacts daily with Internet Service Providers (ISPs), both large and small, through our investigation of cyber crimes committed on their systems. During these interactions, the FBI regularly reminds ISPs that they are required by 42 U.S.C. § 13032 to report any child pornography they may discover on their systems. This obligation applies to all those who provide electronic communication services or remote computing services to the public, regardless of size.

**3. In your testimony, you stated that banks made referrals to law enforcement agencies concerning suspicious banking transactions through the “SAR process”. Please describe that process and provide the citations to the enabling law and/or regulations and guidelines.**

**Response:**

The Bank Secrecy Act (BSA), enacted in 1970, authorizes the Secretary of the Treasury to issue regulations requiring that financial institutions keep records and file reports on certain financial transactions that may be useful in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism. The authority of the Secretary to administer the BSA (codified at 31 U.S.C. §§ 5311-5332 with implementing regulations at 31 C.F.R. Part 103) has been delegated to the Director of the Financial Crimes Enforcement Network (FinCEN). Section 5318(g) specifically authorizes the filing of suspicious activity reports (SARs) by financial institutions.

FinCEN, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the National Credit Union Administration are all owners of BSA information. The Internal Revenue Service maintains all BSA records in a computer database, known as the Currency and Banking Retrieval System (CBRS). FinCEN is responsible for the overall management of this database.

Financial institutions are required to file SARs using one of the four industry-specific SAR forms. Depository institutions are required to file SAR form TD F 90-22.47 upon the discovery of a known or suspected federal criminal violation. This form was designed primarily to report financial crimes and contains check

boxes for certain commonly reported types of financial frauds such as check fraud, money laundering, identity theft, or transactions that may involve terrorist financing. However, other violations of criminal law that the bank discovers may be reported on this form using the "other" category or the narrative portion of the SAR.

Due to their sensitive nature, there are restrictions on how SARs can be used. Financial institutions are prohibited from notifying any person involved in the transaction that a SAR was filed. Likewise, Government employees and officials may not notify any person involved in the transaction, other than as necessary to fulfill the official duties of that employee or official. These reports are to be used for lead value only and, generally speaking, are not used in criminal proceedings. Instead, evidence used in criminal proceedings is generally developed from an agent's review of the underlying documentation obtained from the bank and from other investigative steps, such as follow-up interviews.

Since 1997, depository institution SARs have been provided to the FBI by FinCEN in electronic format. The FBI has also received downloads of newly filed depository institution SARs from CBRS several times a week. In September 2000, the FBI entered into a Memorandum of Understanding with FinCEN pursuant to which trained FBI employees are permitted to access all FinCEN BSA reports electronically.

**4. During the hearing, at the request of Chairman Whitfield, you agreed to provide a formal response to Ranking Member Stupak's questions about the status of the issuance of guidelines or regulations by the Justice Department to facilitate the reporting requirements of 42 U.S.C. § 13032. Please provide that response.**

**Response:**

The Department of Justice (the Department) has issued regulations implementing the reporting requirements of 42 U.S.C. § 13032 and designating agencies to receive and investigate such reports at 28 C.F.R. §§ 81.11 through 81.13. While the FBI is not sufficiently involved in the development of guidelines or regulations to provide a detailed response to this question, we understand from the Department's Criminal Division that the United States Internet Service Provider Association (US ISPA), as the representative of all of the major ISPs, has worked with the National Center for Missing and Exploited Children (NCMEC) to develop and issue "Sound Reporting Practices for ISPs" regarding the reporting practices and report content required by statute. These industry-generated "Sound Reporting Practices" provide for the voluntary disclosure of more information by ISPs than the Department could require by regulation. NCMEC has advised that, since these reporting practices were initiated, the effectiveness of reporting under Section 13032 has improved. The Department anticipates that, over the long

term, these protocols will promote more effective reporting and investigation, not only because they reflect industry consensus, but also because of the efficiencies offered by voluntary compliance.

RESPONSE FOR THE RECORD OF DR. FRANK KARDASZ, SERGEANT, PHOENIX POLICE  
DEPARTMENT, PROJECT DIRECTOR, ARIZONA INTERNET CRIMES AGAINST CHILDREN TASK  
FORCE, UNITED STATES DEPARTMENT OF JUSTICE

**1. Please describe the difficulty of tracking illegal Internet activity that occurs through wireless access points. Are there tools to determine where the activity originates?**

The difficulty in tracking illegal Internet activity originating from wireless access points might best be described by way of a true-life example.

In August, 2005, I received a call from an officer of the Milwaukee, Wisconsin Police Department. He was investigating the case of a missing boy who had disappeared with someone the boy had met via the Internet. Milwaukee computer forensics examiners had looked into the contents of the boys computer. They found the screen name of the suspect with whom the boy had been chatting before he had disappeared. They subpoenaed the Internet service provider (ISP) associated with the suspect's screen name. Subpoena results indicated that the Internet protocol address affiliated with the screen name originated from an apartment in Phoenix, Arizona. Milwaukee PD provided me with the apartment address.

My detectives and I immediately went to the Phoenix apartment. We quickly eliminated the apartment resident as a suspect but we learned that she possessed an unencrypted wireless router and the device provided free Internet access to everyone in nearby apartments. We began interviewing neighbors, asking them if they had observed a new boy in the area. Our diligence and luck prevailed. One local resident said that a man living nearby had recently been accompanied by a boy whom the man said was his son.

We then conducted surveillance for several hours until the man and boy appeared. Detectives apprehended the suspect, a wanted sex offender with felony warrants from prior offenses, and the boy, who had been molested by the suspect.

The Phoenix suspect had used a laptop computer from his nearby apartment to intercept the unencrypted wireless signal from his unsuspecting neighbor's computer router. This permitted the offender to communicate with the boy in Wisconsin and entice him into meeting. The boy is now back with his mother in Wisconsin. The suspect awaits trial.

There were no special tools available to us that could have pinpointed the exact location of the offender who had used his neighbors unencrypted wireless access. We employed two old-fashioned police techniques; interviews and surveillance.

My colleagues nationwide have shared other similar stories with me involving wireless access points used for criminal offenses. In some cases their investigations dead-end at a wireless access point that is providing unencrypted Internet service to everyone in antenna range. In other cases interviews and surveillance fail because the elusive suspect(s) quickly move on to other wireless access points.

Countless libraries, coffee shops, airports, hotels and businesses now provide free wireless Internet access either accidentally, because they fail to enable the encryption features to protect the signal, or as a free-bonus customer service. While free wireless access is a welcome service for law-abiding citizens, it is also a tool for criminals.

**Are there tools to determine where the activity originates?**

The answer is yes and no. A subpoena or search warrant to the ISP associated with an Internet protocol (IP) address is the tool that we use to identify the specific location of the computer assigned to an IP address.

In some cases, the computer we identify is attached to a router that is broadcasting a wireless signal to another computer, the exact location of which is unknown. If the wireless signal is being used by a remote computer, the investigation continues and becomes more difficult. There are technical surveillance tools, to wit, radio spectrum analyzers and direction finders, that can be used to further hone in on the remote computer, but these tools are somewhat expensive for the average local law enforcement agency (\$5,000 - \$25,000), they require advanced training and are often inexact in a city environment where several wireless signals may be present at the same time.

- 2. In your testimony, you stated that the cell phone providers maintained their records for cell phone usage for long periods of time, but that Internet service providers (ISP) did not. Internet service providers have alleged that they do not have storage space to maintain records for any length of time. Do you know why cell phone providers can store this information for long periods of time, but Internet service providers cannot?**

My comments about records preservation were based on my limited knowledge of the cell phone industry and from my experiences, mostly as a cellular service consumer. I know that cell phone providers often closely track customer usage by the minute and cell phone providers often maintain copious records for billing purposes. I have reviewed cell phone billing statements that gave long lists of individual calls including the numbers called from and to, the number of minutes used during each call and the cost of each call. Maintaining so much data likely entails computer servers with large data storage capacity.

Internet service providers do not normally bill customers on a per-minute basis so there is usually not a need to record the frequent changes in Internet data-packet destinations that are needed for billing purposes by cell phone companies. I have seen computer traceroute software that enables reporting of the location of each server through which data packets travel across the Internet but the data storage capacities needed to track all of that information would be incredibly large, and in most cases, unnecessary.

The datum that we believe would be most useful in order to have a starting point for our investigations are, minimally, the subscriber information. There is no privacy violation when ISP's retain subscriber information and we in law enforcement could only subsequently obtain the information through a subpoena or search warrant. I believe that Internet service provider can preserve this data. Many of them already retain the data because without it, they are unable to bill customers who use their services.

If ISP's are stating they cannot store the information, it is probably because they choose not to store it. Computer data storage capacity has increased exponentially in recent years and the cost of data storage has decreased.

I am aware that data retrieval and subsequently reporting the information back to law enforcement requires human intervention and entails labor costs.

It is my opinion that ISP's can store the information if they choose to. It is also my opinion that some ISP's will not satisfactorily store data and recover data for law enforcement until the law mandates them to do so.

- 3. Are you proposing that all records of individual Internet use be maintained by the service provider, including e-mails, instant messages and chat room discussions, or only the IP addresses and other identifying information about the addressee? If all you want is the background information to identify subscribers, do you believe that a lack of storage space is a problem for the ISP?**

I am not proposing that all records of individual Internet use be maintained by service providers.

Maintaining ALL records, including the content of all emails, instant messages and chat room discussions for extended periods of time would present the ISP's with a significant storage responsibility. Although it is possible to preserve all of the data, it would require very large data storage capacities.

Preserving all data, including the intimate details of private text messages and/or the images transmitted during private communications would undoubtedly send privacy protection advocates into a lather! Even though the information would be retained by the ISP's and not released to law enforcement except by court order, privacy advocates would likely balk.

Basic subscriber information, that data which is presently available from cooperating ISPs through subpoena is the minimum we hope to mandate that ISP's preserve for law enforcement investigations. This information would not be available to law enforcement except through subpoena or search warrant.

Although I do not claim intimate knowledge of the specific equipment or storage capacities presently available to all ISP's, I do not believe that storing this information would present most ISP's with storage space problems.

- 4. Are administrative subpoenas only used for business records?**

In my work involving Internet crimes, our administrative subpoenas have been used only for retrieving business records from Internet service providers. As a wider practical matter, I am aware that administrative subpoenas can also be used to demand personal documents and other tangible things from not only businesses but also from private citizens.

- 5. Under Arizona law, if law enforcement has a current IP, e-mail and home address for an Internet user suspected of possessing child pornography, is that sufficient to obtain a search warrant to seize that computer?**

No. In Arizona, a search warrant must be based on probable cause for a felony offense and the warrant must be authorized by a magistrate. The required probable cause is described in the affidavit accompanying the search warrant. The affidavit is written by the investigator(s) who work the case.

Although a current IP address and the physical "home" address where the felony offense originated would be two very important items towards obtaining a search warrant, detectives would also conduct other investigative activities to build the necessary probable cause. The activities could include surveillance of the location, records checks and criminal history checks of the property owners, motor vehicle checks on vehicles frequenting the location, pretext visits and/or calls to the location. The combination of several of these items, along with the physical "home" address associated with the IP address would provide the probable cause needed for the search warrant.

Thank you for the opportunity to respond to the preceding questions. Please contact me if you require additional information.

Regards,

Dr. Frank Kardasz, Sgt. / Project Director  
Phoenix P.D. /AZ Internet Crimes Against Children Task Force  
620 W. Washington  
Phoenix, AZ 85003  
desk: 602 256 3404  
email: [frank.kardasz@phoenix.gov](mailto:frank.kardasz@phoenix.gov)  
web site: <http://azicac.net>



RESPONSE FOR THE RECORD OF JAMES PLITT, DIRECTOR, CYBER CRIMES CENTER, OFFICE OF INVESTIGATIONS, UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

No response was received to the following question submitted to Mr. Plitt.

**The Honorable John D. Dingell**

**Question for Mr. James Plitt, Director**

**Cyber Crimes Center, Office of Investigations**

**U.S. Immigration and Customs Enforcement**

**U.S. Department of Homeland Security**

**April 6, 2006**

**Subcommittee on Oversight and Investigations**

**Hearing entitled: "Sexual Exploitation of Children Over the Internet: What Parents, Kids and Congress Need to Know About Child Predators"**

1. Please describe in detail the relationship between the Cyber Crimes Center of Immigration and Customs Enforcement and the Innocent Images National Initiative of the Federal Bureau of Investigation. When a child exploitation investigation involves trans-border movement of images, which agency takes the lead in dealing with foreign agencies such as Interpol? Do both agencies count that investigation as one of their own?

RESPONSE FOR THE RECORD OF GRIER WEEKS, EXECUTIVE DIRECTOR, NATIONAL  
ASSOCIATION TO PROTECT CHILDREN

No response was received to the following questions submitted to Mr. Weeks.

**The Honorable John D. Dingell**

**Questions for Mr. Grier Weeks, Executive Director**

**PROTECT**

**April 6, 2006**

**Subcommittee on Oversight and Investigations**

**Hearing entitled: "Sexual Exploitation of Children Over the Internet: What  
Parents, Kids and Congress Need to Know About Child Predators"**

1. Please describe state statutes of limitation for possessing and distributing child pornography and any problems that may result. How successful has PROTECT been in increasing these time limitations?
2. Mr. Swecker of the Federal Bureau of Investigations testified, despite the public concern about child pornography, his office had not received any additional investigative resources in the FY2007 budget. Does the same situation exist in the States? Are state legislatures generally more willing to increase penalties for these crimes than to increase resources to investigate and prosecute them?

**SEXUAL EXPLOITATION OF CHILDREN  
OVER THE INTERNET: WHAT PARENTS,  
KIDS AND CONGRESS NEED TO KNOW  
ABOUT CHILD PREDATORS**

---

**WEDNESDAY, MAY 3, 2006**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ENERGY AND COMMERCE,  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 2:25 p.m., in Room 2123 of the Rayburn House Office Building, Hon. Ed Whitfield (chairman) presiding.

Members present: Representatives Walden, Burgess, Blackburn, Barton (ex officio), Stupak, DeGette, Inslee, Baldwin, and Whitfield.

Also present: Representative Gingrey.

Staff Present: Mark Paoletta, Chief Counsel for Oversight and Investigations; Alan Slobodin, Deputy Chief Counsel for Oversight and Investigations; Kelli Andrews, Counsel; Karen Christian, Counsel; Michael Abraham, Legislative Clerk; Edith Holleman, Minority Counsel; and David Nelson, Minority Investigator/Economist.

MR. WHITFIELD. I am going to call this hearing to order, and I apologize for our delay today. There was a hearing in the hearing room prior to our arrival and I certainly want to welcome those on the first panel. We will have a second panel of witnesses as well. Those buzzers that you hear going off are calling us to votes on the floor. We are going to have three votes on the floor, so I apologize in advance for further delay, but we will go do the three votes, then we will come back. We will do our opening statements, then we will swear in the first panel, and then we will get into the questions and answers.

So please forgive us, and we will adjourn the hearing--not adjourn, but recess the hearing until we can do these three votes. Thank you very much.

[Recess.]

MR. WHITFIELD. I will call the hearing to order, and once again apologize for the delay because of the votes on the floor. We are extremely enthusiastic that we have such a great panel of witnesses today on a subject matter that is quite serious, and one that is quite disturbing.

This will be our third hearing on “Sexual Exploitation of Children Over the Internet: What Parents, Kids, and Congress Need to Know About Child Predators.” Our first two hearings brought to light many staggering and sobering facts about how children are victimized over the Internet. We know the number of sexually exploitative images of child victims continues to rise, and that a large-scale commercial industry has developed around taking, trading, and selling sexually exploitative images of children over the Internet. We also heard testimony at our last hearing from several law enforcement agencies that are trying to combat this problem and catch child predators.

It is not an easy task. Although the Immigration and Customs Service, the Federal Bureau of Investigation, the U.S. Postal Service, the Internet Crimes Against Children Task Force, and many State and local agencies are working on putting child predators behind bars. The Internet has caused a proliferation of both the abusers as well as the images of the abused.

At our last hearing, I was struck by how many different law enforcement agencies are working on this problem, and yet, there does not seem to be any national strategy in place to deal with this growing problem. I hope that through our hearing on this topic, a national strategy will be put in place to ensure that our children are safer and child predators are caught and put behind bars.

Today, we will continue to learn about this horrific problem. We have a brave young lady with us today whom I had the opportunity to visit with before the hearing, Masha Allen, and I want to extend my most sincere thanks to you, Masha, publicly, for coming forward to tell us about your experience at the hands of a pedophile who happened to be your adoptive father. I also want to thank her mother, Faith Allen, for accompanying her today. Masha is now 13 years old, will testify about how she was adopted when she was 5 years old from a Russian orphanage by a divorced man living alone in Pennsylvania named Matthew Mancuso. Her adoptive father, Mr. Mancuso, sexually molested Masha from the first day she arrived at his home as a 5-year-old until law enforcement finally caught up with him 6 years later.

Masha is a survivor, and she will be able to tell us as the voice of a child victim and for victims everywhere how she feels particularly violated by the sexually exploitative images taken and posted by Mancuso over the entire Internet.

We will also hear testimony from Nancy Grace, a former State court prosecutor in Atlanta, Georgia, who I understand handled a number of cases involving sexually abused children. We also look forward to hearing from Ms. Grace about her media work involving issues

surrounding the sexual exploitation of children and specifically, over the Internet.

Finally, we will revisit some questions that we previously had for the Department of Justice and Federal Bureau of Investigation witnesses at our last hearing which were not answered because we did not feel like the right witnesses were present.

I am very glad to see that the Department of Justice has sent us up one witness that the subcommittee did request, Ms. Alice Fisher, who I had the opportunity to meet with earlier; however, we are still disheartened that we will once again not hear testimony from Mr. Andrew Osterbein, who is the head of the section at the Department of Justice that actually handles cases involving the sexual exploitation of children over the Internet. I know that Ms. Fisher oversees this section, and I am hopeful that she will be able to add some significant detail to how that section handles these types of cases, particularly when a cooperating child victim witness is involved, and also, we want to hear, obviously, from law enforcement on what we can do to help them do their jobs better.

A daunting challenge in combating the sexual exploitation of children over the Internet continues to be faced by all of us involved in this issue, and we hope to learn more today about the efforts of law enforcement in this area, and also to understand what the Department of Justice's recently proposed legislative package will add to their efforts in this regard.

I thank all of you for being here today. There isn't a more important issue than this one on our plate, and we want to make some efforts to curtail this, obviously, and prohibit it and be very stern in our enforcement of these statutes.

[The prepared statement of Hon. Ed Whitfield follows:]

PREPARED STATEMENT OF THE HON. ED. WHITFIELD, CHAIRMAN, SUBCOMMITTEE ON  
OVERSIGHT AND INVESTIGATIONS

GOOD AFTERNOON. I'D LIKE TO WELCOME EVERYONE TO THE SUBCOMMITTEE'S THIRD HEARING THAT EXPLORES ISSUES RELATED TO THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET. OUR FIRST TWO HEARINGS ON THIS TOPIC HAVE BROUGHT TO LIGHT MANY STAGGERING AND SOBERING FACTS ABOUT HOW CHILDREN ARE VICTIMIZED OVER THE INTERNET. WE LEARNED AT OUR LAST HEARING THAT THE NUMBER OF SEXUALLY EXPLOITATIVE IMAGES OF CHILD-VICTIMS CONTINUES TO RISE AND THAT A LARGE-SCALE COMMERCIAL INDUSTRY HAS DEVELOPED AROUND TAKING, TRADING AND SELLING SEXUALLY EXPLOITATIVE IMAGES OF CHILDREN OVER THE INTERNET.

WE ALSO HEARD TESTIMONY AT OUR LAST HEARING FROM SEVERAL LAW ENFORCEMENT AGENCIES THAT ARE TRYING TO COMBAT THIS PROBLEM AND CATCH THESE CHILD PREDATORS. IT IS NOT AN EASY

TASK. ALTHOUGH THE IMMIGRATION AND CUSTOMS SERVICE, THE FEDERAL BUREAU OF INVESTIGATION, THE U.S. POSTAL SERVICE, THE INTERNET CRIMES AGAINST CHILDREN TASK FORCE AND MANY STATE AND LOCAL AGENCIES ARE WORKING ON PUTTING THESE CHILD PREDATORS BEHIND BARS, THE INTERNET HAS CAUSED A PROLIFERATION OF BOTH THE ABUSERS, AS WELL AS, IMAGES OF THE ABUSED.

AT OUR LAST HEARING, I WAS STRUCK BY HOW MANY DIFFERENT LAW ENFORCEMENT AGENCIES ARE WORKING ON THIS PROBLEM—AND YET, THERE DOES NOT SEEM TO BE ANY NATIONAL STRATEGY IN PLACE TO DEAL WITH THIS GROWING PROBLEM. I HOPE THAT THROUGH OUR HEARINGS ON THIS TOPIC, A NATIONAL STRATEGY WILL BE PUT IN PLACE TO ENSURE THAT OUR CHILDREN ARE SAFER AND THAT THESE CHILD PREDATORS ARE CAUGHT.

AT OUR HEARING TODAY, WE WILL CONTINUE TO LEARN ABOUT THIS HORRIFIC PROBLEM. WE HAVE A VERY BRAVE YOUNG LADY HERE WITH US TODAY—MASHA ALLEN. I WANT TO EXTEND MY DEEPEST THANKS TO MASHA FOR COMING FORWARD TO TELL US ABOUT HER HORRIFIC EXPERIENCE AT THE HANDS OF A PEDOPHILE AND I ALSO WANT TO THANK HER MOTHER, FAITH, FOR ACCOMPANYING HER UP HERE TO THIS HEARING.

MASHA, WHO IS NOW 13 YEARS OLD, WILL TELL US ABOUT HOW SHE WAS ADOPTED WHEN SHE WAS JUST 5 YEARS OLD FROM A RUSSIAN ORPHANAGE BY A DIVORCED MAN, LIVING IN PENNSYLVANIA, NAMED MATTHEW MANCUSO. HER ADOPTIVE FATHER, MANCUSO, SEXUALLY MOLESTED MASHA FROM THE FIRST DAY SHE ARRIVED AS A 5 YEAR OLD UNTIL LAW ENFORCEMENT FINALLY CAUGHT HIM 6 YEARS LATER. MASHA IS A SURVIVOR—AND SHE WILL BE ABLE TO TELL US, AS THE VOICE OF CHILD VICTIMS EVERYWHERE, HOW SHE FEELS PARTICULARLY VIOLATED BY THE SEXUALLY EXPLOITATIVE IMAGES TAKEN AND POSTED BY MANCUSO OVER THE INTERNET.

WE WILL ALSO HEAR TESTIMONY FROM NANCY GRACE, A FORMER STATE COURT PROSECUTOR IN ATLANTA GEORGIA, WHO I UNDERSTAND HANDLED A NUMBER OF CASES INVOLVING SEXUALLY ABUSED CHILDREN. WE ALSO LOOK FORWARD TO HEARING FROM MS. GRACE ABOUT HER MEDIA WORK INVOLVING ISSUES SURROUNDING THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET.

FINALLY, WE WILL REVISIT SOME QUESTIONS THAT WE PREVIOUSLY HAD FOR THE DEPARTMENT OF JUSTICE AND FEDERAL BUREAU OF INVESTIGATION WITNESSES AT OUR LAST HEARING WHICH WERE NOT ANSWERED BECAUSE THE KNOWLEDGEABLE WITNESSES WE REQUESTED WERE NOT SENT UP TO TESTIFY. I MUST STATE THAT THIS HAS BEEN AN EXTREMELY FRUSTRATING PROCESS TO GET THE WITNESSES WE WANT—AND WHO WE BELIEVE WILL PROVIDE THE MOST THOROUGH ANSWERS--FROM THE DEPARTMENT OF JUSTICE AND FROM THE FBI UP HERE TO TESTIFY. I HOPE THAT TODAY IS THE BEGINNING OF THE END OF MY FRUSTRATION ON THIS POINT. I AM VERY GLAD TO SEE THAT THE DEPARTMENT OF JUSTICE HAS SENT UP ONE OF THE WITNESSES THAT THE SUBCOMMITTEE REQUESTED—MS. ALICE FISHER. HOWEVER, I AM STILL DISHEARTENED THAT WE WILL, ONCE AGAIN, NOT HEAR ANY TESTIMONY FROM MR. ANDREW OOSTERBAAN, THE HEAD OF THE SECTION AT THE DEPARTMENT OF JUSTICE THAT ACTUALLY HANDLES CASES INVOLVING THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET. I KNOW

THAT MS. FISHER OVERSEES THIS SECTION AND I'M HOPEFUL THAT SHE'LL BE ABLE TO ADD SOME SIGNIFICANT DETAIL TO HOW THAT SECTION HANDLES THESE CASES, PARTICULARLY WHEN A COOPERATING CHILD-VICTIM WITNESS IS INVOLVED.

I AM ALSO PLEASED TO SEE THAT MR. ROLDAN AND MR. BELL, FROM THE FBI, ARE HERE TODAY TO TESTIFY. MR. ROLDAN—I AM SURE YOU KNOW THAT WE REQUESTED YOUR ATTENDANCE AT THE HEARING WE HAD ON APRIL 6<sup>TH</sup>. WE WERE VERY DISTURBED TO LEARN THAT RATHER THAN ATTEND OUR HEARING, YOU WERE APPEARING ON MORNING NEWS SHOWS LIKE CNN AND THE TODAY SHOW. WE'RE GLAD YOU MADE TIME FOR US TODAY AND LOOK FORWARD TO HEARING ABOUT THE WORK THAT INNOCENT IMAGES IS DOING TO COMBAT THIS GROWING PROBLEM.

I UNDERSTAND THAT THE WORK THAT LAW ENFORCEMENT HAS CUT OUT FOR THEM IN COMBATTING THIS PROBLEM OF THE SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET IS MASSIVE. I HOPE TO LEARN MORE TODAY ABOUT THEIR EFFORTS IN THIS AREA—AND ALSO TO UNDERSTAND WHAT THE DEPARTMENT OF JUSTICE'S RECENTLY PROPOSED LEGISLATION WILL ADD TO THEIR EFFORTS IN THIS REGARD.

THANK YOU ALL FOR BEING HERE TODAY.

MR. WHITFIELD. So at this time, I will recognize our Ranking Member, Mr. Stupak from Michigan, for his opening statement.

MR. STUPAK. Thank you, Mr. Chairman, and thanks for convening this hearing. This committee must take our time to adequately address a number of very serious issues involving child pornography and exploitation on the Internet. These include sexual exploitation of very young children by members of their own family; how to remove pornographic images of children from the Internet; how to keep these images off the Internet; and whether the Department of Justice and the Federal Bureau of Investigation are aggressively investigating and convicting individuals for these crimes.

The sexual abuse and exploitation of children facilitated by the Internet is a criminal activity of horrible dimensions. Last month, we heard the story of Justin Berry, when he was a 13-year-old boy, was manipulated to perform sexual acts in front of a web camera for 5 years. Unlike the case before us today, the FBI and Department of Justice have largely failed to act on the information provided by Justin that would have saved other children from sexual predators. They failed to shut down or arrest the Internet operator of Justin's child pornography site. While the site is now shut down, the operator has fled the country.

Today, we will hear another tragic story of child pornography, this one involving a 5-year-old child adopted from a Russian orphanage for the sole purpose of sexual exploitation. Masha Allen, a young girl of great courage, will tell us of her 5 years of rape and how she became featured in one of the most sought after sets of child pornography images. Masha's adoptive father specifically requested a blonde-haired, blue-eyed 5-year-old girl, and three adoption agencies helped fulfill this

wish. The adoption agency that delivered Masha to this monster did not check the living and sleeping arrangements for the child. The agency did not interview the adoptive father's estranged daughter, whom he had previously abused when she was the same age as Masha. The agency did not perform follow-up home visits after the adoption, as required. The agency delivered a 5-year-old child into a living hell. Masha was rescued only after an undercover Illinois police officer corresponded with her adoptive parents--excuse me, her adoptive father, and obtained his Internet address and a search warrant. When executing this warrant, authorities rescued Masha.

Masha, now 13, will testify how her images became the most sought-after images for pedophiles. We will learn how, because of web file sharing, her terrible ordeal did not end with her rescue.

As the Supreme Court observed over 20 years ago in *New York v. Ferber*, and I quote "The distribution of photographs and films depicting sexual activity by juveniles is intrinsically related to a sexual abuse of children, and harm to the child is exacerbated by their circulation."

Mr. Chairman, this Nation has done very little to stop the Internet exploitation of children like Masha. Last month, we were shocked to learn that 80 percent of the pornographic images on the Internet involve children less than 12 years of age. Thirty-nine percent involve children under 6 years of age, and 19 percent portray children age 3 or younger. Even more disturbing is the fact that at least a third, and perhaps as many as 75 percent of the men caught with these images molest and rape their own children, just as Masha's adoptive father did.

Also today, we will finally hear from the Department of Justice. I will be interested to know why, after 8 months, there has been little follow up in the Justin Berry case, while other cases, like Masha's, received an immediate response with search warrants and arrests. Is there a Constitutional, legal, or resource impediment that Congress does not fully understand? Why are there so few of the tens of thousands of perpetrators who buy, sell, and trade images of young children being raped and tortured are not prosecuted.

After our last meeting, U.S. Attorney General Gonzalez announced that his agency had rounded up 1,100 violent sexual offenders, some of which were child molesters. But from what this subcommittee has heard, 1,100 is a small fraction of the true number of sexual predators in our society. So what is the Justice Department's plan for the rest of these people?

Finally, Mr. Chairman, I know that you plan to call Internet service providers and related businesses that facilitate the transmission of images over the Web. It is important to learn what they believe can be done to prevent the dissemination of the estimated 3.5 million pornographic



images currently on the Internet. I truly hope that when these companies testify, they will have viable plans to remove the horrible images of Masha and other young victims from the Internet. Voluntary action to clean up the Internet has not been successful in dealing with this problem.

I look forward to continuing to work with you to make sure Congress does everything it can to protect our children and prevent images of abuse from flooding the Internet. I yield back the balance of my time.

MR. WHITFIELD. Mr. Stupak, thank you very much, and I am going to go out of order for just 1 minute. Congressman Phil Gingrey is on the first panel with us, and he is the Representative and represents in the Congress Masha Allen and her mother, Faith Allen, and he has some amendments on the House floor that he is going to have to take care of, so Congressman Gingrey, I will recognize you now for any comment you would like to make about Masha and her family, or this issue.

MR. GINGREY. Thank you, Mr. Chairman and Ranking Member Stupak and members of the subcommittee. Thank you for allowing me the opportunity to talk about a remarkable young lady, Masha Allen. Masha is a strong, resilient 13-year-old girl who lives in Georgia's 11<sup>th</sup> District, which I am honored to represent. I want you to hear Masha's story from her in her own words so you can fully grasp what horrors she has lived through, but I guarantee the first thing you will notice, as I did, is her strength of spirit. This little girl was forced to grow up too fast in order for her to process the numerous atrocities that she has experienced. However, Masha's determined spirit gives her the power to stand up and tell her story, illustrating the fact that she is much more than a victim of child sexual exploitation. Masha is a wonderful, willful girl who has decided to be empowered by her situation, and to do something to deter the disgusting world of Internet child pornography that has grown to be a multi-billion dollar industry.

There are many places in this young girl's story where the system failed to protect her from the monster who adopted her. Even before the horrible sexual exploitation began, it is important to understand how she has come to be before you today. You should ask yourself, as I did, how the regulations that exist in international adoption agencies failed, how follow-up visits or school intervention did not rescue this child much sooner, how our Federal laws have really abandoned this area of child welfare, and most importantly, what is Congress's responsibility now that we have heard her story?

The world of Internet child pornography is vast, it is dark, and it is deep. These possessors of child pornography trade these images like we would trade baseball cards, and the business indeed is booming. With the Federal government stretched thin trying to investigate, prosecute,

and convict these numerous and varied possessors of child pornography, advocates are left trying to find new avenues to expose these animals with the goal of deterring future acts of child pornography. This is how the idea of Masha's Law came to fruition: the need to introduce legislation that updates a 20-year-old civil statute and brings it into the 21<sup>st</sup> Century. Current civil law allows victims of child sexual exploitation to recover damages of no less than \$50,000; however, Federal copyright law provides statutory damages of \$150,000 to be awarded to a copyright holder when a song is illegally downloaded from the Internet. There is something wrong with that picture. Masha's Law allows a civil remedy for the dissemination of child pornography to be equal to other illegal downloads. By increasing the amount of damages a victim is able to recover, the Government can accomplish in civil court what is a lengthy and complex process in criminal, stopping the pictures.

Congressman Tierney and I introduced H.R. 4703, Masha's Law, as a companion to legislation in the Senate spearheaded by Senators Kerry and Isakson, to even out a horrible inequity that currently exists in Federal law. It is one step that can be taken to stem the tide of child pornography; however, I know that it is just one step.

As you listen to testimony today, keep in mind the responsibility of the Federal government to protect our children. We need to be proactive. We need to respond to the reality that Internet child pornography is a growing business, one that victimizes our children and leaves them with scars that may never heal. As a physician Member of Congress, it is very important for me to convey to you what a devastating and lasting effect these images have on children. The physical injuries they suffer as a result of child molestation may be more obvious; however, the psychological damages are lengthy and they may not be fully realized until these children are well into adulthood. Child victims struggle with constant feelings of guilt and responsibility for the abuse and betrayal, a sense of powerlessness, and a feeling of worthlessness.

In the case of Internet child pornography, these images are permanent proof of their exploitation. Unfortunately, with these images documented in cyberspace, they are irretrievable and can continue to circulate forever, allowing the child to be victimized each and every time the image is downloaded and viewed. The reality of these crimes are horrible; however, I am encouraged when I see victims who have the courage to tell their story. By supplying Americans with the knowledge of these criminals and arming prosecutors with an avenue in civil court to attack their pocketbooks, we can take tremendous strides toward ending the cycle of pornography.

As I said earlier, I am proud to be here today with such an amazing and courageous girl who is looking to turn her victimization into an avenue to stop this horrendous criminal behavior.

This completes my testimony, Mr. Chairman, and thank you for giving me the opportunity to go out of order.

MR. WHITFIELD. Thank you, Congressman Gingrey.

At this time, I recognize Dr. Burgess for his opening statement.

MR. BURGESS. Thank you, Mr. Chairman, and thank you for having this important series of hearings. As a father of three, I cannot comprehend how people can commit these types of crimes against children. And like my colleagues, I continue to be angered and astonished by the cruelty in the stories that we hear. Just last week, I read another story in my hometown newspaper about a local man charged with sexually abusing children and posting their pictures on the Internet. This is happening in our communities, and it must be stopped. For the sake of our children, we cannot afford to ignore the problem any longer.

Mr. Chairman, I view these hearings as having two main goals. The first, of course, is to educate Congress and the public, and second, to implement stricter laws for deterrence and retribution. I, for one, have learned a great deal more than I ever wanted to know about this topic; however, it is crucial for the safety of our children for all of us to know about these evils so that we can help end this abusive and dangerous practice. It is through the brave souls of children like Justin Berry and Masha Allen that we know so much about this secretive world. Masha, thank you for appearing before us today. Your courage and your dignity are apparent, and you are, in fact, an inspiration to all of us.

I also would like to thank my friend, Dr. Gingrey, for introducing Masha's Law. When enacted, this law will help to ensure that abused children receive a portion of the justice they deserve. I am a cosponsor of the bill and I encourage my colleagues to also cosponsor this important legislation.

As I mentioned before, I feel that the goal of this hearing should be stricter laws regarding this type of abuse. Congressman Gingrey's legislation is a good start. I am also aware that the Department of Justice has ideas regarding an increase in penalties for Internet service providers not reporting known violations. Just one step, as Dr. Gingrey said. It is my sincere hope that these hearings will be a catalyst for even more legislation named at curbing this problem. Our children are depending upon us to do this.

Mr. Chairman, I believe, as we learned in other hearings, we have to hold organizations and Federal agencies like the Department of Justice

accountable for enforcing these laws. It does us no good to continue to pass laws if enforcement is nonexistent.

Mr. Chairman, thank you again for your continued leadership and dedication to this grave situation. I look forward to working with you and others on the committee as we continue to seek solutions to the most egregious deviation from the norm that I think I have ever seen.

I yield back.

MR. WHITFIELD. Thank you, Dr. Burgess.

At this time, I recognize Ms. DeGette for her opening statement.

MS. DEGETTE. Thank you very much, Mr. Chairman, and I want to add my thanks for this series of important hearings. We are all learning a shocking amount, and I am hoping that instead of just emoting for the next few months, we actually have legislation that actually comes out of these hearings.

I want to extend a special welcome to our first witness. Masha, we are really privileged to have you here with us today. You had quite a journey in your life, and I know it has been hard, but we think that there are many, many wonderful things ahead of you and this is just the first one of those many things. You are really brave and you, and also Justin, who testified before, are going to teach us a lot of things that we can help both make laws and enforce laws that will stop this from happening to other children. So you are starting with what I hope will be a lifetime of helping other people.

Mr. Chairman, what happened to Masha is one of the worst cases any of us have ever heard about. It really boggles the mind to comprehend how someone as evil as this was allowed to adopt a young girl. I hope that some light will be shed on how this was allowed to happen, and while it is not under this committee's purview, maybe the hearing will spur some needed changes in the system, the adoption system, to make sure this never happens again.

So Chairman, in preparing for this hearing, I learned that the primary investigators on the case tracked down Masha's adoptive father by using an IP address. They were able to locate his whereabouts by obtaining the IP address, which then led them to his home. Tracing pedophiles and others who produce and distribute child pornography through their IP addresses is an important tool used by law enforcement agencies. In our last hearing, by way of contrast, we heard some testimony from investigators who actually saw a 2-year-old being raped live on the Internet. It was shocking. They were able to trace this to my home State of Colorado. They knew that the perpetrator and the little child were in Colorado, but when they tried to subpoena the IP address, those records had been destroyed by the Internet service provider because ISPs do not keep those records on any kind of consistent basis.

After the hearing, Mr. Stupak and I had the idea, maybe we can do some simple legislation, and what that legislation would say is that Internet service providers have to maintain the addresses for a period of 1 year. This created havoc among the IP community, and I am horrified that the provider community is not working with us on this, because it seems to me to be a very simple piece of legislation. I am going to continue to fight for it. I am telling this to all the people sitting out there in the audience. We are not saying that the Internet providers should keep all of the communications. That would be burdensome. All we are saying is that they should have to keep the IP addresses of their subscribers for a period of 1 year. We are also not saying that we want anybody to violate folks' privacy rights. Instead, just like if you were subpoenaing bank records--and Ms. Grace knows about this. She is a former prosecutor and I used to be a public defender in my youth. If the law enforcement investigators had probable cause, they could go and get a warrant. They could serve that warrant, and they could get that information from the Internet provider. That seems to be a very minor burden to ask to be able to find these horrible criminals who are making crimes on the Internet.

One last thing I will say that I have been thinking about is use of an Internet service provider is a contractual agreement. I would assume that all of the Internet service providers enter into a contractual agreement with their subscribers that they will not commit crimes over that Internet service. And so therefore, if Internet service providers are obtaining evidence of criminal activity under their contract with their subscribers, they should be able to turn that over to law enforcement authorities. I don't understand what the big deal is, but I will tell you this, Mr. Chairman. I have heard that our next hearing is supposed to be a hearing when the Internet service providers come in, and I am very much looking forward to asking them these questions.

In addition, if we have a telecom bill that comes up on the floor next week or the week after, I do intend to work with Chairman Barton, who has said he wants to work with me, and I know you do, too, Mr. Chairman, to make sure that we craft something that is sensible, that is narrowly drafted, and that protects these kids so that all of the kids, just like Masha, that we can find these criminals and we can bring them to justice.

Thank you very much, Mr. Chairman.

MR. WHITFIELD. Thank you, Ms. DeGette, and we do look forward to the Internet service providers when they come to testify. I know that Ms. Fisher is going to be making some comments, I believe, about a recent meeting that she had with some Internet service providers on this issue.

At this time, I recognize the Vice Chairman of this subcommittee, Mr. Walden, for his opening statement.

MR. WALDEN. Thank you very much, Mr. Chairman. I am actually going to waive my opening statement. I very much appreciate our witnesses today, but I want to reserve the extra 3 minutes I will get for questioning of this panel. So I am going to waive at this time.

MR. WHITFIELD. Thank you very much.

At this time, I recognize Ms. Baldwin for her opening statement.

MS. BALDWIN. Thank you, Mr. Chairman.

I want to also acknowledge and commend the subcommittee's work in prior sessions examining the proliferation of child exploitation over the Internet.

Sexual exploitation and the assault of minors is simply one of the most heinous crimes that can ever be committed, yet advancements in Internet technology have greatly enabled the production, viewing, and trafficking of images that are the result of such crimes against children. I applaud this subcommittee's effort to shed light on these abhorrent but burgeoning networks of child predators online, and to educate the public, especially parents, about the dangers such individuals pose to children's access to the Internet.

Having read the New York Times article detailing the harrowing story of Justin Berry and his testimony before the committee several weeks ago, it is clear to me that our Department of Justice has some explaining to do over the way its Child Exploitation and Obscenities Section handles child sexual exploitation over the Internet. Although I am disappointed, as the Chairman is, that Mr. Andrew Osterbein, Chief of CEOS, still will not be testifying today, I hope that Ms. Fisher will be able to offer some insight into the general operations of the Section in handling the referral of online child exploitation cases.

In addition, I am pleased that Mr. Roldan has finally agreed to testify before this subcommittee on its second panel today. I hope we will have an informative discussion regarding the operation of Innocent Images, especially the level of resources that this Section has devoted to investigate sexually explicit images of children online.

Finally, I also want to acknowledge and thank Masha Allen for her courage and the courage you have exhibited in coming before this committee to testify today regarding your experiences. It is really unimaginable to me to know how the international adoption process, which is aimed at giving children a new start through a nurturing family, would become a tool of child predators. Masha, your story is one of both despair and hope. Our adoption system failed you in ensuring that a healthy, stable home was provided to you, and as a result, you have endured years of inconceivable suffering. But yours is also a story of

hope, as law enforcement officers worked to bring you to safety and to provide you an opportunity to live a life free of violence. I admire your courage very much.

I hope that the hearings this subcommittee has been conducting will lead directly to a reduction in such violent crimes against children. Whether it is through informing parents of the dangers of online child predators, or a greater oversight of Federal responses to the issue of child exploitation on the Internet, or new legislative proposals that would deter online pedophilia. Again, I thank the subcommittee for holding this important hearing.

Mr. Chairman, I yield back my remaining time.

MR. WHITFIELD. Thank you, Mrs. Baldwin.

At this time, I recognize Ms. Blackburn for her opening statement.

MRS. BLACKBURN. Thank you, Mr. Chairman. I appreciate that. I thank you for holding the hearing, for the time and effort that you have put into it, and the work that the staff continues to do to help us and work with us on this issue. I also want to thank our witnesses. We appreciate your time and the efforts that you put in to preparing your testimony, and being here with us today. Masha, we are especially happy and we are grateful that you would agree to join us and be with us.

This subcommittee started with these hearings, just as you have heard other members mention today, with testimony from Justin Berry about the pervasiveness of child predators on the Internet. One of the things that has surprised us, it is like anything else you begin to investigate and you look at it, and you realize as you are peeling back the layers that it is much deeper than you ever imagined it could possibly be. So we know that there is a lot of work to be done on this. Justin described for us how the predators help teenagers set up websites and webcams and how they lure them into the sexual acts for money. He also told the committee that the Department of Justice's CEOS failed to act on information provided to them. At the risk of his own life, he provided that information of over 1,500 child predators and distributors of child pornography, yet it seems that the Department of Justice is unconcerned about the information or has chosen not to move forward. We are looking forward to getting that answer, because it is troubling when the FBI has used similar information in Operation Falcon and the Regpay investigations that led to hundreds of warrants and arrests and convictions. It is very difficult for us to comprehend why the information from Mr. Berry has not led to similar actions.

I would have to say, too, I am also concerned about the funding for the Departments that are investigating child pornography and exploitation. I have yet to hear from the Department about their budget submissions to cover the exponentially increased workload that has come

from the investigations. But not all the blame should be put on the Department of Justice. Right now, unfortunately, there are some Members of Congress who would rather see multi-hundred million dollar railroads and multi-million dollar subsidies to corporations that already have \$7 billion in revenues, but yet cannot adequately fund the Departments that are trying to save our children from being victims of these crimes.

The House has acted to implement a nationwide sex offender registry and enhanced criminal penalties for crimes against children. The bill, the Child Safety Act, was passed by the House this past September, but we have got some members in the Senate that have refused to allow the bill to be considered. These members have put their unpolitical ambitions ahead of the protection and welfare of our children. That needs to stop.

I have also had brought to my attention, and I would like to bring to the attention of the committee, a recent investigation by News Channel 5 in Nashville, Tennessee, which is there in my district, and they found a fast-food restaurant franchise all over the country that had been hiring sex offenders to work in the restaurants. This has seriously troubled me because of the actions that we have seen of these despicable people and what they go to to try to get close to the children so that they can proposition the children. This is something we are still working on, Mr. Chairman, and hope to have more information for the committee on that issue at some point soon. We are also looking at the work opportunity tax credit that is there to help in hiring and retraining expellant and wanting to be certain that none of that money is directed towards individuals that would have committed these crimes.

Again, to our panel, I thank you. I thank you so much, Mr. Chairman. Thank you, and I yield back.

MR. WHITFIELD. Thank you, Mrs. Blackburn.

At this time, I recognize Mr. Inslee for his opening statement.

MR. INSLEE. Thank you. I just hope that the courage of Masha Allen and Justin Berry is matched with appropriations by the U.S. Congress for resources to actually do something about this instead of just talk about it.

As a prosecutor, I learned that you could have all the laws on the books and you can have all the fancy library books you wanted in your library of all the great statutes that legislators had passed with great fanfare, but if you didn't have detectives, if you didn't have Internet search tools, if you didn't have prosecutors, if you didn't have victim advocates to help them through this process, this didn't get shut down. This is not getting shut down. It is a \$20 billion industry, we are told, on the Internet. To put that in context, it is a \$3 billion industry for music, just to give a context to how large this is.



So while this has exploded exponentially, the United States Congress, the way it is currently formed, has had tiny little dribs and drabs of additional appropriations to get the prosecutors, to get the detectives, to get this job done. There is no secret here. When Justin Berry had the courage to come forward several weeks ago to talk about this, we learned from these detectives that said I got stacks, I got boxes back in my office that we can prosecute tomorrow if we had any resources to investigate them. So you will know whether Masha Allen's courage is matched by Congress when you see whether or not we do the Federal appropriations to help the FBI and the Justice Department to get to the bottom of this, and whether also we help local communities with their local prosecution, because they are just as important as the Feds are in this. And instead, what this Congress has done is cut funding for local law enforcement in the COPS program and a variety of other places.

So I just want to say I just hope that Congress will show respect for Masha's courage here with appropriations in addition to our verbal thanks for her courage here today. Thank you.

MR. WHITFIELD. Thank you, Mr. Inslee.

The Chairman of the full Energy and Commerce Committee has just come in from a meeting, and at this time I recognize Chairman Barton for any opening statement he may want to make.

CHAIRMAN BARTON. Well, thank you. I am not going to give an opening statement. I do want to appreciate you, Mr. Chairman and Mr. Stupak for continuing to focus on this issue. I want to thank the young lady here who is brave enough to come forward. I want to thank the media representatives who have stood by her and helped to protect her and bring her story to the public. I appreciate what you all are doing.

This is an issue that this subcommittee takes absolutely seriously. I have four children and two stepchildren, of which three are still at home, and on a bipartisan basis, we are going to absolutely guarantee that when the hearings get through, if there is legislation that can be passed at the Federal level to help prevent this obscenity, we are going to do it.

I will be back to ask my questions, Mr. Chairman. I will come back for the second panel. I want to ask our friends at the Justice Department some questions. But on this panel, I just want to say thank you and we will continue to work together to try to find ways to prevent this problem.

Thank you, Mr. Chair.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY  
AND COMMERCE

Thank you, Mr. Whitfield, for holding this hearing.

Today's hearing marks the third in a series of hearings that this subcommittee has held about the sexual exploitation of children over the Internet. Our previous hearings have revealed a shocking and revolting problem. Unfortunately, with regard to the Justin Berry case, these hearings also have raised serious questions about whether the Justice Department and the Federal Bureau of Investigation are being aggressive enough in pursuing those individuals who seek to abuse and exploit children over the Internet.

Today, we are joined by two witnesses who can help explain how the Justice Department and the FBI investigate and prosecute these cases: Alice S. Fisher, Assistant Attorney General for the Criminal Division at Justice, and Raul Roldan, Section Chief of the Cyber Crime Section of the Cyber Division at FBI. I thank you both for taking the time to appear before us this afternoon although I am disappointed that Andrew Oosterbaan, the chief of the Child Exploitation and Obscenity Section at the Justice Department, was not sent to this hearing.

The recent arrests of 1,102 sexual offenders as part of the "Operation Falcon II" investigation are an example of the progress that is being made by the Justice Department, FBI, and other law enforcement agencies in the war against the sexual exploitation of children. I would like to take this opportunity to commend your departments for everything they did to make "Operation Falcon II" a success. Bringing these sexual predators to justice will undoubtedly help to make this world a safer place for our children. However, I think one thing this Committee's investigation has shown us is that there is still much more work to do.

Therefore, in addition to learning how effectively these cases are investigated and prosecuted, I hope Ms. Fisher and Mr. Roldan can comment on the role of Internet Service Providers and credit card companies in these investigations. The previous hearings have demonstrated that the war against child pornography is not simply a matter of law enforcement resources. For example, at our last hearing, agents from the state Internet Crimes Against Children task forces explained that some of their investigations have been thwarted because Internet Service Providers did not retain the data that would allow them to identify online child predators. There may be other areas where more should be required of the Internet and financial services industries with respect to retaining data and conducting due diligence of those who use servers and financial networks to distribute child pornography. As the Committee moves forward with this investigation, we are simply trying to better understand the scope of the problem, the adequacy of law enforcement efforts to fight it, and what we should do legislatively to help put an end to this epidemic of abuse.

We are also joined today by Masha Allen. After being adopted from a Russian orphanage, Masha was raped and molested by her adoptive father, Matthew Mancuso, who placed images of that abuse on the Internet. Thankfully, Mancuso was prosecuted, convicted, and is now incarcerated. However, hundreds of images of Masha's abuse are still on the Internet today. For this reason, Masha bravely decided to come forward and tell the public about the abuse she suffered and about the dangers lurking online. I know appearing before us today must not be easy, Masha, but I hope you will take some comfort in knowing that your story might help others.

With Masha today is our colleague, Congressman Phil Gingrey of Georgia. Congressman Gingrey has introduced a bill, H.R. 4703, also known as "Masha's Law," which he will discuss with us today. This bill will increase the civil statutory damages available to victims of online child exploitation to \$150,000, the same fine that is imposed on those who illegally download music from the Internet. I thank the Congressman for taking the time to appear before the Committee this afternoon.

I look forward to hearing from the witnesses and yield back the balance of my time.

MR. WHITFIELD. Thank you, Mr. Chairman, and I think that concludes all the opening statements, so we will now get to the testimony, which is where we learn most of the important issues that we need to deal with.

You are aware that--I would, first of all, say that on the first panel, obviously, there has been a lot of reference to Masha Allen. Masha is on this first panel. She is 13 years old. She was the young lady who grew up until she was 5 years old in Russia. She was adopted by a gentleman in Pennsylvania and she will be testifying today. In addition, Ms. Nancy Grace, who is with CNN and was a former prosecutor, and has had a lot of experience and interest in this particular subject matter. We welcome her.

In addition, although the next three people that I am going to introduce are not going to be giving opening statements, they may be answering some questions. Mr. James Marsh, who is the attorney for Masha, and then Maureen Flatley, who works with Masha and her family and I understand she is an expert on adoption agency practices and other child issues. And then, of course, we are delighted that Masha's adoptive mother, Faith Allen, is with us today, and we welcome you to the panel as well, Faith.

So we take this testimony under oath because it is an investigatory hearing, and I would ask you now, do any of you have any objection to testifying under oath? I would also advise you that under the rules of the House and the rules of the committee, everyone is entitled to legal counsel, and we know that Masha does have legal counsel. I have already introduced him. But the rest of you, do any of you desire to be advised by legal counsel? Okay.

All right. In case not, then I would ask all of you to stand and raise your right hand, and I will swear you in.

[Witnesses sworn.]

MR. WHITFIELD. Thank you very much. You are now sworn in, you are under oath, and we will begin the opening statements.

Masha, we are going to recognize you first for your 5-minute opening statement, and once again, we genuinely appreciate your willingness to testify before the committee and help bring this issue to the public.

**STATEMENTS OF MASHA ALLEN, C/O JAMES R. MARSH,  
ESQ.; AND NANCY GRACE, CNN NANCY GRACE**

MS. ALLEN. Thank you. My name is Masha Allen. I am 13 years old and I live near Atlanta, Georgia, with my mother, Faith Allen.

When I was 5 years old, Matthew Mancuso, a Pittsburgh businessman who was a pedophile, adopted me. I was rescued almost three years ago when the FBI raided his home in a child pornography citing. After I was rescued, I learned that during the 5 years I lived with Matthew, he took hundreds of pornographic pictures of me and traded them over the Internet.

Thank you for conducting this hearing. Also, thank you for letting me have Nancy Grace here. Nancy is really special to my family and me. She has been an advocate for me and lots of other kids.

The Internet is everywhere in my story. You need to do something about it right away.

I was born August 25, 1992, in Russia. For the first 3 years of my life, I lived at home with my mother and siblings. My mother was an alcoholic. When I was 3 years old, she tried to kill me. She stabbed me in the neck and I almost died. The Government took me away from her and I went to live in an orphanage near my family's home in Russia.

Living in the orphanage was scary and dangerous. There was constant noise and the older children abused the younger ones. I was afraid all the time. I kept all my belongings under my pillow because I was afraid that they would be stolen. After living in the orphanage for 2 years, I found out that I was going to be adopted. Matthew visited the orphanage a couple of times. He seemed nice. He gave me presents. I asked if he was married and if I would have a mother, but he said no. He adopted me in Russia in July, 1998. After that, we left Russia and traveled to his house outside of Pittsburgh. The abuse started the night I got there.

Matthew didn't have a bedroom for me. He made me sleep in his bedroom from the very beginning. He molested me all the time. He made me dress up in adult clothes and even pretended to marry me. Sometimes he kept me chained in the basement. Because he didn't want me to grow up, he only let me eat a little bit of food: plain pasta, raw vegetables, no meat. Five years after I went to live with him, I was only gaining a little bit of weight. When I was rescued, I was 10 years old, but I only wore a size 6X.

Matthew let me go to school and sometimes play with friends, but he told me if I ever told anyone what was happening, that something bad would happen to me. Even though I was the size of a 5-year-old when I was 10, no one at my school ever said anything to anyone. No one from the adoption agency ever came to check on me to make sure I was okay. I never told anyone about the abuse because I was afraid and I thought that no one cared.

A lot of people ask me how anyone could let a pedophile adopt a little girl. I didn't know very much about my adoption until my lawyer

investigated everything. Now, I know there were three adoption agencies involved with my adoption by Matthew. The first was Families Through International Adoption in Indiana. I think Matthew found them on the Internet. He went to an office they had in New Jersey. The State of New Jersey found out that they were operating without a license and closed them down. The same people who worked for that agency just started a new agency in the same office in New Jersey that they called Reaching Out Through International Adoptions. The two agencies are fighting over who was really responsible for Matthew adopting me, but the name of the Families Through International Adoption is on the home study, the immigration paperwork, and the Russian government documents. I think Matthew also paid Families Through International Adoptions. Reaching Out Through International Adoption was really just the same agency, the same people, with different names. A third agency did Matthew's home study to adopt me. They were in Pittsburgh and were called the Family Health Council, but they just changed their name to Adagio Health.

I found out, after I was safe, that none of these agencies asked Matthew any questions. They never really checked him out. They showed him pictures of me, probably on the Internet, before he had a home study to adopt me. In some of the pictures they showed him of me from the orphanage, I was naked. He told them he was divorced and had a daughter that he wasn't close to. I found out later that the reason his daughter didn't talk to him was because she was molested, too.

While I lived with Matthew, no one from any of the adoption agencies ever came to check on me, though the Russian government requires it. As my story came out, we found out two other kids, a boy from Romania and a girl from Russia were adopted by pedophiles, too. Just so you know, 14 other Russian kids have actually been murdered by their adoptive parents. I am sure there are other kids in trouble, but no one seems to care about any of this. When I told my story in public for the first time, all the adoption agencies, not just Matthew's, tried to cover up my story. I lived with Matthew for 5 years. The whole time, he starved and molested me. The whole time, he took pictures of me. I didn't know until later that he was putting my pictures on the Internet to trade, maybe to sell to other pedophiles. I was rescued when the FBI discovered that Matthew had a lot of child pornography on his computer. They came to raid his house; they didn't know I would be there. When the FBI arrested Matthew, I was taken to the hospital, examined, and then put in foster care. My foster mother was Faith Allen. She understood what I was going through because she was sexually abused when she was little. She was a foster child in Georgia when she was

growing up. As soon as I went to live with her, I felt safe. She adopted me on May 14, 2004.

Matthew was prosecuted by the U.S. Attorney's Office in Pittsburgh on September 25, 2003. He was convicted on child pornography charges for all the pictures he had on his computer. He was only sentenced for 15 years in prison for that. I was afraid he would get out of jail too soon. He was convicted again in Pennsylvania State Court on August 23, 2005, of 11 criminal acts for some of the things he did to me. He was sentenced last November to 35 years in prison. I was really upset that he didn't receive a harder sentence. I was even more upset that he was sent to a hospital in Massachusetts so he could be rehabilitated. A person like Matthew can never be rehabilitated. Plus, in this hospital prison, he has free healthcare, free mental health services, and can read magazines, play ping-pong, and have hobbies. No one cares about rehabilitating me. I just lost my Medicaid and my mom has to work doubly hard to pay for the things that I need while Matthew lays around in the hospital playing games.

I was really mad that Matthew didn't get a harder sentence and that he went to an easy prison, but I got much more upset when I found out about the pictures of me that he put on the Internet. I had no idea he had done that. When I found out about it, I asked our lawyer to get them back. He told me that we couldn't do that. I found out that they would be there forever. That is when I got mad and decided to go public with my story. Usually when a kid is hurt, the abuser goes to prison and the abuse is over, but because Matthew put my pictures on the Internet, the abuse is still going on and everyone can see them. People are still downloading them. We get notices from the FBI every time someone is arrested for it. I want every single one of them to go to jail, and they will be punished, but that is a problem too.

I found out last summer that if someone downloads a song off the Internet, the penalty is three times worse than if someone downloads child pornography. I couldn't believe it. How could this be? That is when I decided we had to change the laws about downloading child porn. Senator Kerry and Senator Isakson and Congressman Gingrey and Congressman Tierney introduced bills in Congress that make the penalty the same as downloading songs. That was a few months ago. There hasn't been a vote on it. I want every single Member of Congress to support these bills and want Congress to pass them right away. There are lots of cases of people downloading our pictures, and I want every single one of them to be punished as much as possible.

There might be more pictures of me on the Internet than any other real child. The police told my lawyer that a lot of child pornographers, more than half even, have my pictures on their computers, and there are a

lot of other kids like me, too. People who are doing this should be afraid. We know who they are. A lot of people downloading those pictures are professionals. They are doctors and teachers and ministers who would like to put their pictures on the Internet and tell people what they are doing. People stopped downloading songs when they found out they could be sued. We are going to sue these guys too, every single one of them. I want to tell them you aren't doing this in secret anymore. Everyone can find out who you are.

I am really upset about the pictures on the Internet, and I am upset about what Matthew did to me, physically. A lot of people are surprised that I wanted to go public with my story, but I have been on the Internet since I was 5 years old. Going on television shows wasn't going to hurt me. I did it because I don't think anyone is doing enough about the things that happened to me and a lot of other kids. Talking to John Quinones and Nancy Grace helped me. They were my champions. I felt in charge of my story because of them. I know they will help me to help other kids like me. People need to know about this stuff. The adults who let this happen have just tried to cover it up.

You have to do something about the Internet. Matthew found the adoption agency on the Internet. They let him look at my pictures from Russia on the Internet, even though they didn't know anything about him. Other kids have been adopted by pedophiles the same way. Matthew put my pictures on the Internet after he got me. People are still downloading them, even though he has been in prison for 2 years. We don't even know whether he still makes money from them, even though he is in jail. Even now that I am safe, the Internet is still a dangerous place for me to go. The police detective who found Matthew's home for the FBI said I should never go to chat rooms even for fun things, because they almost always have pedophiles.

Ten years ago, I was a scared little girl in a Russian orphanage. For 5 years, I was held hostage by a monster. But in the last 2 years, a lot of amazing things have happened. John Quinones and Nancy listened to me and told my story to the whole world. I called my Congressman, Dr. Gingrey, who didn't even know me. He introduced a bill in Congress right away to help me and other kids like me. Because of all these things, I believe I can do something for other kids so they don't have to go through what I did.

Some people say we can't control what is on the Internet, but that is ridiculous. If we can put a man on the moon, we can make the Internet safe for kids. That is just common sense. I am going to work hard to protect other kids and make sure people who hurt them are punished. I hope you will help me. You can start by passing Masha's Law right away. That would be a good start.

Thank you.

[The prepared statement of Masha Allen follows:]

PREPARED STATEMENT OF MASHA ALLEN, C/O JAMES R. MARSH, ESQ.

My name is Masha Allen. I am 13 years old and live near Atlanta, Georgia with my mother, Faith Allen. When I was five years old Matthew Mancuso, a Pittsburgh businessman who was a pedophile, adopted me. I was rescued almost three years ago when the FBI raided his home in a child pornography sting. After I was rescued I learned that during the five years I lived with Matthew he took hundreds of pornographic pictures of me and traded them over the Internet. Thank you for conducting this hearing. Also, thank you for letting me have Nancy Grace here. Nancy is really special to my family and me. She has been an advocate for me and lots of other kids. The Internet is everywhere in my story. You need to do something about it right away.

I was born on August 25, 1992 in Novochakhtinsk, Russia. For the first three years of my life I lived at home with my mother and siblings. My mother was an alcoholic. When I was three years old she tried to kill me. She stabbed me in the neck and I almost died. The government took me away from her and I went to live in an orphanage near my family's home in Russia.

Living in the orphanage was scary and dangerous. There was constant noise and the older children abused the younger ones. I was afraid all the time. I kept all of my belongings under my pillow because I was afraid they would be stolen. After living in the orphanage for two years I found out that I was going to be adopted.

Matthew visited the orphanage a couple of times. He seemed nice. He gave me presents. I asked him if he was married and if I would have a mother but he said no. He adopted me in Russia in July 1998. After that we left Russia and traveled to his house outside of Pittsburgh. The abuse started the night I got there.

Matthew didn't have a bedroom for me. He made me sleep in his bed from the very beginning. He molested me all the time. He made me dress up in adult's clothes and even pretended to marry me. Sometimes he kept me chained in the basement. Because he didn't want me to grow up, he only let me eat a little bit of food – plain pasta, raw vegetables, no meat. Five years after I went to live with him I had only gained a little bit of weight. When I was rescued I was 10 years old but I only wore a size 6X.

Matthew let me go to school and sometimes play with friends. But he told me if I ever told anyone what was happening that something bad would happen to me. Even though I was the size of a five year old when I was ten, no one at my school ever said anything to anyone. No one from the adoption agency ever came to check on me to make sure I was OK. I never told anyone about the abuse because I was afraid and I thought no one cared.

A lot of people ask me how any could let a pedophile adopt a little girl. I didn't know very much about my adoption until my lawyer investigated everything. Now I know there were three adoption agencies involved in my adoption by Matthew. The first was Families Thru International Adoption in Indiana. I think Matthew found them on the Internet. He went to an office they had in New Jersey. The state of New Jersey found out that they were operating without a license and closed them down. The same people who worked for that agency just started a new agency in the same office in New Jersey that they called Reaching Out Thru International Adoption.

The two agencies are fighting over who was really responsible for Matthew adopting me. But the name of Families Thru International Adoption is on the home study, the immigration paperwork and the Russian government documents. I think Matthew also paid Families Thru International Adoption. Reaching Out Thru International Adoption was really just the same agency and the same people with a different name. A third



agency did Matthew's home study to adopt me. They were in Pittsburgh and were called the Family Health Council. But they just changed their name too, to Adagio Health.

I found out after I was safe that none of these agencies asked Matthew many questions. They never really checked him out. They showed him pictures of me, probably on the Internet, before he had a home study to adopt me. In some of the pictures they showed him of me from the orphanage I was naked. He told them he was divorced and had a daughter that he wasn't close to. I found out later that the reason his daughter didn't talk to him is that he molested her too. While I lived with Matthew no one from any of the adoption agencies ever came to check on me even though the Russian government requires it. Since my story came out we found out that two other kids – a boy from Romania and a girl from Russia – were adopted by pedophiles too. Just so you'll know, fourteen other Russian kids have actually been murdered by their adoptive parents in America. I'm sure there are other kids in trouble. But no one seems to care about any of this. When I told my story in public for the first time all the adoption agencies, not just Matthew's tried to cover up my story.

I lived with Matthew for five years. The whole time he starved and molested me. The whole time he took a lot of pictures of me. I didn't know until later that he was putting my pictures on the Internet to trade and maybe sell to other pedophiles. I was rescued when the FBI discovered that Matthew had a lot of child pornography on his computer. They came to raid his house. They didn't know I would be there.

When the FBI arrested Matthew I was taken to the hospital, examined and then put in foster care. My foster mother was Faith Allen. She understood what I was going through because she was sexually abused when she was little. She was a foster child in Georgia when she was growing up. As soon as I went to live with her I felt safe. She adopted me on May 14, 2004.

Matthew was prosecuted by the US Attorney's office in Pittsburgh and on September 25, 2003 he was convicted on child pornography charges for all the pictures he had on his computer. He was only sentenced to fifteen years in prison for that. I was afraid he would get out of jail too soon. He was convicted again in Pennsylvania state court on August 23, 2005 of eleven criminal acts for some of the things he did to me. He was sentenced last November to 35 years in prison. I was really upset that he didn't receive a harder sentence. I was even more upset that he was sent to a hospital in Massachusetts so he could be rehabilitated. A person like Matthew can never be rehabilitated. Plus in this hospital prison he has free health care, free mental health services and he can read magazines, play ping-pong and have hobbies. No one cared about rehabilitating me. I just lost my Medicaid and my mom has to work double hard to pay for the things I need while Matthew lays around the hospital playing games.

I was really mad that Matthew didn't get harder sentences and that he went to an easy prison. But I got much more upset when I found out about the pictures of me that he put on the Internet. I had no idea he had done that. When I found out about it I asked our lawyer to get them back. He told me we couldn't do that. Then I found out that they would be there forever. That's when I got mad and decided to go public with my story.

Usually, when a kid is hurt and the abuser goes to prison, the abuse is over. But because Matthew put my pictures on the Internet the abuse is still going on. Anyone can see them. People are still downloading them – we get notices from the FBI every time someone is arrested for it. I want every single one of them to go to jail and really be punished. But that's a problem too.

I found out last summer that if someone downloads a song off the Internet the penalty is three times worse than if someone downs child pornography. I couldn't believe it! How can this be? That's when I decided that we had to change the laws about downloading child porn. Senator Kerry and Senator Isakson and Congressman Gingery and Congressman Tierney introduced bills in Congress that make the penalty the same as downloading songs. That was a few months ago. There hasn't been a vote on it. I want

every single member of Congress to sponsor these bills and I want the Congress to pass them right away.

There are a lot of cases of people who downloaded my pictures and I want every single one of them to be punished as much as possible. There might be more pictures of me on the Internet than any other real child. The police told my lawyer that a lot of child pornographers – more than half even – have my picture on their computers. And there are a lot of other kids like me too. The people who are doing this should be afraid. We know who they are. A lot of the people downloading these pictures are professionals. They are doctors and teachers and ministers. We're going to put THEIR pictures on the Internet and tell people what they are doing. People stopped downloading songs when they found out they could be sued. We're going to sue these guys too – every single one we find out about. I want to tell them, "You're not doing this in secret anymore. Everyone can find out who you are!"

I'm more upset about the pictures on the Internet than I am about what Matthew did to me physically. A lot of people are surprised that I wanted to go public with my story. But I've been on the Internet since I was five years old. Going on a television show wasn't going to hurt me. I did it because I didn't think anyone was doing enough about the things that happened to me and to a lot of other kids. Talking to John Quinones and Nancy Grace has helped me. They were my champions. I feel in charge of my story because of them. I know they will help me to help other kids like me. People need to know about this stuff. The adults who let this happen have just tried to cover it up.

You have to do something about the Internet. Matthew found the adoption agency on the Internet. They let him look at my pictures from Russia on the Internet even though they didn't really know anything about him. Other kids have been adopted by pedophiles the same way. Matthew put my pictures on the Internet after he got me. People are still downloading them even though he has been in prison for two years. We don't even know whether he still makes money for them even though he's in jail. Even now that I'm safe the Internet is still a dangerous place for me to go. The police detective who found Matthew's house for the FBI said I should never go to chat rooms even for fun things because they almost always have predators.

Ten years ago I was a scared little girl in a Russian orphanage. For five years I was held hostage by a monster. But in the last two years a lot of amazing things have happened. John Quinones and Nancy listened to me and told my story to the whole world. I called my Congressman, Dr. Gingery, who didn't even know me. He introduced a bill in Congress right away to help me and other kids like me. Because of all these things, I believe I can do something for other kids so they don't have to go through what I did.

Some people say we can't control what's on the Internet but that's ridiculous. If we can put a man on the moon, we can make the Internet safe for kids. That's just common sense. I'm going to work hard to protect other kids and make sure people who hurt them are punished. I hope you will help me. You can start by passing Masha's Law right away! That would be a good start!

Witness contact information:

James Marsh, Esquire  
Marsh, Menken and Weingarden, PLLC  
81 Main Street  
Suite 305  
White Plains, NY 10606  
914.686.4456

MR. WHITFIELD. Thank you very much, Masha, for your testimony. At this time, I will recognize Ms. Grace for her 5-minute opening statement.

MS. GRACE. Thank you.

After growing up in a loving home where there was nothing the eye could see except soybean fields and pine trees, I suddenly learned about a whole other world, a world I had never known anything about, after the murder of my college sweetheart just before our wedding, my fiancé. In deep grief, I answered the call not just to be a crime victim, but to fight violent crime. I applied, entered, and graduated from law school and had the opportunity to fight violent crime over 10 years in inner city Atlanta. I learned about a world I never knew existed. I learned there were people who do not follow the rules as we know them. During that time, I often represented the single most innocent segment of America, its children.

I learned in court that children speak a language all their own. Prosecutors and social workers are very hard-pressed to understand it sometimes. Once I broke that barrier, I was pained to learn the suffering of our children. No, not children far, far away in some other country, where we can go to bed at night and put our head on the pillow and sleep, and think no, no, not here. Not here in America. They are here in our country, in our States, on this very block. Their suffering knows no barrier, white, black, good students, bad students, the well-to-do, the poor.

I can't begin to tell you what I saw with my own two eyes. How many children ranging from infants to toddlers, elementary schoolers, beaten, raped, used, covered in cigarette burns, sometimes starved, left alone. Child by child, case by case, jury by jury, I tried so hard to make a difference so that one day these children would know when they grow up that someone had fought for them when they were too powerless to struggle.

As the years went on, I began to realize that I was simply putting a band-aid on a mortal wound. That while I could detect, apprehend, and punish child predators, I had no way of stopping future predators. What could be done, I wondered, besides taking the individual offender off the street. I didn't know the answer, so I, like you, just struggled every day and wrestled.

My life path landed me at Court TV and CNN's Headline News, and I have the opportunity to continue this battle in another forum. It is there at Headline News I learned of Masha. When I approached Headline executives, we joined together to tell the world her story. Together, we join forces today to ask you for our voices to be heard.

All the statistics that you have heard became real for me when I met this girl, this little girl, a tiny girl with a big, big voice. As you know, her case highlights so many grievous failings of our system, from illegal foreign adoption, what can go so horribly wrong, to undetected full-blown child molestation that went undetected by teachers, friends, neighbors from age 5 to age 10. Most of us have memories of birthday cakes, of Christmas trees, of dinner around the table when your parents come home from work with your brother and your sister. Not her. Her memories are fear and pain and sexual exploitation at the hands of a man we now know to be a virtual clearinghouse for the most horrific child pornography I have ever laid my eyes on.

In addition to the outright abuse he heaped on his own child, dozens and dozens, hundreds of photos of this girl will be forever on the Internet. Did you hear her say, I asked my lawyer could he get them back? Nothing she said hurt me so much as that, that innocence of a child believing she could take it all back and it would be okay.

Now, technology has made it so easy for these twisted perpetrators to not only fill their appetite for our children, but allow them a window back into the child's home, every home in America where a child is sleeping, is playing, is setting the dinner table tonight, doing their homework. In addition, the so-called Super Highway is just that. It is just a pit stop for predators to gather, to share stories, share their illegal photos, and pass on tips to each other, and they do, to how better meet, seduce, have sex with, and sometimes kidnap our children.

This child, a little girl, has been so very brave. A staggering majority of little children, child molestation victims, never speak out. They never make a peep. Often, they can't. They go on living their lives in quiet desperation with the albatross hanging around their neck of pain and helplessness like no other. Not only has this child come forward and spoken out, she has made her way here to our Nation's capital. How many of us dreamed of being here one day to make a difference?

As you all know, it is written in the oldest book of all, "A little child shall lead us," and so she has. She has displayed more courage in her short life than many of us will in a lifetime. I am here today before you, humble, on behalf of every child victim I ever knew, every child victim I never met, for those who are too young or weak or innocent or simply afraid to speak out, to ask you, sirs and madams, for your help in passing legislation, forcing it through, that will stop child sex predators.

I am so proud to be in this room today that you may often take for granted. My prayer is that you will use your power to protect the weakest among us.

Thank you.

[The prepared statement of Nancy Grace follows:]

## PREPARED STATEMENT OF NANCY GRACE, CNN NANCY GRACE

After growing up in a loving home, where there was nothing but soybean fields and tall pine trees as far as the eye could see, I suddenly learned about a whole other world. Suddenly and without warning, I became a victim of violent crime when my fiancé, my college sweetheart was murdered shortly before our wedding. In deep grief, I answered the call not to simply be a victim of violent crime, but to fight it. In that vein, I applied, entered, and graduated from law school and then, had the opportunity to fight violent crime for over ten years in the courtrooms of inner-city Atlanta. During that time, I learned about a world I had never before known existed. A world where rules, as we know them, do not apply...where those more powerful or cunning prey on others that are weaker or simply more innocent than themselves. During that time, I often represented the single most innocent segment of American life, specifically, children.

I learned in court that children speak a language of their own that prosecutors and social workers are hard pressed to understand. Once I broke that barrier, I was pained to learn the suffering of children...not far, far away in another country so we could say "No, no...never here in America!" and put our head to our pillow at night to sleep easy, but here, in this country, in this region, in this state....on this street. Their suffering knows no barrier, white, black, good students, bad students, the well-to-do, the poor.

I can not begin to tell you what I saw with my own two eyes. How many children did I see? Ranging from infants to toddlers to elementary schoolers beaten horribly, raped, used, covered in cigarette burns, sometimes starved, left alone. Child by child, case by case, jury by jury, I tried so very, very hard to make a difference in these particular children's lives...so that one day they would know when they grew up, that someone had cared, someone had fought for them when they were to young and innocent, too powerless to fight back.

As the years went on, I began to realize that I was simply putting a Band-Aid on a mortal wound... that while I could detect, apprehend, and punish child predators, I had no way of stopping future predators. What could be done, I wondered, besides taking that individual offender off the street after-the-fact? I didn't know the answer...so I just kept on and on and on.

My life-path landed me at Court TV and at CNN's Headline News, where I have the opportunity to continue my battle in another forum. And it is there, at Headline News, I first learned of Masha. When I told Headline News executives of her story, the call to try and DO SOMETHING was heard. Together, we join forces in asking you for her, for our voices to be heard.

The threat of internet child predators is like no other. Some studies put numbers of child internet victims at one in five young internet users. (Youth Internet Safety Survey, 2001). When asked, many of the children stated the solicitation made them feel extremely upset or afraid. Ninety-seven percent of the solicitors were strangers. (Id.) Shockingly, seventy percent of these unwanted solicitations happened when the child was using a computer in their own home.

These statistics became real to me the evening I met Masha, a tiny little girl who now, has a big, big voice. As you know, her case highlights so many grievous failings of the legal system, ranging from illegal foreign adoptions and what can go so horribly wrong, to undetected full-blown child molestation that went undetected by teachers, friends, and neighbors from Masha's age five to age ten. Most of us have memories of birthday cakes, Christmas trees. School bus rides and dinners around the family table each night. Not Masha. Her early childhood memories are those of fear, pain, and sexual exploitation at the hands of a man we now know to be virtual clearing house for internet child pornography.

In addition to the outright abuse he heaped on his own adopted child for years, dozens and dozens of photos of her in pornographic poses remain forever in cyberspace, traded like baseball cards amongst child predators. It is horrific. It is wrong.

And now, technology has made it so easy for these twisted perpetrators to not only fuel their own sick appetites for our children through internet child pornography, but to allow them a window into every home in America where a child is sleeping, playing, setting the table, doing their homework. In addition, the so-called Super Highway is just that, and serves as a pit stop for predators to gather, share stories, share their illegal photos, and pass on tips to each other as to how better to meet little children, then seduce, and even abduct them.

This child, Masha, a little girl for Pete's sake, has been so very, very brave. A staggering majority of child molestation victims never speak out, never make a peep, and go on living their lives in quiet desperation, never really being free of the albatross hanging around their necks, a hidden pain and feeling of helplessness like no other. Not openly has this child come forward and spoken out, she has made her way here, to our nation's capital, to ask for you to act.

As it was written "a little child shall lead us," and so she has. She has displayed more courage in her short life than many will show in a lifetime. I am here today on behalf of every child victim I ever represented, of every child victim I never met, on behalf of those who are too weak or young or innocent or simply too afraid to speak out, to ask you for your help in passing legislation that will not only crack down upon, but help stop ongoing child sex predators.

I am so proud to be here today. My prayer is that you will use your power to protect the weakest among us.

Thank you.

MR. WHITFIELD. Thank you, Ms. Grace. Your testimony was certainly compelling, both of you. You almost don't know where to really start. When you think about this subject matter, it shows, I think, something systemically wrong with our society because I have been told that in the U.S. this problem is so pervasive that it is just mind-boggling for everyone. We have heard testimony about Masha and what has happened to her, and earlier today I found out that there have been 14 adopted children from Russia that have been murdered by their American adoptive parents. We can't fathom why adoptions like this have been allowed to happen, why someone like Mancuso would be able to adopt a child from anywhere.

So one of the questions that I would like to get into to start off with relates to this adoption issue. It is my understanding, and Mr. Marsh, you may be able to help in this, or Ms. Flatley or maybe Ms. Grace, that the name of the adoption agency was the Families for International Adoption, is that the name of the agency?

MS. FLATLEY. Families Through International Adoption is the agency of record.

MR. WHITFIELD. Families Through International Adoption. And Mr. Mancuso initially went to New Jersey, is that correct?

MS. FLATLEY. An office that they had in Cherry Hill, New Jersey, correct.

MR. WHITFIELD. And was that a licensed agency in New Jersey?

MS. FLATLEY. It was not, and the State of New Jersey ultimately suspended their operations.

MR. WHITFIELD. And when did he actually adopt Masha, was it in 1998?

MS. FLATLEY. The adoption was finalized, I believe, in July of 1998.

MR. WHITFIELD. And he went to Russia to pick her up, is that correct?

MS. FLATLEY. Correct.

MR. WHITFIELD. Now, Masha, when you first met Mr. Mancuso in Russia, how was it explained to you about who he was or what he was or why he was there?

MS. ALLEN. I knew that he was going to adopt me because I found out, but they didn't really tell me a lot about him, so yeah.

MR. WHITFIELD. So the people at the orphanage in Russia told you that you would be adopted by an American?

MS. ALLEN. Yes.

MR. WHITFIELD. And I suppose at that time you were maybe excited about it, because from what you said about the orphanage, that was a rather unpleasant experience also. Is that correct?

MS. ALLEN. Yes.

MR. WHITFIELD. And how many times did you meet Mr. Mancuso and spend time with him before you actually went to America with him?

MS. ALLEN. About two or three times.

MR. WHITFIELD. Two or three times?

MS. ALLEN. Yes.

MR. WHITFIELD. And how long did you stay with him?

MS. ALLEN. He came like for the day to visit for a couple hours sometimes.

MR. WHITFIELD. How did you feel about it? Did you want to go to America? Did you feel like that was in your best interest at that time?

MS. ALLEN. Well, he seemed nice. He would bring me gifts.

MR. WHITFIELD. And you knew that he was not married, correct?

MS. ALLEN. Yeah, he told me he wasn't.

MR. WHITFIELD. I guess that was maybe disappointing for you, but at the same time, it was an opportunity for maybe a new life for you. Would that be accurate?

MS. ALLEN. Yeah.

MR. WHITFIELD. Now, when you arrived at Mr. Mancuso's home, it is my understanding that there was only one bedroom. Is that right?

MS. ALLEN. Yeah, he only had one bedroom.

MR. WHITFIELD. And that is when he told you that you would actually be sleeping with him?

MS. ALLEN. Yeah, he told me that because we got in late, and so we just went to bed like first thing.

MR. WHITFIELD. And what did you think about that?

MS. ALLEN. I didn't--

MR. WHITFIELD. Of course, you were very young at the time, weren't you?

MS. ALLEN. Yeah.

MR. WHITFIELD. How old were you?

MS. ALLEN. I was 5. At first I thought it might be normal, because you know how some little kids sleep with their parents, but then after the first night I figured out that there was something wrong because he tried to touch me or something.

MR. WHITFIELD. Now, I know this has been difficult for you, but you did testify also that he actually kept you chained in the basement or in a room or where?

MS. ALLEN. In the basement.

MR. WHITFIELD. How frequently were you chained in the basement?

MS. ALLEN. Maybe like once a month or something.

MR. WHITFIELD. For how long?

MS. ALLEN. A couple hours, or sometimes he would leave me down there for a while.

MR. WHITFIELD. Now, why would he do that?

MS. ALLEN. I don't know.

MR. WHITFIELD. He would just take you downstairs and chain you?

MS. ALLEN. Yeah, he would take my pictures and--

MR. WHITFIELD. Were you nude?

MS. ALLEN. Yes, I was.

MR. WHITFIELD. And did he have you chained to a bed or to a post or--

MS. ALLEN. Yeah, it was a post. There were two of them.

MR. WHITFIELD. Two posts?

MS. ALLEN. Yes.

MR. WHITFIELD. Your hands would be chained, or your legs?

MS. ALLEN. Both.

MR. WHITFIELD. Both?

MS. ALLEN. Yes.

MR. WHITFIELD. That went on for the entire period of time that you lived with him?

MS. ALLEN. Yes.



MR. WHITFIELD. And did he ever tell you what he was going to do with those pictures?

MS. ALLEN. No, he just said he was keeping them. I don't know.

MR. WHITFIELD. So you had no idea that he was trading them over the Internet--

MS. ALLEN. No.

MR. WHITFIELD. --all around the world?

MS. ALLEN. At the time, I didn't think that that was possible. I didn't know.

MR. WHITFIELD. Was there ever a time that you were scared of him, that he might injure you physically or try to harm you?

MS. ALLEN. I was always scared of him, but I don't really think that he--like he never hit me a lot or anything, but I was always scared of him.

MR. WHITFIELD. Now, he did tell you frequently that if you told anyone that you might be harmed. Is that correct?

MS. ALLEN. Yes.

MR. WHITFIELD. Did you ever think about telling someone else? I often wonder when a child is experiencing the type of things that you are experiencing, and we talked to Justin Berry about this as well. Can you explain to us how you felt and why you didn't tell anybody?

MS. ALLEN. I was afraid because I thought he would do something to me, and I didn't know what would happen. At school, they would never talk about any of this kind of stuff, so I was really confused, too.

MR. WHITFIELD. Yes, yes. Mr. Marsh or Ms. Flatley, how is it that an adoption agency--do you have any idea how much money Mr. Mancuso paid this adoption agency?

MS. FLATLEY. We are informed by a reliable source that it was probably in the neighborhood of about \$15,000, which is actually somewhat less than we might have expected.

MR. WHITFIELD. And from the facts of this case and from the information that you have seen on applications or whatever, is there any reason that you can fathom why an adoption agency would approve a gentleman like Mancuso to adopt any child?

MS. FLATLEY. I think the question, Mr. Chairman, is more does an adoption agency like this ever decline to place a child with anyone. The adoption, as we have discussed, was exceptionally unregulated. In fact, I wanted to share with Mr. Walden as an aside that the two other children that we know of who were adopted by pedophiles were adopted in Salem County, Oregon. The perpetrators were prosecuted by the same State prosecutor, who did a wonderful job, by the way. So one of the underlying issues here, and the thing that I think was of greatest concern to us is that when we began to investigate the circumstances around

Masha's adoption, and we certainly believe that the adoption agencies in this case might have been manipulated by him, although it turns out not to have been the case, that they have characterized on national television that the process that went on in Masha's adoption was actually typical.

MR. WHITFIELD. Typical?

MS. FLATLEY. It begs the question in our minds how many other Masha's are there out there. The fact is, no one knows. But the fact is, we are quite certain that there are.

MR. MARSH. We also, in looking into this, Mr. Chairman, believe that the fragmentation in the adoption system worked to Mr. Mancuso's advantage. He was dealing with a well-regarded agency in Pittsburgh to do the home study. He was dealing with another agency headquartered out of State to do the adoption. That agency was dealing with a facilitator in Russia to actually find the child. The facilitator was dealing with a different set of orphanages in Russia to identify and procure the child. So based on the fragmentation in the system, he was able to basically pick and choose the avenue by which he wanted to adopt and I think this is definitely a factor that helped facilitate.

MR. WHITFIELD. Did you say a well-respected agency in Pittsburgh did the home study?

MR. MARSH. We initially thought that it would be an independent social worker or someone very new that had signed off on the home study, which really reads like a public relations document. In fact, I wish we had a copy here today because it is laughable. On the last page of the document, the writer refers to Mr. Mancuso as being a highly moral individual and an outstanding citizen. I am not mincing words here. It says that, ironically and unbelievably. So we believe that it would be a rookie social worker doing the report that he could have conceivably paid off, and in fact, it was a well-respected agency that--

MS. FLATLEY. And Mr. Whitfield, if I may add, we also believe that one of the reasons this happened so readily is the U.S. State Department has effectively become a lobbying arm for the adoption industry. We were quite disturbed to learn from the Salem County, Oregon prosecutor's office who prosecuted the two other pedophiles who adopted children, one from Romania and one from Russia, that the U.S. State Department, this past fall, attempted to coerce him into deleting any references to adoption from his press releases, and in fact, furnished him by e-mail with a draft press release to substitute for the press release that he had written. Now, it should be noted that he really didn't get the adoption connection at the time. It appeared a coincidence to him. But to the extent that you and we have been hampered in our efforts to institute greater and more effective regulation of adoption, it is in large

part because, in fact, the U.S. government has conspired with the system to remain unregulated.

MR. WHITFIELD. So in that instance, it sounds like the State Department was doing a cover-up as well as the adoption agency wanted to cover up.

MS. FLATLEY. Exactly. When Masha's story went public on ABC News Primetime Live in December, 3 weeks before Primetime's story aired, when the adoption agencies--not just the ones involved, I should say, but all of the adoption agencies involved in international adoption, discovered that Primetime was doing a story on this, they inundated ABC News with over 3,000 e-mails attempting to coerce them into canceling the story and/or censoring the story. So to the extent that we have a culture here in this industry that is not about the children, we have a more serious problem and the problem you see in front of you today.

MR. WALDEN. Mr. Chairman, just a point of order. Just for the record, it is actually Marion County. It is the City of Salem, but I know we may want to follow up just for our record, but I appreciate the reference.

MS. FLATLEY. Very good, thank you.

MR. WHITFIELD. At this time, I would recognize Mr. Stupak. We have, unfortunately, 7 minutes to cast a vote, five votes. So we are going to recess and we will be back at 5:00. I apologize once again, and Mr. Stupak will be recognized.

MR. STUPAK. Before we leave, Mr. Marsh, can you give us that document that you testified to where they described Mr. Mancuso--

MR. MARSH. Yes, we can.

MR. STUPAK. --so we can have it for the record to complete your testimony.

MR. MARSH. Absolutely.

MR. STUPAK. Thank you.

[Recess.]

MR. WHITFIELD. I apologize. You have been very patient and at this time, I am going to recognize Mr. Stupak for his line of questioning, then I understand that some people on the first panel, Ms. Grace in particular, have some time deadlines, so I recognize Mr. Stupak.

MR. STUPAK. Well, thank you. Let me thank all the witnesses for their testimony, especially Masha, for your testimony. I think we should also acknowledge your mother, Faith Allen, who is here with you, for her very important role that she plays in your life.

Let me ask you, Masha, if I may, one question. What is most important to you, and from your testimony, I think I can understand it, but I would like you to explain it. Is it getting your images off the Internet, is that the most important thing to you?

MS. ALLEN. Yeah, it is very important for me, but I understand that it is very unlikely that they all will be taken off. The thing that is most important to me right now is trying to help other people and trying to get everyone aware of the topic.

MR. STUPAK. Okay.

Mr. Marsh, you are Masha's attorney, and I know you are contemplating a civil litigation against a number of parties involved in the actual adoption. We have a book here, it is titled "Beyond Tolerance: Child Pornography on the Internet" by Philip Jenkins, in which he describes the great difficulty in removing these images from the Internet. There are literally thousands of collectors all over the world who have thousands of images, some of them decades old. In fact, they call them the classic collections, if I am correct. These people are technologically very sophisticated and a click of the button can give them a new location and a new life. So what can we in Congress and law enforcement do to help remove these images?

MR. MARSH. That is a very good question, Congressman.

The first thought that I had when Masha asked me that question last summer as to whether or not we could remove her pictures from the Internet was in the nature of copyright law, whether or not we could gain any sort of legal control over them so that we would have at least a remedy or a cause of action or some way to assert a legal claim over the images themselves. I was quite frankly--

MR. STUPAK. Would you have to cert that through the victim?

MR. MARSH. Excuse me?

MR. STUPAK. The copyright.

MR. MARSH. We were actually quite surprised to find that that provision was already provided for in the criminal code--

MR. STUPAK. Sure.

MR. MARSH. --and it involved what is the precursor to Masha's Law and had been on the book for 20 years. I was, quite frankly, very shocked to find that our current code provides for civil remedies for a violation of the criminal possession, distribution, and creation provisions. Not surprisingly, I guess, that law had never been used in 20 years. There were no reported decisions, and at the time we were developing a strategy to deal with this, there did come a decision from the Eastern District of Virginia which dealt with this law. It was the first reported case, and that is when we contacted our friends on the Hill about enhancing this.

MR. STUPAK. Sure.

MR. MARSH. And giving the victims an actual cause of action so that they can go in and assert a legal claim over these images.

MR. STUPAK. So I take it that Virginia court then upheld the cause of action?

MR. MARSH. The Virginia court did uphold the cause of action.

MR. STUPAK. For civil--

MR. MARSH. For the civil--

MR. STUPAK. --remedies?

MR. MARSH. --remedies, but it pointed out that due to a quirk in the law, the law--and your question is very relevant here--the law as written only allows a victim to file a claim when they are age 18 or younger.

MR. STUPAK. Right.

MR. MARSH. So once the victim hits age 19, they lose the cause of action. It was just based on inartful drafting.

MR. STUPAK. But no matter when images may have been taken--

MR. MARSH. Exactly.

MR. STUPAK. They may have been 12 years old at the time.

MR. MARSH. So part of what we are doing with Masha's Law is we are removing that limitation. In terms of the--

MR. STUPAK. But if you file a claim--you are under 18, let us say you have filed a claim that probably hasn't been litigated, and then as we talked about the classic collectors may produce these images years later, would you be able to come back and bring a claim?

MR. MARSH. That is what Masha's Law allows us to do. It basically eliminates the cap of age 18, so if you discover that somebody has downloaded the images when you are 20 or 30 or 40, you still have the cause of action to pursue them.

MR. STUPAK. So caps lifted, how about statute of limitations?

MR. MARSH. The statute of limitations, because of the way the law is structured, you can get current downloaders--

MR. STUPAK. Correct, okay.

MR. MARSH. We are actually receiving now notices through the victims of crime--

MR. STUPAK. So every download or every transmission of the image should be a new cause of action?

MR. MARSH. That is correct, and that is how it is worded, and that is what the criminal law recognizes. In terms of the international reach of the problem, I was, quite frankly, shocked by a recent report by the International--it is basically the equivalent of the National Center for Missing and Exploited Children--

MR. STUPAK. Right.

MR. MARSH. Ninety-four countries have no laws regarding child pornography at all.

MR. STUPAK. But still underneath this civil remedy, if you will, that may be available, you still almost have to go at it each image at a time.

MR. MARSH. Absolutely, and that is what we are doing and that is being facilitated for us by the Victims of Crime Act which Congress passed 2 years ago. We are now receiving notices from the FBI and from the U.S. Attorney's Office regarding every prosecution and every investigation involving Masha's pictures. So this really allows us, instead of being a needle in a haystack, where do you start, how do you find these guys, how do you find the perpetrators? We are actually, under the Victims of Crime Act, receiving notices of individual cases, and we are receiving dozens of those at a time of individuals who have pled guilty or been convicted criminally of this crime today, and then we can pursue civil remedies against each one of them.

MR. STUPAK. Let me ask you this. Going back to Mr. Jenkins' book, he states on page 215, let me just read this here. "In spite of all the enforcement efforts of recent years, it is still remarkably easy for any reasonably discreet person to pursue this highly illegal conduct indefinitely, as long as obvious traps are avoided. Law enforcement agencies and their political masters have just had a very poor idea of the organization and the mechanisms of child porn subculture, and above all, of its critical institutions, such as news groups and bulletin boards." Do you agree with that?

MR. MARSH. Absolutely I agree with that.

MR. STUPAK. Is it because of lack of resources, technical know-how?

MR. MARSH. I was surprised, Congressman, and we are always on the lookout technologically for Masha's pictures, different means of transmission, how are these pictures being distributed. I was actually surprised that something called the UseNet--I don't know if you know what the UseNet is. I used it 15 years ago prior to the Internet. The UseNet is still out there and being used to transmit binary pictures of child pornography. Certainly, some of the earliest FBI stings involved the UseNet. I thought it had gone from the face of the Earth, but it is actively in place out there.

What we are also seeing is that pedophile networks are using a Napster-like technology to create basically parallel Internets that only they have access to that are widely distributed, widely diffuse. There is no central server, and images and access to that basically underground Internet are strictly controlled by masterminds in the business of child pornography.

MR. STUPAK. I was going to ask you this question, but let me go to Ms. Grace, if I may.

As you know, it is a crime for anyone other than law enforcement agencies to possess images of child sexual exploitation, so not even news gathering organizations can view it. So the entire field of knowledge, if

you will, or knowing how horrible this really is and how effectively or ineffectively the laws are being enforced are really hidden. Do you think there is a need to have some broader public knowledge of exactly what is going on than there currently is?

MS. GRACE. Certainly, a broader public knowledge of what is going on, but absolutely under no condition further dissemination of child pornography and some misled attempt to inform the public. And as to the earlier question is how do you get these off the Internet? There is no way. They are just like roaches, you can't stop them. But the ones that you can apprehend, they you can stop. And I feel that just like the orphanage that sent her here, the adoption agency that mishandled it to another one that did a fake home study, they go off one title and spring up under another name. If they could just be stopped, just like these--

MR. STUPAK. Sure.

MS. GRACE. Yes.

MR. STUPAK. Ms. Flatley, you were indicating a little bit about--and I would like to hear your views a little bit more on this adoption, because the way Masha has described the problems with the due diligence done by the U.S. adoption agencies that facilitated her adoption from a Russian orphanage, and by the agency that did the home study, it is our understanding that although Mr. Mancuso had a large house, he had no bedroom set up for Masha?

MS. FLATLEY. Correct.

MR. STUPAK. One would assume that when you are doing an adoption home or foster home study, almost the first thing you do would just look to see if the person is going to have their own room, a place to sleep--

MS. FLATLEY. Exactly.

MR. STUPAK. That the basic steps, it seems like even if they were initially taken, there was no follow-up. I find it sort of outrageous, you take a look at it, even the Humane Society does follow-up on placement of dogs and cats and things like that, but we don't do it for children?

MS. FLATLEY. The standards are quite a bit lower for home studies for foreign adoptions than they are, for instance, for adoptions from foster care. So one of the first exercises that we went through when we obtained Mancuso's home study, which we did with some difficulty, was to compare his home study done in Pennsylvania to the one that was done when Faith readopted Masha, and they are like night and day. They have had to submit to all kinds of invasive tests, there were home visits and so forth.

I think the thing that we found the most troubling about this home study is that it is not clear from the language of the home study that they ever visited Mancuso's house even once.

MR. STUPAK. After the adoption?

MS. FLATLEY. Before the adoption. But there is a very vivid description in the home study, which I believe we are having faxed to the committee right now--

MR. STUPAK. Okay.

MS. FLATLEY. --that there was no room set up for the child, that there was an extra room, but it was a mix and match of furniture. Let us say for the sake of discussion that they might have tried to play that off by saying well, he hadn't gotten the child yet and so therefore he wasn't ready. Any reasonable person might suggest that you would go back to make sure that he had, especially because he was a single father.

MR. STUPAK. Well, international adoptions by U.S. child welfare agencies, are there any legal oversights?

MS. FLATLEY. There is not only no real oversight, this has been a conspicuous exception to what is in every other respect in this country a broad regulatory framework at the Federal and the State level. The argument is often made by the industry to foreclose more regulation, but adoption is a State law issue and we can't tell the States what to do. That will come as quite a shock to the States in a number of other important areas. More importantly, they extend that argument by saying in the case of foreign adoption that we simply can't dictate to the foreign governments about what should happen. But that is in two important ways. One is that the Russian government requires post-placement supervision, which almost never happens, or at least doesn't happen enough, but the other issue is that we have had a number of foreign countries who have closed down international adoption to the United States because we apparently suspend American child welfare law when these children enter the country.

So we have some real serious issues in terms of the regulatory framework.

MR. STUPAK. Well, when these children enter the country, do they come in as U.S. citizens then if the adoption is--

MS. FLATLEY. They do and they don't. There has been a change recently that Congress passed a couple of years ago, the Child Citizenship Act, which now facilitates citizenship for kids when they are adopted abroad before they enter the United States as if they were born to their families, but that was probably not in effect when Masha was adopted. But more importantly, so what? What difference does it make, if they are here as illegal aliens or they are adopted by American families or if they are here to visit people, the child welfare system in this country would shut down if we said that families who had children had any kind of right to privacy when there was an issue of the best interest of the child. And so the agency--and I have interviewed the agency at some



length about why there wasn't supervision, and they argued to me that, well, Mancuso didn't want to cooperate with the Russian standards. Well, I believe the Russian standards are the standards we should have, and in fact, that the Russian standards for post-placement supervision are not only quite a bit stronger than ours, we don't have any that are standard.

The other issue is that adoption is largely inherently interstate commerce. Every single international adoption is--I believe that the Energy and Commerce Committee should have jurisdiction over this issue. I have said that for years. But ultimately, if we are allowing children to enter this country with people that we have not done adequate due diligence on, and then on top of it we are going to argue that we have no moral or legal authority to check on those children once they get here, we are out of our minds.

MR. STUPAK. Well, I believe the chairman and everyone on this committee would agree that the Energy and Commerce Committee certainly has jurisdiction over this. This subcommittee though, Oversight and Investigations, we do not write legislation. We can only make recommendations, but we are very interested and we will make sure we get those recommendations to the proper people.

MS. FLATLEY. Thank you very much.

MR. STUPAK. Thank you. Thank you all.

MR. WHITFIELD. Thank you, Mr. Stupak. Mr. Walden is going to be recognized next, but I understand, Ms. Grace, that you have another commitment and we need to dismiss you. But before you go, Mr. Walden, do you have a specific question for her?

MR. WALDEN. I just have one quick question for Ms. Grace, and first of all, I appreciate all the work you have done in this area, both as, I guess, a prosecutor, but also on the air, I think you have gotten the message out to Americans on the kind of problem that we have uncovered here and that you have continued to do work on.

I guess this morning you were on Good Morning America and had some ideas about how we might be able to combat the proliferation of--

MS. GRACE. Yes, I did.

MR. WALDEN. Can you share those ideas?

MS. GRACE. Yes, and I consider them to be more innovative than simply increasing the time that felons would do behind bars, which I coincidentally am all for.

First of all, I feel that parents don't know what their children are doing online. It is very obvious. I mean, if you look at Columbine, they were cooking up bombs in the garage and they didn't know that, much less where they go online. I think that it would be a fantastic idea, and so easily done, just as you get a readout of what calls you have made on

your cell phone every month to pay another dollar to AOL and they could for \$6 a month to get a readout of where your computer has gone. Also, when you buy a beer, not that any of you esteemed drink or imbibe, but when other people buy a beer, look at it. There is a warning there, and I don't understand why on laptops and desktops all over the country there is not a warning for adults to see. Also, I don't know how many of you have a TiVo, but to get into the thing, you have to go through a tutorial. And I don't understand why every time you buy a computer, a new computer, which can be controlled through interstate commerce, there is not a warning. They are on microwaves, they are on beer bottles, they are on cigarettes, and none as to the dangers of the Internet. We do public warnings all the time. I have a very extensive list of ideas which I will be happy to submit to the committee.

MR. WALDEN. Thank you. That would be most helpful. I appreciate it. I realize you do have to leave. I have got questions for the other panelists.

MS. GRACE. Yes, sir.

MR. WALDEN. Thanks again for your good work.

MS. GRACE. And again, thank you for having me.

MR. WHITFIELD. Chairman Barton, Ms. Grace is going to be dismissed. She has--

CHAIRMAN BARTON. I don't have any questions for this panel, Mr. Chairman.

MR. WHITFIELD. Ms. Grace, thank you very much for being with us, and thank you for the leadership that you are providing on this issue.

MS. GRACE. We are focusing on you. This committee is so kind to hear us tonight on our live show and taking calls from America, so I hope you listen.

MR. WHITFIELD. Okay.

MS. GRACE. Thank you.

MR. WHITFIELD. Thank you.

Mr. Walden, you want to continue?

MR. WALDEN. Yes, thank you, Mr. Chairman.

Ms. Flatley, if I might ask you just a follow-up question. I may have missed this in the intervening period. What has become of the agency in Pennsylvania that did the home study review that said that her adoptive father was this marvelous moral character?

MS. FLATLEY. As is the case with the other two social service agencies involved in this, they continued to operate and thrive. I believe, although I am not positive, that the agency in Pennsylvania may receive actually some Federal funding because they do quite a bit of family planning. They are all in business. They are all considered leaders--

MR. WALDEN. Did they suffer any penalty?

MS. FLATLEY. Absolutely none. This is the first public discussion. Today is the first day that their identities have been revealed publicly.

MR. WALDEN. What is the name of the agency that did the reviews?

MS. FLATLEY. The agency in Pittsburgh was called the Family Health Council at the time that the home study was done. They recently changed their name to Adagio Healthcare. They are based in Pittsburgh.

MR. WALDEN. Mr. Marsh, are you Masha's legal counsel?

MR. MARSH. Yes, I am.

MR. WALDEN. Is there not some grounds here for litigation?

MR. MARSH. There are plenty of grounds, and to be quite frank with you, we have been so busy in the 6 months since I met Masha trying to figure out exactly what happened, who were the players, how it happened, we have a fraction of the documentation that we believe is out there. Because of the confidentiality concerns, we are only able to get it through a third party, not through the agencies themselves. Despite waivers and requests and letters, they are hiding behind Mr. Mancuso's right to privacy and refusing to release those documents to us so we can gain a fuller understanding of exactly why this happened. We know why it happened, excuse me, we don't know exactly how it happened and we are going to get to the bottom.

MR. WALDEN. Mr. Chairman, that almost sounds like something we ought to be looking at and perhaps use our subpoena power to get there.

MS. FLATLEY. Well, if I may add that, when James and I because involved in this case, we had a sense of what had happened, but even we, I don't think, under any circumstances anticipated the alacrity with which this adoption took place. And we have reached out to all the social service agencies involved because we initially believed that they, in fact, had been somehow manipulated and would want to join with us in helping to close these loopholes and do a better job.

As I said before, not only did they argue that this adoption was routine and this is how they always did business, but in fact, when we began a discussion with them to obtain voluntarily from them a copy of Masha's home study, they asserted that Mancuso had a right to privacy and they could not disclose it. We ended up getting it from another source in November, but to your point, I think that what has been the most troubling about this is that the more we have investigated it, the more we realize we needed to know, so in fact, this case is much more complicated than we originally thought it would be.

MR. WALDEN. And I appreciate the work you are doing, and just for the record, I am a big fan of adoption. My two brothers are adopted, my niece is adopted.

MS. FLATLEY. Adoption is what saved this child, and I just want to say that at many points in this discussion, James and I and Masha and

Faith have been accused of trying to somehow undermine adoption, stop adoption, being anti-adoption. Nothing could be further from the truth. Let it be clear that adoption saved this child's life. Faith adopted her.

MR. WALDEN. No, I--

MS. FLATLEY. And that Masha felt so strongly about the power of adoption in her own life that she actually wrote a letter to President Putin which was hand-delivered to him several months ago. So I think we all want to say very clearly that the only good adoption is a safe adoption--

MR. WALDEN. Right.

MS. FLATLEY. --and it makes it safer for all consumers of adoption services to regulate adoption effectively and consistently.

MR. WALDEN. Masha, if I could, first of all, thank you for speaking out. I can't begin to imagine the pain and suffering and sorrow you have gone through, but what you are doing today obviously will have enormous benefit for others.

When Justin Berry was in that very seat not long ago, testifying about the problems he encounters on the Internet and all, I asked him a similar question, one I want to ask you. As a child, what advice do you have for parents and adults and for other children who might be in your situation, who might be watching this sometime and say I know somebody who may be in this situation. How could your friends have helped? What should we be looking for? What would you tell other kids who might find themselves in a situation similar to that which you were in?

MS. ALLEN. I would just say that even if you are threatened, you should speak out because that is the only way that it is going to stop.

MR. WALDEN. Who do you speak out to, your teacher, your pastor, your--

MS. ALLEN. Whoever you trust more, because it is easier to talk to someone you trust.

MR. WALDEN. Right.

MS. ALLEN. And I think parents should be watching out for their kids, too, like and doctors should be checking to see if the kids have any problems or eating disorders or anything like that.

MR. WALDEN. Did you get any medical treatment in those years when you were--

MS. ALLEN. Yes, I did.

MR. WALDEN. And the medical providers didn't question your health status?

MS. ALLEN. No.

MR. MARSH. She did receive, if not routine, sporadic healthcare. We did get a copy of her medical records, and ironically, in the context of all of this, we got the school records. It is obvious to me that Mancuso

was a very savvy operator. His initial contact with the school was with the school nurse, who he immediately befriended, knowing that as a medical professional on site she would be a natural conduit for any sort of abnormalities or information. Although it is hard to believe that the growth charts that are in the school records show Masha at the 10<sup>th</sup> percentile in terms of weight, and she was quite a bit taller, so that even suppressed her more, because her height was normal but her weight was severely underweight. So consistently throughout her school record, we have--and we have a doctor here--a growth chart which indicates a child year after year after year, growing--

MR. WALDEN. Did they never ask?

MR. MARSH. They never asked, according to Masha. No one ever asked anything about her. Nobody ever asked anything about her time in Russia, why she came to America. It was as if the person is in front of your house screaming rape and no one is hearing, seeing, or realizing what is going on right under their nose.

And so for us, at least, the growth charts were a chilling indication that something was very wrong with this child and someone should at least have made an inquiry about her health status, given that she was so underweight.

MS. FLATLEY. If I could just add, I mean, having interviewed a lot of people that were involved in life, what is shocking to me as a parent myself--

MR. WALDEN. Nobody noticed.

MS. FLATLEY. --is that her teachers never said anything, despite the fact that she looked emaciated. The pictures of Masha when she was rescued, she literally looks like a concentration camp survivor. The social service agencies involved, there were three, none of them checked on this child. The neighbors never said a word, obviously. It is somewhat mystifying to me that her physician did not somehow want to explore even perhaps a neglect allegation because she wasn't growing.

So it is one of the issues in Masha's case that is particularly troubling is that this child was failed by literally everyone that could have protected her.

MR. WALDEN. Well, Masha, thank you, and thanks to all of you on our panel, and to my colleague for the work that you are doing to bring light to this problem. Hopefully we can bring a little legislation to this problem, get a handle on it.

So thank you, and thank you, Mr. Chairman.

MR. WHITFIELD. Thank you, Mr. Walden.

Mr. Chairman, Chairman Barton, do you have any questions for this panel?

CHAIRMAN BARTON. Not for this panel. I am here to support this panel, and I have questions for the second panel.

MR. WHITFIELD. Thank you.

Well, I want to thank those of you on the first panel. Masha, we once again appreciate very much your coming forward. You have been immensely helpful. Mr. Marsh, Ms. Flatley, we will continue to stay in touch with you. Ms. Allen, best wishes to you, and Congressman Gingrey, thank you very much for being with us today, and for your legislation as well. This panel is dismissed.

MR. MARSH. Thank you, Mr. Chairman.

MR. WHITFIELD. At this time, we will call the second panel. First, we have the Honorable Alice Fisher, who is Assistant Attorney General for the Criminal Division, U.S. Department of Justice, Washington, D.C.; and Mr. Raul Roldan, who is the Section Chief for the Cyber Crimes Section of the Cyber Division, FBI, U.S. Department of Justice. And we have Mr. Arnold Bell, who is the Unit Chief, Innocent Images Unit, FBI, U.S. Department of Justice. They are also joined by Mr. Swecker from the FBI.

As you all--I want to apologize to this panel as well. I know when you arrived at 2:00 you thought you would probably be home by 6:00, but we had a lot of interruptions, and thank you for your patience. We appreciate your being here.

You are aware that the committee is holding an investigative hearing, and when doing so, we have the practice of taking testimony under oath. Do any of you have any objection to testifying under oath? And of course, under the rules of the House and rules of the committee, you are entitled to be advised by counsel. Probably all of you are lawyers, so I am assuming you don't need to be advised by counsel.

So if you would please stand and raise your right hand, I would like to swear you in.

[Witnesses sworn.]

MR. WHITFIELD. Thank you. You are now under oath. Ms. Fisher, you may give your 5-minute opening statement.

**STATEMENTS OF ALICE S. FISHER, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, UNITED STATES DEPARTMENT OF JUSTICE; AND RAUL ROLDAN, SECTION CHIEF, CYBER CRIME SECTION OF THE CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE**

MS. FISHER. Thank you, Mr. Chairman, Ranking Member Stupak, Chairman Barton, and other distinguished members of this committee. Thank you for inviting me here to testify before you today about the Department of Justice's efforts to protect children from sexual exploitation on the Internet, and thank you for having these hearings that shine light on this horrific growing problem.

The anonymity of the Internet has provided opportunities for criminals who prey upon our children. Our children face a threat from molesters who troll the Internet, looking for young victims so they can lure and molest. Other criminal elements sponsor sex tourism aimed at children and facilitated by the Internet, but the most pervasive crime against children perpetrated on the Internet is child pornography. The mere thought, yet alone depictions, of children, some still in their infancy, being subjected to such degrading treatment turns the stomach and boggles the mind. Despicable, unconscionable, intolerable, sickening. These are words you have used over the past weeks describing this problem, and I could not agree with you more.

In my role at the Department of Justice and as a mother of two boys, 4 and 8, I would like to see all child predators put behind bars. I am committed to doing what we can for this problem.

You have heard testimony about the scope of the problem, which is enormous, but make no mistake, the investigation and prosecution of those who generate, traffic in, and possess child pornography is a top priority of the Department of Justice. The Attorney General has reiterated this time and again, and he is personally committed.

The Department of Justice prosecutes these cases in all 94 U.S. Attorney's Offices across the Nation. The Criminal Division also through its Child Exploitation and Obscenity Section coordinates nationwide investigations, takedowns, and also prosecutes these cases. These career prosecutors, as well as State prosecutors, as well as Federal and State law enforcement, I thank them all for their service, for they have one of the hardest jobs. I can tell you that I am still haunted today by some of the materials which I have reviewed, but these professionals who work day in and day out to protect our children are exposed to and are forced to review these horrific materials, photos, videos, every day, and then come home to their own children. These professionals come to work every day because they are committed to making a difference and protecting our children, and stopping the pain that we have heard so much about over these weeks at your hearings.

The Department has made great progress, and I want to take a moment just to give you a few examples of some of our recent prosecutions and takedowns. First, an example of trading in child pornography. The Internet, as you know, has allowed predators who

create and traffic in child pornography to create a virtual community where they can share and trade in these disgusting images. One such community, a chat room that went by the name "Kiddypics & Kiddyvids" allegedly included among the images, a live streaming video of one member sexually molesting an infant. Law enforcement conducted an undercover operation resulting in charges against 27 individuals in the U.S., Canada, Australia, and Great Britain, and seven child victims of sexual molestation were identified.

Second, an example of sexual abuse of children. Child predators have also used the Internet to provide so-called molestation on demand. In one case, a predator took scripts here in this country, so-called orders, then went to Cuba and to Ecuador and paid poverty-stricken families to let him molest their children, some of whom were under the age of 12. He would then send those pictures back over the video of him playing out these sick fantasies. We caught that man responsible for this ring. We prosecuted him and his co-conspirators, and he received a 100-year prison term.

But our efforts did not stop there. We launched Operation Lost Innocence to target Mariscal's customers across the country, and to date, that operation has resulted in 107 searches, 55 arrests, and 44 convictions.

Third, we also prosecute, as we must, the financial facilitators. We pursue the companies that provide the means by which these predators can create, market, and sell these horrendous images. In the Regpay case, for example, we prosecuted the Belarus company that had provided credit card processing services to hundreds of child pornography sites. We secured guilty pleas from the executives, but again, that was only the beginning. That Regpay case gave rise to a follow-on investigation, which resulted in 341 domestic and approximately 703 foreign arrests, 254 indictments, and 241 convictions.

I could go on all day with examples like these, successful prosecutions of horrendous crimes. Prosecuting child predators is and remains a top priority for the Department of Justice. The Attorney General made this clear when he announced the Project Safe Childhood Initiative, which seeks to integrate Federal, State, and local efforts to prosecute child pornography, to educate the communities, and to provide enhanced training for law enforcement, and \$14 million will go out this year to support ICECs across the country who prosecute these things on a State and local level.

Federal prosecutions, investigations, and caseloads in these matters have dramatically increased in the last decade, and the Department is working aggressively, but is it enough? You heard from Ernie Allen of NCMEC last week who told you that 1,500 leads come into the Cyber



TipLine every week, and 50 percent of those come from ISPs, but it will take all of us to combat this problem. I pledge to you, as the Attorney General has pledged, that the Department is committed and dedicated to this task.

Congressman Barton said he had never been more revolted in preparing for a hearing than having to read the material about these predators who prey on our most vulnerable, our children. I have looked at the pictures and I have looked at the videos, and sir, you are right.

I thank you for this hearing, and I look forward to answering your questions.

[The prepared statement of Hon. Alice S. Fisher follows:]

PREPARED STATEMENT OF THE HON. ALICE S. FISHER, ASSISTANT ATTORNEY GENERAL,  
CRIMINAL DIVISION, UNITED STATES DEPARTMENT OF JUSTICE

**STATEMENT OF  
ASSISTANT ATTORNEY GENERAL ALICE S. FISHER  
BEFORE THE COMMITTEE ON ENERGY AND COMMERCE  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS**

**CONCERNING SEXUAL EXPLOITATION OF CHILDREN ON THE INTERNET  
MAY 3, 2006**

Mr. Chairman, Ranking Member Stupak, and distinguished Members of the Subcommittee, thank you for inviting me to testify before you today about the efforts of the Department of Justice to protect children from sexual exploitation on the Internet. In my comments this morning, I will outline for you how the Department is meeting President Bush's commitment that, "Anyone who targets a child for harm will be a primary target of law enforcement." In a recent speech at the National Center for Missing and Exploited Children, Attorney General Gonzales underscored our mission, stating that, "We cannot, and will not, tolerate those who seek to abuse or exploit our children." The Department of Justice furthers this mission through the efforts of the Criminal Division's Child Exploitation and Obscenity Section, and through the efforts of the 94 United States Attorneys' Offices around the country, to hold those who would victimize our children accountable for their actions.

In his speech, the Attorney General said that he welcomed the recent interest in this issue by Members of Congress and the press, as do I, because a key to preventing this victimization of children is educating the public. The American people need to appreciate the scope, the nature, and the impact of this problem on our youth. It is a problem that demands a community-wide response. The Attorney General noted with astonishment how many online predators there are and how aggressively they act toward children. The threat of the online sexual enticement of our

children is serious and it is real, and law enforcement will continue to work hard to protect our children from it.

The Attorney General noted the unprecedented efforts and successes by law enforcement — in the Criminal Division’s Child Exploitation and Obscenity Section, in the Federal Bureau of Investigation’s (FBI’s) Innocent Images Unit, in U.S. Attorneys’ offices nationwide, and in the Internet Crimes against Children task forces. And he also made clear the Department’s commitment to doing even more to protect children from online exploitation and abuse.

When Principal Associate Deputy Attorney General and United States Attorney for the District of Montana William W. Mercer testified before you on April 6, 2006, he gave you a general overview of the Department’s efforts to protect children from sexual exploitation. While I will try not to cover the same material, I will necessarily address similar topics.

As you know, federal law, codified at Chapter 110 of Title 18, United States Code, prohibits all aspects of the child pornography trade, including its production, receipt, transportation, distribution, advertisement, and possession. Federal law, codified at Chapter 117 of Title 18, United States Code, also prohibits enticing children to engage in unlawful sexual activity.

As the Attorney General said in his recent speech at the National Center for Missing and Exploited Children, “Most images today of child pornography depict actual sexual abuse of real children. Each image literally documents a crime scene.” In other words, each image is graphic visual evidence of sexual abuse.

The Attorney General also thought it was important to explain just how significant the problem of child pornography is in our society. Many understand it is a problem in the abstract,

but do not have a genuine grasp of its gravity and pervasiveness. This is not light stuff: the images today are graphic, sadistic, and horrific. They are often pictures or video recordings of demeaning and wicked abuse of real, innocent children. In part because of the Internet, the images grow even more explicit and vulgar by the day, and involve younger and younger children — with some even depicting the molestation and penetration of babies and infants.

I have seen some of these images, and, just like the Attorney General said, they make your stomach turn. I don't think many people realize how difficult it is for the law enforcement professionals who have dedicated their careers to this difficult work. It is revolting to view even one of these images. Imagine having to view hundreds and thousands of them – repeatedly, on a daily basis – in order to build the cases against offenders. That is what these dedicated professionals do, and it is challenging and traumatizing on a deeply emotional level. I join the Attorney General in personally thanking all of those in law enforcement and elsewhere who are enduring those challenges and working hard to protect our children.

As you know, these disturbing images are only the beginning of a cycle of abuse. Once created, these images become permanent records of the abuse they depict, and can haunt the victims literally forever once they are posted on the Internet. Advances in technology have made it easier and easier for offenders to share these images with each other – and to cover their tracks while doing so – making it very difficult to remove the images from circulation once they have been posted on the Internet. Even more disturbing, though, is that offenders rely on these images to develop a “plan of action” for targeting their next victim, and then use the images to “groom” their victims into submission by lowering their inhibitions.

We remain committed to stopping this cycle of abuse, and the dramatically increased

volume of cases the Department has brought reflects that. The increase in caseload is evident both throughout the 94 U.S. Attorneys' Offices and within Criminal Division's Child Exploitation and Obscenity Section (CEOS). According to the Executive Office for United States Attorneys, total federal prosecutions of child pornography and abuse cases rose 358%, from 344 cases in FY 1995 to 1,576 cases in FY 2005, and the increase in prosecutions continues unabated. Likewise, the Child Exploitation and Obscenity Section (CEOS) within the Department's Criminal Division increased its caseload, including child pornography cases and investigations, by more than 400% over three years. While the dramatic increase in the number of prosecutions is an indicator of the importance of this issue to the Department, it is but one indicator. In addition to increasing the number of investigations and prosecutions it brings, the Department is constantly seeking to improve the quality and import of its cases by adapting to the ever-changing methods by which the predators seek to purvey these horrible images and evade detection by law enforcement.

On February 15th, the Attorney General announced a new Department initiative, "Project Safe Childhood," aimed at further improving law enforcement efforts to combat the growing threat of child pornography and enticement offenses. This initiative will provide for more coordination by law enforcement at every level in investigating and prosecuting child exploitation cases, and in identifying and rescuing children; it will provide a national framework for effectively pursuing the local leads that result from large national operations; it will enable us to bring even more federal prosecutions for child exploitation offenses throughout the country; it will make more training available for officers and prosecutors; and it will further ongoing community education and awareness efforts. The components within the Department, including

the Child Exploitation and Obscenity Section and the U.S. Attorneys' Offices, will be central to making Project Safe Childhood a success. The Department is moving closer to formally implementing Project Safe Childhood, and the Attorney General has made clear that this is one of the highest priorities for the Justice Department.

As I have noted, and as this Committee knows, child pornographers have shown themselves to be remarkably adept at seizing upon each technological advance – from webcams to instant messaging – and turning it to their own malevolent purposes. It is therefore incumbent upon law enforcement to respond to – and indeed anticipate – these technological advances by taking full advantage of our existing computer forensic capacity. To that end, the Criminal Division created a special High Tech Investigative Unit (HTIU) within CEOS in August 2002. The HTIU consists of computer forensic specialists, who team with expert prosecutors, to ensure the Department of Justice's capacity and capability to prosecute the most complex and advanced offenses against children committed online. HTIU computer forensic specialists provide expert forensic assistance and testimony in districts across the country in the most complex child pornography prosecutions conducted by the Department. The HTIU also regularly receives and reviews tips from citizens and non-governmental organizations, such as the National Center for Missing and Exploited Children, and initiates investigations from these tips.

As you know, child pornography is distributed over the Internet in a variety of ways, including online groups or communities, file servers, Internet Relay Chat, e-mail, peer-to-peer networks, and commercial web sites. We investigate and prosecute offenses involving each of these technologies and employ sophisticated investigative techniques, including undercover operations, to do so. While the investigation of a commercial child pornography web site may

seem like a straightforward matter, I can assure you that it is not. Such an investigation requires us to determine where the servers hosting the web site are located, identify the persons responsible for operating the web site, and follow the path of the many financial transactions offenders use to purchase the child pornography, whether by credit card or other means. Such cases require detailed information about all aspects of the transaction in order to determine the exact identity and location of the offenders, who often take elaborate steps to shield their identity and prevent detection. Additionally, many of these cases require coordination with law enforcement from other countries. It is essential that these complex cases be handled by law enforcement agents and prosecutors with the necessary specialized expertise.

In short, the Department is committed – as it must be – to matching and indeed exceeding the level of innovation demonstrated by the online offenders. For example, CEOS' HTIU has developed a file server investigative protocol and software programs designed quickly to identify and locate individuals distributing pornography using automated file-server technology and Internet Relay Chat. Because file servers, or "f-serves," provide a highly effective means to obtain and distribute enormous amounts of child pornography files, 24 hours a day and 365 days a year, with complete automation and no human interaction, this trafficking mechanism is a premier tool for the most egregious child pornography offenders. The protocol recommends standards for identifying targets, gathering forensic evidence, drafting search warrants, and making charging decisions. It is designed to ensure that agents and prosecutors understand all aspects of these complex investigations. The software program written by the HTIU automates the process of stripping from the computers used as file-servers all of the information necessary to make prosecutions against all of the individuals sharing child pornography with the file-server

computer.

A recent example of HTIU's success is the case of *United States v. Schiffer* (D. D.C). This case was part of HTIU's initiative, and was developed in-house. CEOS is prosecuting the case together with the United States Attorney's Office for the District of Columbia. The defendant pled guilty on October 14, 2005, to one count each of using his computer to advertise, transport, receive, and possess child pornography. By operating his personal computer as a file server, he allowed selected files to be downloaded and uploaded by the public from and to his computer. He also advertised on specified Internet Relay Chat (IRC) channels a willingness to receive or distribute files, making available to the public a collection of approximately 11,000 image and movie files of child pornography and erotic depictions of children over the course of about five months beginning on or about September 1, 2004 and continuing until on or about January 14, 2005. A particularly shocking fact is that among the items seized from the defendant's bedroom, pursuant to a search warrant, were two boxes of catalogued correspondence between the defendant and roughly 160 prison inmates, the vast majority of whom had either sexually assaulted or murdered children. At his sentencing, currently set for June 28, 2006, the defendant faces a minimum of 15 years and a maximum of 30 years in prison for advertising child pornography and a five-year mandatory minimum sentence for transporting and receiving child pornography.

Law enforcement has launched several national enforcement initiatives against the use of peer-to-peer networks to commit child pornography offenses. These initiatives include operations by the Federal Bureau of Investigation, the Department of Homeland Security, Immigration and Customs Enforcement (ICE), and state and local Internet Crimes against



Children task forces, which are funded through the Department. To give you a sense of the scope and impact of these operations, the FBI's Operation Peer Pressure, as of January 2006, has resulted in over 300 searches, 69 indictments, 63 arrests, and over 40 convictions. The Criminal Division, and CEOS in particular, contributed to the development of Operation Peer Pressure by reviewing the investigative protocol to be used, providing training to the agents involved in the operation, and drafting model search warrant affidavits for agents to tailor as needed.

CEOS is currently coordinating 18 multi-district operations involving child pornography offenders. These investigations are national in scope and have the potential for maximum deterrent effect on offenders. Nearly each one of the eighteen investigations involves hundreds or thousands, and in a few cases tens of thousands, of offenders. The coordination of these operations is complex, but the results can be tremendous. By way of example, the FBI is currently investigating the distribution of child pornography on various eGroups, which are "member-only" online bulletin boards. As of January 2006, the FBI indicated that the investigation has yielded over 180 search warrants, 89 arrests, 162 indictments, and over 100 convictions.

While these statistics reflect the Department's commitment to rooting out child pornography, they are more than just statistics. Once you have viewed these images – as I have, and as I know you have – it becomes impossible to forget that behind these numbers are the innocent victims of these unspeakable crimes. I can assure you that the Department remains committed to identifying and rescuing the victims depicted in images of child pornography. One example of this commitment is the FBI's Endangered Child Alert Program (ECAP), which was launched on February 21, 2004, by the Department's Innocent Images Unit. The purpose of

ECAP is proactively to identify unknown offenders depicted in images of child pornography engaging in the sexual exploitation of children. Since ECAP's inception, seven of these "John Doe" subjects have been profiled by *America's Most Wanted*, and with the assistance of tips from viewers, six have been identified. Even more important, however, are the 35 victims (so far) in Indiana, Montana, Texas, Colorado, and Canada who have been identified as a result of this initiative. All of the victims had been sexually abused over a period of years, some since infancy. The Department will continue to make full use this program.

The Department recently has had substantial success in eliminating several major child pornography networks. There are several cases and operations that I can describe where the Department has worked with other domestic law enforcement agencies and our foreign counterparts to root out child pornography.

The first example, announced by Attorney General Gonzales on March 15, 2006, involved a private Internet chat room that was used by offenders worldwide to facilitate the trading of thousands of images of child pornography – including streaming videos of live molestations. The chat room bore the title "Kiddypics & Kiddyvids," and was hosted on the Internet through the WinMX software program that also allowed users to engage in peer-to-peer file sharing. We managed to infiltrate the chat room in an undercover investigation that has yielded charges against 27 individuals to date in the United States, Canada, Australia, and Great Britain (13 of these 27 have been charged in the United States). One of the 27 charged defendants is a fugitive. Seven child victims of sexual molestation have been identified as a result of the investigation, and four alleged molesters are among the 27 defendants charged to date in the continuing investigation. This investigation is international in scope and highlights

our ability to work together with U.S. Immigration and Customs Enforcement, state and local authorities, and international law enforcement agencies to effectively fight these crimes.

The second example I'd like to share with you is the *Mariscal* case. In that case, Angel Mariscal received a 100-year prison sentence on September 30, 2004, after being convicted on seven charges including conspiracy to produce, importation, distribution, advertising, and possession with intent to sell child pornography. As with the first example I mentioned, this case was international in scope: Mariscal traveled repeatedly over a seven-year period to Cuba and Ecuador, where he produced and manufactured child pornography, including videotapes of himself sexually abusing minors, some under the age of 12. But our efforts did not stop with the arrest and prosecution of Mariscal. We launched Operation Lost Innocence to target Mariscal's customers across the country. To date, Lost Innocence has resulted in 107 searches, 55 arrests/indictments, and 44 convictions.

The third example I'd like to tell you about is the *Regpay* case, which led to the follow-on *Operation Falcon* investigation. Regpay was a Belarus-based company that provided credit card processing services to hundreds of commercial child pornography websites. Regpay contracted with a Florida company, Connections USA, to access a merchant bank in the United States. In February 2005, several Regpay defendants pled guilty to various conspiracy, child pornography, and money laundering offenses. Connections USA and several of its employees also pled guilty in connection with this case. As with the *Mariscal* case, however, that was only the beginning: the Regpay investigation spawned U.S. Immigration and Customs Enforcement's Operation Falcon, an international child pornography trafficking investigation that as of February 2006 has so far resulted in 372 open investigations, 579 search warrants, 341 domestic and

approximately 703 foreign arrests, 254 indictments, and 241 convictions. This case is an excellent example of how one child pornography investigation into the activities of individuals involved in a commercial website operation can lead to the apprehension of hundreds of other offenders.

While these major operations continue to be a priority for the Department, I would again underscore how the ultimate goal of each prosecution – whether it is of an international production and distribution ring or of a single consumer – is to protect the children who are the victims of these predators. Since the offenders we incarcerate often have a history of sexually exploiting children, keeping them off the street has undoubtedly prevented untold numbers of children from becoming victims. I'd like to give you a few examples of some of our cases against these repeat offenders.

In *United States v. Wilder* (D. Mass.), the Department prosecuted a repeat child pornography offender. After this defendant was released from prison for a prior child pornography offense, he violated the terms of his supervised release by committing additional child pornography offenses. Not only was he re-incarcerated for violating the terms of his supervised release, but we prosecuted him for those new offenses. He was convicted on March 21, 2006, following a jury trial. Because he is a repeat offender, he currently faces a mandatory minimum sentence of 15 years in prison and a maximum of 40 years when he is sentenced in June 2006.

In *United States v. Wilson* (S.D. Indiana), the Department prosecuted a defendant who was caught with a 14-year-old runaway girl and who was convicted in state court for molesting her. CEOS's HTIU made a critical contribution to the case by establishing that the defendant

was responsible for the child pornography found in his possession. Using metadata, link file analysis, chat logs, e-mail, and other forensic evidence, HTIU was able to connect the child pornography specifically to the defendant, which precluded a possible defense argument that the child pornography did not belong to him. On December 8, 2005, the defendant was sentenced to 99 months' federal incarceration and supervised release for life.

In *United States v. Poynter* (E.D. Kentucky), the Department prosecuted a defendant who had earlier been convicted in state court of sexually abusing a child under the age of 14. On May 5, 2005, he pled guilty to four counts of travel with intent to engage in illicit sexual conduct with a minor. The defendant had been taking boys out of state under the guise of making deliveries for his business and also on pleasure trips to resort locations. He would perform various sexual acts on these boys, all under 16, while on these trips. On August 18, 2005, the defendant was sentenced to 60 years in prison followed by supervised release for life.

In *United States v. Whorley* (E.D. Virginia), the Department secured the conviction, on December 1, 2005, of a convicted sex offender on 74 counts of receiving obscene material and child pornography. Among his other offenses, the defendant downloaded 20 images of Japanese anime cartoons from the Internet which depicted prepubescent minors engaged in sexually explicit behavior. We believe this to be the first case ever brought under 18 U.S.C. § 1466A, which criminalizes obscene visual representations of the sexual abuse of children of any sort, including drawings and cartoons such as the anime cartoons the defendant downloaded. On March 10, 2006, the defendant was sentenced to 240 months' imprisonment, to be followed by 10 years' supervised release.

In *United States v. LaFortune* (D. Mass.), the Department prosecuted an offender who

had previous convictions for raping his own children and for advertising child pornography. He was convicted of advertising, transporting, receiving, and possessing child pornography and, on March 10, 2006, was sentenced to thirty-five years' imprisonment.

In addition to these types of cases, the Department is also involved in two key efforts to protect children from commercial sexual exploitation or sex trafficking. The first of these is the Innocence Lost Initiative, which combats domestic child prostitution. The Innocence Lost Initiative is conducted by the Department, together with the FBI and the National Center for Missing and Exploited Children, and has so far resulted in at least 166 open investigations, 533 arrests, 101 indictments, and 75 convictions. As part of this initiative, we have developed an intensive week-long training program on the investigation and prosecution of child prostitution cases. Task forces from 19 cities have been trained on all aspects of investigating and prosecuting child prostitution cases through Innocence Lost, and 16 U.S. Attorneys' Offices have set up task forces. Four additional task forces are currently in development. Investigative tools such as wiretaps continue to be an invaluable tool to help track pimps as they move from city to city, exploiting children as they go, as well as identifying the loose network that exists among pimps in cities around the country.

The second initiative aims to protect children from so-called sex tourism, in which offenders travel to foreign countries and sexually exploit children. The Department's Criminal Division has been working to increase the number of sex tourism cases being investigated and prosecuted in order to address the serious offense of Americans' sexual exploitation of children in foreign countries. Since the passage of the PROTECT Act in April 2003, which facilitated the prosecution of these cases, there have been approximately 52 sex-tourism indictments or

complaints and at least 31 convictions. There are currently approximately 60 investigations ongoing.

Finally, the Department of Justice is always looking for ways to improve our enforcement efforts against child predators, and we have worked very closely with Congress to improve the laws in this area. Just recently, as part of his speech at the National Center for Missing and Exploited Children in which he highlighted our efforts to combat the scourge of child pornography, the Attorney General announced a new piece of legislation aimed at combating child pornography and obscenity on the Internet.

The new legislation is designed to help ensure that electronic communications services providers report the presence of child pornography on their systems by strengthening the penalties for failing to report the presence of child pornography. The legislation is also aimed at protecting individuals from inadvertently coming across pornographic images on the Internet.

In order to help encourage communications providers to report the presence of child pornography on their systems, the legislation would triple the current criminal fines available against providers for knowing and willful failures to report, making the available fines up to \$150,000 for the initial violation and up to \$300,000 for each subsequent violation.

In order to protect individuals from inadvertently accessing pornographic materials on the Internet, the legislation would require all websites that are operated primarily for commercial purposes to include warning labels on every page that contains sexually explicit material. Sexually explicit material" under this legislation would mean material depicting sexually explicit conduct, as that term is defined in 18 U.S.C. § 2256 -- in other words, actual or simulated sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the

genitals or pubic area, unless the depiction at issue is a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.

Note that these labels are not a “rating” system as some news reports have suggested. Rather, the labels are designed to simply alert individuals to the presence of sexually explicit material, much like the voluntary warning labels currently employed by music producers. In addition, the legislation would prohibit such websites from initially displaying sexually explicit material without further action, such as an additional click, by the viewer. This provision is similar to the CAN-SPAM Act of 2003.

Finally, the new legislation would prohibit the practice, often engaged in by certain sexually explicit websites, of hiding innocuous terms in a website’s code so that a search for common terms on the Internet will yield links to the sexually explicit websites. The legislation would prohibit an individual from knowingly acting with the intent to deceive another individual into viewing obscene material, and would also prohibit an individual from knowingly acting with the intent to deceive a minor into viewing material harmful to the minor. This provision is similar to the Misleading Domain Names Act, enacted by Congress as part of the PROTECT Act in 2003.

The provisions contained in the Administration’s legislative proposal are in addition to the many important changes in law that the Administration proposed last year and that the House of Representatives has passed as part of H.R. 4472, now pending in the Senate. That legislation would improve sex-offender registration laws and toughen criminal penalties for violating registration requirements. It also includes the provisions of the Administration’s proposed Child Pornography Prevention and Obscenity Prosecution Act of 2005, which would improve the legal



arsenal available to detect and prosecute child pornography. We applaud the House of Representatives' passage of H.R. 4472, and we look forward to the Senate's quick passage of this legislation, as its enactment into law is a key component of a more effective anti-child pornography strategy.

In his recent speech at the National Center for Missing and Exploited Children, the Attorney General also indicated that the Department will engage Congress and members of the Internet and other communications industries in ensuring that law enforcement has all of the tools and information it needs to succeed in protecting children. He has directed Department experts to examine and provide recommendations regarding the issue of Internet service providers' maintenance of records that investigators need in order to pursue child exploitation cases. The Attorney General looks forward to working with CEOs of the Internet service providers and other industry leaders on this issue.

*Conclusion*

The Attorney General has made it very clear that protecting children from exploitation over the Internet is one of his highest priorities. We consider this a critically important task and will continue to do our utmost to protect children by enforcing federal child exploitation statutes.

Mr. Chairman, I again thank you and the Committee for the opportunity to speak to you today, and I would be pleased to answer any questions the Committee might have.

MR. WHITFIELD. Thank you very much, Ms. Fisher.

At this time, I recognize Mr. Roldan for his opening statement.

MR. ROLDAN. Thank you, chairman.

Good evening Mr. Chairman, Congressman Stupak, and members of the subcommittee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in combating the sexual exploitation of children through the use of the Internet.

I will start with the personnel involved in this particular program. The number of funded positions assigned to the FBI's Innocent Images program is 127. Due to the seriousness of these matters, however, the FBI has consistently utilized the equivalent of 242 agents working child exploitation matters. Let me emphasize something, too, that is just not the agents. We have many other employees involved in this. I don't give you the numbers because there are so many analysts, people involved in the forensic analysis, secretaries that are supporting this particular program, so it is just not the agents.

The men and women involved in the Innocent Images program are some of the most dedicated and hardworking people in the Federal government. They enjoy my respect and sincere appreciation for the work they do every day. I can tell you this: I have been assigned here for approximately 10 months. I have been in the FBI for over 18 years, and I have met some of the most committed individuals that I have worked with anywhere and anyplace. So I am very proud to be among them.

At any one time, the FBI has more than 2,400 active child sexual exploitation investigations. Because of the magnitude of the crime problem, our primary focus is on complex investigations targeting organized criminal groups, financiers, and illegal websites, individuals, or groups who engage in the production of child abuse images, sexual predators who travel from one jurisdiction to another, and persons with large collections of child abuse images. As an example, I would like to describe how we work a typical sexual abuse website investigation.

First, we must locate the server where the website content is physically located. Once the server is located, and upon finding probable cause, a search warrant is requested. Once a search warrant is executed, the media containing the illegal content is seized for forensic analysis. Once a computer analysis is completed, the targets of the investigation are prioritized. I want to state unequivocally that any information that would lead us to a child who is being sexually abused is treated as a top priority, and not only as a top priority, but as an urgency. That includes expediting the forensic analysis. Then after we identify the website administrators, the producers of the images, and the financiers of the website. Once the illegal website and the organizations managing, financing, and producing the child pornography have been taken out of business, the information associated with the customers paying for access to the website is analyzed and acted upon. However, this endeavor is very complex.

First, we must attempt to accurately identify each and every customer accessing the website. This piece of the investigation requires vast resources. Child sexual abuse websites investigated by the FBI have been found to contain anywhere from 9,000 to more than 30,000

different customer entries. The most useful data utilized to identify the customers at this time is the credit card information. In order to obtain credit card information from a financial institution, the FBI must seek a Federal Grand Jury subpoena for each bank who issued a credit card use for the website customers. The information obtained can then be utilized to identify each and every individual account holder who paid to enter the illegal website. Even after all of the financial information is obtained, and a thorough analysis of all of the information is conducted, there is not enough probable cause established to request a search warrant on the customer's residence. The only option that remains is knocking on the customer's doors and asking for consent to access their computers. If this consent is not granted, the investigation cannot proceed until additional incriminating evidence is uncovered. This whole process is labor intensive and takes an excessive amount of time. In addition, it would also take more than 11 special agent hours to accomplish what we would call a knock and talk type of investigation on each illegal website customer.

In contrast, another totally separate investigative technique that the FBI currently utilizes addresses child sexual abuse matters in a peer-to-peer investigation. It allows for us to capture the child sexual abuse images as they are being transmitted real time and collect identifying information on the perpetrators the instant the crime occurs. Immediately thereafter we can obtain search warrants and seize the evidence. One such investigative initiative resulted in over 400 cases open, 300 search warrants, 50 convictions, and 14 victim children identified and rescued.

In conclusion, we would like nothing more than to knock on each person that is involved as a customer in child sexual abuse websites, but again, those are the resources that are required, for example, in a case of 30,000. That is how many people we would require to send out. My comments today are intended to reassure the subcommittee and the American people that the FBI takes this matter very seriously, and has a very aggressive program assigned to address child sexual exploitation.

I would like to express my appreciation to the subcommittee for addressing this very serious issue. I look forward to answering your questions.

[The prepared statement of Raul Roldan follows:]

PREPARED STATEMENT OF RAUL ROLDAN, SECTION CHIEF, CYBER CRIME SECTION, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE

Good Morning Mr. Chairman, Congressman Stupak, and Members of the Subcommittee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in combating the sexual exploitation of children through the use of

the Internet. Specifically, I would like to explain to the Subcommittee how the FBI manages the Innocent Images National Initiative on a national and an international level.

Two weeks ago, the Subcommittee heard the testimony of Acting Executive Assistant Director Chris Swecker which described this initiative and its accomplishments. As he testified, over the past 10 years, the Innocent Images program has grown exponentially. Between fiscal years 1996 and 2005, there has been a 2050% increase in cases opened (113 to 2500). During this ten-year period, the program has recorded over 15,556 investigations opened; 4,784 criminals being charged; 6,145 subjects being arrested, located or summoned to appear in a court of law; and 4,822 convictions obtained.

The FBI's Innocent Images Unit is responsible for the creation and implementation of national and international initiatives targeting those who use the Internet to sexually exploit defenseless children. The unit, housed in Calverton, Maryland, also works closely with and has a sizable contingent assigned to the National Center for Missing and Exploited Children. The Innocent Images Unit serves as a central location for addressing major cases such as the sexual exploitation of children through pornographic websites, distributing investigative leads to our field divisions and Legal Attaché offices, and managing the FBI's national program. Its responsibilities include developing and publishing policy, managing program funds, certifying undercover operations, and the training of FBI employees, state, local and international partners.

The number of funded positions for the Innocent Images program is 127 positions. Due to the seriousness of these matters, however, the FBI has consistently utilized personnel resources at a higher level than those funded. We currently have the equivalent of 242 Agents working child sexual exploitation matters. Not just anyone can do this work. Our dedicated men and women are exposed to the most graphic and disturbing images and movies that you could possibly imagine. They wade through thousands of pieces of material every day, all day, and then they go home and tuck their own children into bed. However, the men and women of the Innocent Images Unit, and those involved in investigating the sexual exploitation of children in our field offices, are some of the most dedicated and hard working people in the federal government. They enjoy my respect and sincere appreciation for the work that they do everyday. They are some of the most dedicated and passionate employees I have met in my 18-year career as a Special Agent of the FBI.

At any one time, the FBI has more than 2,400 active child sexual exploitation investigations. Because of the magnitude of the crime problem, and in an effort to capitalize on the FBI's intelligence collection, analysis, and investigative strengths, our primary focus is on complex investigations targeting organized criminal groups involved in commercial child sexual abuse websites. As Mr. Swecker testified, these investigations almost always span multiple jurisdictions and usually expand beyond the borders of the United States. In an effort to reach beyond the borders of the United States in a more efficient manner, the FBI has partnered with law enforcement officials from several countries who work side by side with FBI agents in Calverton, Maryland in a task-force setting.

Other areas where the FBI makes a major impact include investigating the financiers of illegal websites, as well as individuals or groups who engage in the production of child sexual abuse images. The FBI also investigates sexual predators that travel from one jurisdiction to another to engage in sex with minors. Finally, we target persons with large collections of child sexual abuse images. These individuals represent a real danger as we find a large percentage of those we arrest for possession of images of child sexual abuse are also committing contact offenses. Our investigative efforts attempt to maximize the impact the FBI can have on this very serious crime problem. I would like to describe how we work a typical case, such as a child sexual abuse website investigation.

An investigation may sometimes be initiated from a referral by the National Center for Missing and Exploited Children. We utilize a variety of investigative techniques, to include administrative subpoenas and data base checks, to capture evidence in an attempt to locate the server where the website contents are physically located. Once the server is located and upon finding probable cause, a search warrant is requested and issued. In many cases the company that runs the server is not aware that its computers contain illegal content as they may also host hundreds of legitimate websites. Once the search warrant is executed, the media containing the illegal content is seized and delivered to our Computer Analysis and Research Teams (CART) for forensic analysis. Given the tremendous amount of digital data seized by the FBI, this analysis could take months to accomplish, as these teams are responsible for the forensic examination of digital data in all of the FBI's investigative programs, to include counterterrorism investigations and other high priority matters.

Once the computer analysis is completed, the targets of the investigation are prioritized in partnership with prosecutors from the Department of Justice. I want to state unequivocally that any information that would lead us to a child who is being sexually abused is treated not only as a top priority, but also as a matter of great urgency. Our second priority is the identification of the website administrators. Generally, these individuals administer more than one child sexual abuse website. Thereafter, the producer of the images is identified, as these images represent evidence of the actual sexual molestation of a child. Next the funding vehicle and the financiers of the website are identified.

Once the illegal website and the organizations managing, financing, and producing the child sexual abuse and exploitation images have been taken out of business, the information associated with the customers paying for access to the illegal website is analyzed and acted upon. Of course we recognize that the customers of the websites may also be sexually exploiting children and we do everything possible to investigate these individuals. But this endeavor is complex and labor intensive. First, we must accurately identify the customers accessing the website. I must reemphasize the word accurately, because in order for us to initiate an investigation, each and every one of the perpetrators must first be accurately identified. This phase of the investigation is very lengthy and requires vast resources as child sexual abuse websites investigated by the FBI have been found to contain anywhere from 9,000 to more than 30,000 different customer entries. Another issue to consider is the fact that most illegal-website customer entries are normally years old. Once outdated, this information cannot be utilized to show probable cause, request search warrants, or acquire the appropriate evidence to proceed with an investigation.

The most useful data for the purpose of attempting to identify the customer is the credit card numbers. In order to obtain credit card information from a financial institution on these types of investigations the FBI must seek a Federal Grand Jury subpoena. Currently this requires a presentation to a Grand Jury to request a subpoena for each individual bank in order to identify each and every individual account holder who paid to enter the illegal website. Even after all of the financial information is obtained through these subpoenas, and a thorough analysis of all of the information is conducted, there is rarely enough probable cause established to request a search warrant on the customers' residences. The only option that remains is knocking on the customers' doors and asking for consent to access to their computers. If this consent is not granted, the investigation cannot proceed any further until additional incriminating evidence is uncovered through other investigations. Under our current process, it takes an excessive amount of time for a team of intelligence analysts to process and analyze a customer list on an average child pornography website. It would also take more than 11 special-agent-hours to accomplish a knock-and-talk type of investigation on each illegal-website customer. Again, let us remember that every illegal-website investigation will

have a minimum of thousands, and sometimes hundreds of thousands of customers. We are exploring ways to expedite this process, but there are numerous hurdles to overcome.

In contrast, another totally separate investigative technique currently being utilized by the FBI to address child sexual abuse matters through Peer-to-Peer investigations, allows for us to capture child sexual abuse and exploitation images as they are being exchanged by pedophiles, and collect identifying information on the perpetrators the instant the crime is occurring. Immediately thereafter, we can obtain search warrants, and have the authorities go in and seize evidence in as little as a one-week time period. Using the technique I just described, and others also currently available, the FBI makes hundreds of arrests and prosecutable cases every year. For example, one such investigative effort resulted in over 400 cases opened, 300 search warrants, over 50 convictions to date, and 14 victim children identified and rescued.

This example was presented to you in order to better describe how the FBI has to prioritize not only who must be targeted in an investigation, but also what investigative tools must be utilized in order to maximize investigative results by making a serious impact on the overall crime problem, and putting the most egregious sexual offenders behind bars.

My comments today are intended to reassure the Subcommittee and the American people that the FBI takes this matter very seriously and has a very aggressive program designed to address child sexual exploitation. In closing, the FBI looks forward to working with other law enforcement agencies, private industry, and the Department of Justice in continuing to combat this very serious crime problem. The protection of our children requires the combined efforts of all sectors of our society. I would like to express my appreciation to the Subcommittee for addressing this very serious issue, and I would also like to thank Chairman Whitfield, Ranking Member Stupak, and the Subcommittee for the privilege of appearing before you today. I look forward to answering your questions.

MR. WHITFIELD. Well, thank you, Mr. Roldan and Ms. Fisher both. The committee values your testimony and certainly the input the FBI and the great job that you do in trying to bring perpetrators of these crimes to justice.

As you know, when we first started these hearings we got off on a little bit of a rough edge, I guess, with the Bureau, the FBI, and the Department of Justice, and I think a lot of that stemmed from the fact that it appeared to us that in the Justin Berry case that there was some bias against Justin Berry. There was some relationship there that just did not work out with the FBI and the Department of Justice, and many of us felt--whether we are correct in that perception or not, but we felt that valuable information that was given to the Department was not followed up on in an expedited way and a timely way and that, in effect, jeopardized the opportunity to catch some perpetrators that you had some very hard evidence on.

So I would make that comment just starting off, and we will get into some of this later, but I know Ms. Fisher, for example, you had a meeting recently with some Internet service providers, and one of the issues that we have heard a lot about is maintaining those records for a length of time that would facilitate an investigation by the Bureau or other law

enforcement agencies. Could you tell us how your meeting with the Internet service providers went?

MS. FISHER. I would be happy to.

I think the data retention issue that was raised by the Congresswoman is a very important one, because law enforcement does need data to track down ISPs and track down some of these perpetrators, but it is also, as I learned from the ISPs, a very complex one, and I am glad that you will be hearing from them directly next week as to how data is stored and how you can retrieve it and those issues.

Many of the service providers retain it for a certain period of time, 90 days or longer. Some retain it for much less periods of time, some 14 days. So I think it is important that we all look at this issue. The Attorney General, in a speech that he gave at the National Center for Missing and Exploited Children just last week or the week before, said that he wanted the Department to look at this issue and has set forth an expert group to deal with this issue, both with the policy people and people that understand the technology. That working group has already been meeting and those meetings are going to go forward.

MR. WHITFIELD. Now, do you have any information that would lead you to believe that some of the Internet service providers and remote computing services are not reporting apparent child pornography on their network that they know about?

MS. FISHER. Well, I know that there are several, about 217 ISPs that are reporting to the National Center for Missing and Exploited Children, and have reported evidence of these crimes. Those go into the database, and then of course NCMEC sends it out to law enforcement so it can be acted on, whether it is in the State, local, Federal level.

Whether there are others out there that are not reporting on evidence of these crimes is something that we are on the lookout for. One thing that I would like to point out to you, because now we are into talking about the statute that you have, 13032, that requires ISPs to report when they have this kind of evidence, and in that statute it talks about liability when ISPs don't report. We just cleared today, the Administration just cleared today a proposal that would add and enhance, I believe, significant penalties for ISPs to report in the following way. Right now the statute provides that the penalties exist for people who willfully and knowingly fail to report. This new proposal which we have talked to your staff about just this morning, because it just got cleared, this new proposal would allow for civil penalties for people who negligently fail to report evidence of the crime. That, I believe, enhances our efforts and our ability to go after those who aren't reporting when we discover that they aren't reporting.

MR. WHITFIELD. Have you all ever prosecuted anybody under the existing statute?

MS. FISHER. To date we have not prosecuted anyone under the existing statute, but that certainly shouldn't imply that we wouldn't, and it came to our attention that there were ISPs out there that were willfully and knowingly not reporting to NCMEC. We are on the lookout for that and we would prosecute under the statute.

We want to enforce all the laws in this area and we want to enforce them aggressively and we want to use the sentences and the penalties that Congress has given us under the PROTECT Act and others to put these people behind bars.

MR. WHITFIELD. I would ask you and Mr. Roldan both this question as people involved in law enforcement and prosecuting what I would consider some of the worst crimes that could be committed. What is the most frustrating aspect of this whole process from your perspective, and what frustrates you the most in bringing people to justice for committing these crimes?

MS. FISHER. Well, when we actually bring them to justice and get them convicted, that doesn't frustrate me. That is a good thing. But what I think, as these hearings have demonstrated, what is frustrating is that this problem continues to grow, and it is going to take all of us working together. Law enforcement alone is not the answer. It is going to take Congress, it is going to take educators, it is going to take parents, and that is why I think the visibility of these hearings and making people aware of what happens when there are children going on the Internet is so important.

MR. WHITFIELD. It is so pervasive. I know I was reading an article just yesterday that a gentleman from Saudi Arabia, 37 years old, flew to California and he had been involved in the Internet and he thought he was in a conversation with the father of a two and a half year old child, and he flew to California for the purpose of molesting this child and was paying the parents. Of course, when he arrived, it was law enforcement that had set him up. But this was a 37-year-old psychiatrist from Saudi Arabia who flew to California for this purpose.

Mr. Roldan, in your testimony you indicated that from '96 to 2005 that the FBI had opened something like 15,500 some odd cases in this area, but had obtained like 4,800 convictions. I was just curious what happened in those other cases. The evidence just was not good enough to convict, or--

MR. ROLDAN. There is a variety of reasons. I am going to go ahead and defer to Mr. Bell because he has worked most of those cases. Arnold, please?



MR. BELL. Thank you, Mr. Chairman. Before I begin my remarks, I would like to thank the committee for bringing this issue to light, and thanks for the opportunity to be here this evening.

In cases that we investigate, oftentimes the evidence either is not there to have a successful prosecution, or in some instances, cases are deferred to other agencies or deferred to a State authority, and we don't capture some of those statistics.

MR. WHITFIELD. Okay. Now, you all presented a legislative proposal just in the last couple of days that you feel like would assist the Department, is that correct?

MS. FISHER. That is correct.

MR. WHITFIELD. And could you briefly cover some of the provisions of that legislation that you think would be particularly helpful?

MS. FISHER. Are you referring to the legislation that was sent up last week and this is included in that--

MR. WHITFIELD. Right.

MS. FISHER. And this relates to ISP reporting.

MR. WHITFIELD. Right.

MS. FISHER. There is also some other legislation that I think the House for passing on child safety and that is now with the Senate, but that is important. The PROTECT Act was very important to this effort.

What this new legislation does is again, for ISPs that fail to report it increases the penalties for those who willfully and knowingly fail to report, and in addition, it now allows us to set up a regulatory scheme where ISPs that negligently fail to report will also be fined \$50,000 for the first time, \$100,000 for each subsequent time.

We look forward to working with this committee and with Congress in any other ideas in this area to move forward, and we are constantly looking for new ideas. I think it is important, again, to make sure that we have all the tools to fight this problem.

MR. WHITFIELD. Well, do you feel like there is any specific way that this committee can help or--

MS. FISHER. Well like I said, I think you are already helping. I think the fact that the House passed the Child Safety Act helped.

MR. WHITFIELD. Okay.

MS. FISHER. I would note also on sentencing, you know, sentencing reform is an issue that the Department is very concerned about. The Sentencing Commission just did a look at what has happened in the post-Booker world, after the Supreme Court came out and said that the sentencing guidelines were advisory instead of mandatory. And one important thing that they noted was that in child sexual abuse cases they are seeing more downward departures, meaning more sentences given by

judges under the guidelines. So sentencing reform is another thing that should be focused on here.

MR. WHITFIELD. Okay. Well, I see my time is about expired, so I am going to recognize Mr. Stupak, but I think he is yielding his time to Ms. DeGette, so Ms. DeGette.

MS. DEGETTE. Thank you, Mr. Chairman. We are working together because we both have scheduling constraints, so I will just take a few minutes and then I will yield the rest of the time to Mr. Stupak.

I want to thank all of you for coming and I have a few questions. One of them, my main issue as I discussed in my opening statement is this concept of retention of subscriber information by ISPs, not, in fact, the communications, but rather the subscriber information. I am wondering if all of you in law enforcement--and I know, believe you me, Ms. Fisher, I have been meeting with these ISPs, too, and I know all of the explanations and the excuses and everything else, but the fact is, these ISPs retain subscriber information now. What we would really be talking about is accounts that had been closed, because if it was an ongoing account and law enforcement tried to subpoena that, it would be available because it is an existing account. So what you are really talking about is closed accounts, and I think that having that retained so if there was probable cause to think that a crime had been committed by that subscriber, law enforcement could subpoena that and it would be useful in the investigation. Don't you think that that would be helpful to investigators? Maybe I should ask some of the investigators.

Mr. Swecker, I think you testified before that that would be useful.

MR. SWECKER. It would be. We find that the information is often stale by the time we get the information, if we get it. Most of the major ISPs are keeping it for about 90 days, but you are right on the money when you talk about retaining at least the ISP. Maybe not necessarily the content, but at bare minimum at least the ISP addresses.

MS. DEGETTE. I just keep thinking about that investigator who we have talked to quite a bit in my office who talked about the child who was being raped online, and then by the time they got to Colorado the data was gone. Mr. Roldan or Mr. Bell, do you have any sense of how helpful do you think that would be towards investigation of these cases?

MR. ROLDAN. Yes, if you notice from my testimony, the process is very long to initially identify the individuals, the customers that are entering the illegal websites, and obviously the IP address would provide the first information. The more information we have, the more helpful it is to the investigation.

MS. DEGETTE. And because it does take some time to identify the perpetrator, you can't always subpoena that information within 14 or 30 days, correct?

MR. ROLDAN. And there is also a difference in the subpoenas that are available. On the credit cards, we have to go through a grand jury. On the ISPs for the IP address, we go through--

MS. DEGETTE. It is administrative, right.

I have a couple more questions, and then I will yield to Mr. Stupak, about the search warrants. In the Larry Walt case in Missouri, there was a Sergeant Michael Ziglefa who was involved in that case, the local FBI office got a warrant with an e-mail address and an IP address, which led to a physical address for the defendant, which was obtained from the ISP. Nobody knew whether the computer was at that address or not, but the FBI got a search warrant anyway, and the judge said that probable cause for the issuance of a search warrant exists when there is "a fair probability that contraband or evidence of a crime will be found in a particular place." Any of you who know the answer to this, is that the criteria used by the Justice Department and the FBI when requesting search warrants for child pornography?

MS. FISHER. Certainly, all of the cases depend on the facts and circumstances, and I am not sure about the facts in that case. But you have cited the right standard for probable cause. Now, what is going to allow you to get a search warrant with your judges in that district is going to be best known by the prosecutors in that district, as far as what more you are going to need. If you have an ISP address that takes you back to a computer and you have evidence that somebody is in the house using that computer, what do you know about that person, are they living there, et cetera. But all of those facts and circumstances are going to be looked at I believe that the prosecutors that I work with are going to look for that first opportunity to get that search warrant.

MS. DEGETTE. So you wouldn't have to prove that the computer was actually there, just that there was a fair probability? That is the definition of probable cause, right?

MS. FISHER. Well again, yes, but you would have to look at the whole facts and circumstances.

MS. DEGETTE. Exactly. Thank you very much, and I will yield to Mr. Stupak. Thank you for your comity, Mr. Stupak.

MR. STUPAK. Ms. Fisher, you indicated that these new provisions have been sent up here on Section 13032, had there been any prosecutions? You said no. Have any efforts been made to prosecute anyone under 13032?

MS. FISHER. I know that there have not been any prosecutions.

MR. STUPAK. Have any efforts been made to seek any prosecutions under 13032?

MS. FISHER. Well, certainly we are on the lookout for it, and if we found evidence of that. I can't tell you how far certain investigations have gone, but I can assure you, Congressman--

MR. STUPAK. 13032 was an act in '99 by the Congress, right?

MS. FISHER. That is correct, sir.

MR. STUPAK. And in 2000, the Clinton Administration put forth the regulations to implement the law, is that correct?

MS. FISHER. I believe there were some regulations that did go out, sir.

MR. STUPAK. And then since then, nothing has been done to use this law to apply it to any cases, isn't that correct?

MS. FISHER. I can't say that nothing has been done, but I will agree with you, sir, that there have been no prosecutions under the standard that is put forth in the statute. With regard to ISPs, again, with regard to ISPs who have not reported--

MR. STUPAK. Has the Justice Department or you or anyone ever come to Congress and say we don't feel your law is enforceable, and therefore we have to make some changes until today?

MS. FISHER. No, I am not aware of that.

MR. STUPAK. Well, we had testimony at the last hearing from the Center for Missing and Exploited Children that you weren't using the law because you didn't think that it was enforceable, that the Department of Justice didn't think it was enforceable.

MS. FISHER. There is nothing that strikes me about this law that is not enforceable.

MR. STUPAK. Then why are you recommending changes to it?

MS. FISHER. We believe that we are going to make it more enhanced, because now we will be--

MR. STUPAK. Well, how would you know if it needed to be enhanced if you have never used it?

MS. FISHER. Sir, we have never prosecuted a case under that. I can't say that we have never used the statute.

MR. STUPAK. So why would you want--

MS. FISHER. In fact, I think the whole--

MR. STUPAK. The law has never been used for prosecution, why would it have to be changed?

MS. FISHER. Well, this act has a lot of provisions that have been used with regard to reporting in, and I am sure, as you know, you heard from NCMEC, the reporting in is a success story. There are over 200 ISPs that are reporting--

MR. STUPAK. Out of how many ISPs are there?

MS. FISHER. I don't know the answer to that, sir, but Congressman--

MR. STUPAK. And they don't report underneath this law. They report under a different law.

MS. FISHER. There are over 217 ISPs that are now reporting to NCMEC. This deals with ISPs that are not reporting and willfully and knowingly not reporting. That is correct.

MR. STUPAK. So why isn't this law being enforced?

MS. FISHER. I can't say that it is not being enforced. I think we are talking past each other for there has not been a prosecution under this law. That does not mean that it hasn't been investigated. That does not mean that we don't stand ready, that when--

MR. STUPAK. Wait a minute. We already had testimony that it hasn't been used at all. Are you saying that the people who testified before did not tell the truth before this committee?

MS. FISHER. No, absolutely not.

MR. STUPAK. Well, one of you--

MS. FISHER. I think I am being completely consistent.

MR. STUPAK. Well, either Justice is not telling us the truth, or the other people who testified are not telling the truth. We can't have the same reading or the same understanding of the same law.

Let me ask you this question. Isn't it true, with your so-called changes today, you are really shifting your responsibility, Justice Department's responsibility, to the Federal Communications Commission?

MS. FISHER. Absolutely not.

MR. STUPAK. Well, under Section C, the purpose of this paragraph, "The Federal Communications Commission shall have the authority to levy civil fines under it and shall promulgate the rules and consultation with the Attorney General to effectuate the purposes of subparagraph B and to provide the appropriate administrative review of civil penalties." To some of us sitting up here, it looks like you are shifting this responsibility from Justice to the FCC.

MS. FISHER. Absolutely not. The criminal penalties for willful and knowing failure to report will still be prosecuted by the Department of Justice. The civil penalties in the civil regime as under this bill will be administered by the FCC, but now, what is great about this is that we can get both. We can get people who negligently failed to report, but we can also get people who willfully and knowingly failed to report.

MR. STUPAK. Have you ever used it?

MS. FISHER. We stand by--it has not been prosecuted. There is--

MR. STUPAK. Can you tell me a case where you have used it?

MS. FISHER. No, sir, I agree with you. This statute has not been used to prosecute an ISP for failing to report.

MR. STUPAK. And I will bet you if we never would have brought up these hearings, we wouldn't have these so-called enhancements of this law unless we had these hearings, correct?

MS. FISHER. I don't know when exactly these enhancements were starting to be discussed at the Justice Department. I can tell you that we are always looking at enhancements on reporting and looking at enhancements to laws that combat this horrific problem. I thank you for these hearings.

MR. STUPAK. Let me ask you about Operation Falcon. You discussed in your testimony, you said it resulted in 372 open investigations, 579 search warrants, 341 domestic arrests, 254 indictments, and 241 convictions. ISIS told us that they, as well as State and local law enforcement, verified the names, credit card information, and physical addresses of over 21,000 individuals in the United States that paid to download images of the rape and torture of children. You have testimony that at least one-third, as much as three-fourths of these individuals have or will engage in such horrible acts themselves. There are at least 20,000 individuals known to the Department of Justice that are a threat to the safety of children where no attempt has been made to remove them from the community. Are you content that CEOS has done everything it can to prosecute these individuals, these remaining 20,000?

MS. FISHER. Well, I certainly, as I said, want all child predators put behind bars. That--

MR. STUPAK. I am just going off the 20,000.

MS. FISHER. This investigation, like many others, continue, and hopefully we will find and prosecute the people that are committing these horrible acts on our children.

MR. STUPAK. So it is your testimony you can't find the 20,000? You have the names and addresses--

MR. WHITFIELD. Mr. Stupak, your 10 minutes have expired. I am going to go to the full committee Chairman, and then we will come back. Very good.

CHAIRMAN BARTON. Mr. Chairman, thank you, but if Mr. Stupak wants to conclude that, I am happy to defer until he has concluded that particular line.

MR. STUPAK. What happened to the other 20,000? You had the credit card information, their names, and their physical addresses, so what happened to 20,000? You said you couldn't find them.

MS. FISHER. I never said I couldn't find them.

MR. STUPAK. Okay.

MS. FISHER. I said that the investigation continues.

MR. STUPAK. Okay. So you are still working on it?

MS. FISHER. Absolutely. We are still working on all of these investigations and these operations.

MR. STUPAK. Is that since we have had these hearings or--

MS. FISHER. No, sir.

MR. STUPAK. I just wondered if it was like the statute, that is all.

Thank you, Mr. Chairman. I will look forward to my 5 minutes later.

MR. WHITFIELD. Mr. Chairman.

CHAIRMAN BARTON. Well, thank you, Chairman Whitfield, for holding this hearing. I am going to start off thanking all you witnesses for being here. I mean that. One of you has been here before, in a little bit of a difficult situation. The other three of you have gotten here in a somewhat unusual fashion, but the truth is, you are here and we are happy you are here. I want this to be a positive hearing. I have not normally had the Attorney General of the United States walk into my office and say that either he would come or you folks would come, and so I thank Attorney General Gonzalez for making that commitment, and I have not often had to call the Director of the FBI and have the kind of conversation I had with him to get some of our FBI witnesses here. So I am sincere in saying we appreciate it and I think we are on the same team. Congress wants to bring these folks to justice, these child predators, and you folks obviously do. You all have dedicated a large part of your professional career to that.

So I want to start off by kind of reestablishing what the problem is, and I guess, Ms. Fisher, I go to you since you are the senior Department of Justice official here. How many perpetrators do we think there are in the country that engage in child pornography and preying on children for pornographic purposes? Does the Department of Justice have an estimate of that?

MS. FISHER. I don't have an estimate with me, but it is hundreds of thousands.

CHAIRMAN BARTON. Hundreds of thousands. Mr. Swecker, as the FBI senior person, would you agree with that?

MR. SWECKER. I would. I mean, it is very difficult. There are different categories, if you will, possessors versus people who are actually producing and abusing the children. So there are different--as you well know, there are different categories, but there are a lot of them out there and I think--

CHAIRMAN BARTON. So you wouldn't disagree with the order of magnitude?

MR. SWECKER. No, not at all.

CHAIRMAN BARTON. Okay. Do we have an estimate of the number of commercial child pornographic sites there are on the Internet on any given day? Anybody?

MR. BELL. I don't know if there is a way to determine with certainty a number like that. I did a simple Google search on some terms that I know, and I had 130,000 hits.

CHAIRMAN BARTON. One hundred thirty thousand?

MR. BELL. Right, and that was on one search term.

CHAIRMAN BARTON. So we have hundreds of thousands of potential if not actual predators. We have hundreds of thousands of commercial sites. What is our estimate on number of victims then, the actual children themselves, based on that? Would that also be in the hundreds of thousands, the millions, the tens of thousands? Just kind of a general order of magnitude, what would it be?

MR. ROLDAN. Sir, it would have to be in the hundreds of thousands-

CHAIRMAN BARTON. Hundreds of thousands.

MR. ROLDAN. --because every time we arrest someone, there is more than one victim.

CHAIRMAN BARTON. Okay.

Now, at our previous hearing, one of our witnesses from law enforcement made the point that I thought was rather telling, that this wasn't just a law enforcement problem, and I agree with that. I mean, with this kind of an order of magnitude, we cannot ask a handful of Federal officials backed up by State and local--I mean, this is a huge problem. My first question, and I will direct this to Ms. Fisher, given the order of magnitude, when I look at the number of officials at the Department of Justice and the number of agents at the FBI that are dedicated to this problem, it is in the dozens at DOJ, and at the FBI, it is several hundred. What does the Congress need to do to significantly increase the personnel and the financial resources that are being dedicated to tracking this problem? I have no doubt that everybody that is assigned is absolutely committed to bringing to justice these fiends, but I am a little puzzled as to why given the order of magnitude that we all understand in general terms, there hasn't been a huge request to put more agents, more prosecutors, more resources into combating the problem? We are fighting a forest fire with a can of aerosol spray or something. Is it a Congressional problem that we are unwilling to work to increase the resources, or is it there are so many other problems that you just don't feel like you can put more resources into it?

MS. FISHER. I think you can always put more resources to attack this problem. One of the things that we have tried to do in the Department of Justice, and I will let the FBI follow me, because I know that they put a great deal of resources on this. We use all 94 of our U.S. Attorney's offices to prosecute this. Second, the Attorney General himself has told the prosecutors and told the U.S. Attorneys this is our priority. Third, we



have this new initiative called Project Safe Childhood, and what that does is it makes us link up with the State and locals who also have resources to prosecute these crimes, to train them, to give them money to prosecute. I think \$14 million is going out to ISIS this year, and to enhance community awareness.

So those are some of the things that we are trying to do to address the problem, sir.

CHAIRMAN BARTON. I don't want to beat a dead horse here. The young man who was the primary witness at the last hearing who had been sexually abused indicated that the website that he was operating, his one website, if I understand, that one website took in \$1 million a month. We estimate that the national take on child pornography in the United States through the Internet is upwards of \$20 billion a year, \$20 billion. And we are talking about a \$14 million upgrade? A million million, a thousand million is a billion. I think the Congress will work with the Administration to find a way, instead of having a couple of hundred FBI agents, a dozen or so specialists at DOJ, or even--so let us put thousands. If we are serious about this, let us put some real muscle in. Again, I am not negative on what you are doing, but if I have got to put out a major forest fire, I don't send out one firefighter, no matter how good he is. You know, I mobilize the entire operation.

My next point. The gentleman on the end here, Mr. Bell, said that he put in a phrase and he got 130,000 hits that there was--he thinks there may be a commercial site on the Internet for child pornography. Now, it is illegal to engage in child pornography. Why wouldn't it be possible, and if we need to change the law, if you can prove that that is a site that is a child pornographic trafficker, shut it down immediately? Why can't you do that? It is an illegal act, it is engaged in illegal activity. Why don't we just take it off as soon as we know it is there?

MR. BELL. The difficulty in addressing the commercial websites in particular is there are several mechanisms for masking where they actually are. We have to identify where the host server is. Oftentimes, that is not in the United States. Oftentimes, these websites are administered by people who are not in the United States.

CHAIRMAN BARTON. Is there anyplace in the world where child pornography is legal?

MR. BELL. Not that I am aware of, but I think as you mentioned there are 90-some countries where it is not--I am sorry, there are 94 countries where it is not illegal, we heard testimony today. Some of the guys that are doing this that are doing it for profit and as a business are situating themselves in those places where they kind of have safe harbors. We have tried to address this through international cooperation. We have an international task force. I think some of your staff members

have met some of the officers that we have from overseas that are working with us, and we are trying hard to address these sites, wherever they might be in the world.

MR. WHITFIELD. Mr. Chairman, I might just make a comment, though, that 94 countries do not have any laws on child pornography, but I have been told that it is estimated that 40 percent of all the sites are right here in the U.S.

MR. BELL. What we found through some of our investigation is that oftentimes when we finalize our investigations, we find the services to be housed in the U.S. are in Western European modernized countries and the reason for that, we believe, is that the infrastructure is so much better here for high speed broadband and such.

So the guys--the subjects who are administering these sites tend to be offshore, but the mechanisms are here.

CHAIRMAN BARTON. Do we have the technical capability, if it were legal, if I put up a child pornography site called Kiddyporn.barton--or Bartonkiddyporn.com, and I am engaged in illegal transactions for child pornography, it is technically possible to shut my site down and not let it be accessed. Is that not correct?

MR. BELL. It is possible. It is possible to shut the site down, but what happens is sites are generally hosted in several locations at one time. The analogy I like to use is owning four homes. If you are a drug dealer and you own four homes and the police raid one of your homes, you just go to the next home. What we are finding in our investigations is that sites are located in multiple servers in multiple locations.

CHAIRMAN BARTON. But my point is, if we have detective capability to shut these sites down, why don't we make sure you have the constitutional and legal ability to just do it if you can prove by accessing it there is child pornography on that site. Boom, shut it down, just do it. Make it tough on these guys, you know, make it tough on them. There are not that many of you, so just--I mean, I think we will back you up. I don't believe anybody on either side of the aisle this is the committee of jurisdiction for the Internet. Now, we don't have criminal penalty enforcement. That is your friends on the Judiciary Committee. But if you need--I mean, what the Attorney General has sent up in terms of a legislative package I think is a step in the right direction, but it appears to me that there is so much that we could do if we are serious about this, and we just are not doing it.

And so my plea is let us think big. Let us think as big as the traffickers think. They are having hundreds of thousands of sites, hundreds of thousands of perpetrators, and we are fighting that with, you know, just a handful of people.

I have some other questions, Mr. Chairman, but my time is expired. I do want Mr. Roldan's thoughts in writing and will give him a question in writing. He says the best way to get at these folks is through credit card information, but they have to go on a case-by-case basis to a Grand Jury to get a subpoena to get that identification of the individual with the credit card number. I would like to see what we need to do to make it possible to access those credit cards without having to go on a case-by-case basis. Again, if you can prove that that credit card has been used at a site that traffics in commercial child pornography, I would be willing to vote for a bill that makes it an automatic that you can go to the bank and get the identification of that credit card holder. If you prove that they purchased child pornography or accessed a site and paid to go to a site where child pornography was there, that would be prima facie evidence that they are engaged in it and you can get their name. You don't have to spend all the time to go to do th--and again, I don't want to violate anybody's constitutional rights, but I would think if you can prove that that credit card has been used, you ought to be able to get the name of the person using it without having to do all the effort that the FBI and the State law enforcement people are having to do.

Thank you folks for coming, and again, Mr. Whitfield, thank you, and Mr. Stupak for doing this investigation.

Lastly, I am told that the million dollars a month was not a site that was operated by Justin Berry, it was another case, the Reedy case. Thank you.

MR. WHITFIELD. Thank you, Mr. Chairman.

At this time, I recognize Mr. Stupak for his remaining 6 minutes.

MR. STUPAK. Thank you, Mr. Chairman.

Ms. Fisher, you said in your response to the Chairman that 94 DA's are all working on this and it is a priority with the Attorney General to prosecute these cases. Then what happened last July when Justin Berry came to the Justice Department with some current IP addresses, physical addresses, credit card information of persons who were subscribers to his website, but neither the FBI nor Justice has used this information to obtain search warrants? What happened there?

MS. FISHER. Of course because this is a pending investigation there is some stuff that is public that I can talk about and there is material that is not public with regard to the investigation that I can't talk about. What is public is that there has been two people charged with regard to this investigation, Mr. Mitchel and Mr. Richards--

MR. STUPAK. Two out of 1,500 I believe it is, right? Wasn't there 1,500?

MS. FISHER. There have been two people charged. One has been convicted, one is pending trial. There have been--the website itself has

been taken down. There have been search warrants. It would be inappropriate for me--that is public and that is what I can tell you about the investigation.

MR. STUPAK. Wait a minute. You guys didn't do anything to shut down this server. The guy fled the country.

MS. FISHER. I am sorry. There were search warrants that were done that have taken down that commercial website.

MR. STUPAK. Tell me, what was done to put down this website then?

MS. FISHER. I will leave that to the FBI.

MR. STUPAK. Okay, someone tell me.

MR. SWECKER. I can just say that all the information that was given to us is being aggressively pursued, very aggressively pursued with substantial resources. Without going into the details--

MR. STUPAK. Sure. So are there going to be more indictments or what? You have 1,500 names and addresses, credit card information, physical addresses, IP addresses. Do you anticipate more indictments or anything on this case? It has been 8 months.

MR. SWECKER. It is ongoing, but what I would like to do is have Mr. Bell just generically go over--

MR. STUPAK. We all sit here and talk about the courage of these young people coming here, and when they give you the information and it is 8 months and you get two out of 1,500, their confidence is rather shaken. I think we do more harm to these young people who are willing to step forward if we take the information and it is such a slow process. The website, the person fled the country. That is a given, right? The operator fled the country by the time you got around to it.

MR. SWECKER. The agents working this case, the prosecutors working this case are aggressively pursuing every lead in this case.

MR. STUPAK. Understood, and I have heard that so much today, but the point I hope you understand as we sit up here and these young people who are willing to come forward, and we hear oh, we are aggressively pursuing this case. Justin Berry has gone to you a couple times and asked for information, and no one would give him information. Don't you think you at least owe him an explanation what is going on, other than can't talk about it or ongoing pending case?

MR. SWECKER. Sir, I know you have a law enforcement background and I know that you know that we don't discuss cases with witnesses in terms of the details of the case.

MR. STUPAK. But you certainly discuss cases with the victim, because they have the right to know.

Let me ask this one. The Chairman was making an excellent point, Chairman Barton. In the UK, Internet service providers have a process

for identifying websites that contain this filth and remove those images 48 hours after identification, unless law enforcement requests otherwise. I understand that is a voluntary regulatory system that will not work here, as most of our ISPs are unwilling to even use the NCMEC reporting forms. The UK reduced the percentage of its images located on their servers from 18 percent of the worldwide total to four tenths of one percent in 2005. In 2 years, they went from 18 percent to four tenths of one percent. Of course, that doesn't count the U.S. part.

So has the Department thought about requesting from the Congress some legislation that would create a mechanism to notify ISPs of violation or sites that may be violating and mandate removal of these sites from our servers within 48 hours of notification from either NCMEC or from law enforcement? Have you thought about that?

MS. FISHER. Congressman, just last week when I met with the ISPs I raised this issue with them, and I know they are coming in next week to talk about this. In fact, one of the ones that I met with is AOL, who has been a very good reporter to NCMEC, but they, I believe, are on the board of that entity in the UK, and so I think that they would be better seen to address that particular issue, but I can tell you that we constantly work with the ISPs and with NCMEC to do everything that we can.

MR. STUPAK. All right, I guess we will talk to the ISPs.

Do you have any suggestions? We heard administrative warrants last hearing on how we crack down on this, other than talk to the ISPs? We heard administrative warrants, which I thought was a good idea. We will work on that. Do you have any other comments for us or this proposal that you gave us today where you shifted to the Federal Communications Commission? Any other suggestions?

MS. FISHER. I applaud the legislation that was passed by the House that is now pending with the Senate. I think that you should look at sentencing reform with regard to the downward departures, that is an issue. There is something called the cyber convention that is now pending also in the Senate that tries to get our foreign countries that sign on to that cyber crime treaty to have data retention in place so we can work with our international partners. I think any--

MR. STUPAK. Let me ask you this idea. How about if we pay overtime to local law enforcement who work this area? You do it Justice-based terrorism task force and violent crime task force, because the sergeant who really broke Masha's case doesn't do it anymore because his jurisdiction can no longer afford the overtime. So why doesn't Justice use some of that money and pay overtime to local law enforcement who seem to be ahead of this problem, or trying to stay ahead of this problem? Would that be an idea?

MS. FISHER. Certainly. We do send money out through the ICECs to help the local efforts. The State and locals do such an amazing job at combating child exploitation, and I commend them for their work.

MR. STUPAK. Thank you, Mr. Chairman.

MR. WHITFIELD. The gentleman's time is expired.

At this time, I recognize Mr. Walden for 10 minutes.

MR. WALDEN. Thank you very much, Mr. Chairman.

Ms. Fisher, at our hearing on April 4, concerns were raised by Justin Berry and his attorney, Steve Ryan, about the handling of Justin's case by Department of Justice. I am sure you are aware of our hearing. In particular, Justin and Mr. Ryan described how an affidavit was unsealed in the case involving Gregory Mitchel, a man we understand allegedly molested Justin and also was engaged in a commercial enterprise involving the production of sexually exploitative images of children. The unsealing of this affidavit was particularly detrimental to Justin because it was only partially redacted and contained information that other child predators involved with Mr. Mitchel in this commercial enterprise would realize came from Justin. In effect, it alerted, I should say, other potential perpetrators that Justin was a government witness.

Mr. Ryan, Justin's attorney, testified under oath that he had been assured the day before the unsealing of Mr. Mitchel's affidavit by Mr. Andrew Oosterbaan, head of the CEOS section, that the affidavit would remain sealed. Subsequently, we learned that an error was made and the affidavit was unsealed. I understand that those sorts of mistakes can happen. However, I asked Justin's attorney, Steve Ryan, while he was under oath, whether he, on behalf of Justin, ever requested the Justice Department reseal the affidavit. Mr. Ryan said that he would get back to us on that question because he wanted to make sure he gave us an accurate response. I have an e-mail that was forwarded from Mr. Ryan to staff the following day. There should be a copy of it on the dais for you if you want to read it.

MS. FISHER. That is okay.

MR. WALDEN. We can share it with you. I don't know if somebody is able to do that.

I would like to move that the e-mail be entered into our record, Mr. Chairman.

MR. WHITFIELD. Without objection.

[The information follows:]

**Andrews, Kelli**

**From:** Ryan, Stephen [sryan@manatt.com]  
**Sent:** Wednesday, April 05, 2006 2:20 PM  
**To:** Paoletta, Mark; Andrews, Kelli  
**Cc:** kewald@nytimes.com; speak2justin@gmail.com  
**Subject:** Vital email re: releaseof affidavit

Yesterday Congressman Walden asked me during testimony if I had asked CEOS to reseal the affidavit. I could not recall doing so myself, but I attach documentary proof we did so contemporaneously. I was in Kansas City traveling and directed my partner to do so. You will also see earlier versions of the Department's dog ate the homework. It is very important to me that Congressman Walden knows that we did request resealing. Sorry my memory was inexact.  
 Steve Ryan.

-----Original Message-----

**From:** Roth, Holly  
**Sent:** Thursday, September 15, 2005 6:35 PM  
**To:** 'Andrew.Oosterbaan@usdoj.gov'  
**Cc:** Sherri.Stephan@usdoj.gov; Stephanie.Thacker@usdoj.gov; Ryan, Stephen  
**Subject:** RE: Immunity Agreement

**Drew:**  
 Reserving all of our rights in light of what has happened, we would like you to take every possible action to get the warrant affidavit back under seal. Please advise us right away of your position on this.  
 Holly

-----Original Message-----

**From:** Andrew.Oosterbaan@usdoj.gov [mailto:Andrew.Oosterbaan@usdoj.gov]  
**Sent:** Thursday, September 15, 2005 6:04 PM  
**To:** Roth, Holly  
**Cc:** Sherri.Stephan@usdoj.gov; Stephanie.Thacker@usdoj.gov; Ryan, Stephen  
**Subject:** RE: Immunity Agreement

Steve and Holly:

The US Attorney in the WDVA (Roanoke) just called to advise that, on its own, the clerk of court redacted and unsealed the arrest warrant affidavit issued against Mitchel. The redacted affidavit is attached. I have not had a chance to review it yet, but the USA told me that the names had been redacted. We had the Assistant United States Attorney check with the clerk only yesterday to ensure that the affidavit would not be unsealed. He learned then that, because it had been sealed by order of the court, it would not be unsealed until 30 days had expired, unless we moved to extend. Obviously that did not happen.

The USA also advised that a local reporter had the affidavit and planned to publish a story in the local paper tomorrow. I just wanted you to know.

Drew

---

#####  
 IRS CIRCULAR 230 DISCLOSURE: To comply with requirements imposed by recently issued treasury regulations, we inform you that any U.S. tax advice contained in this communication (including any attachments) is not intended or written by us, and cannot be used by you, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another person any transaction or matter addressed herein. For information about this legend, go to [http://www.manatt.com/uploadedFiles/Areas\\_of\\_Expertise/Tax\\_Employee\\_Benefits\\_and\\_Global\\_Compensation/Circular230.pdf](http://www.manatt.com/uploadedFiles/Areas_of_Expertise/Tax_Employee_Benefits_and_Global_Compensation/Circular230.pdf)

1

MR. WALDEN. The e-mail he forwarded staff is an e-mail dated September 15 of 2005 from Holly Roth, an attorney working with Mr. Ryan and Justin, to Mr. Andrew Oosterbaan, Sherri Stephan of DOJ, and Stephanie Thacker of DOJ. In this e-mail, Ms. Roth writes, and I quote "Drew: Reserving all of our rights in light of what has happened, we would like you to take every possible action to get the warrant affidavit back under seal. Please advise us right away of your position on this." We note this affidavit remains unsealed. Can you explain to us why this affidavit was not resealed?

MS. FISHER. Well, I can. When this e-mail was sent about resealing the affidavit, which the complaint underlying arrest warrant affidavit that

describes all the facts that was unsealed in a redacted form by the court, that affidavit was already in the public realm, and according to the U.S. Attorney, the press already had that affidavit. So the judgment was made that they would offer protection for Justin, and I believe that that offer--

MR. WALDEN. Physical protection?

MS. FISHER. Yes, physical protection and any other kind of protection, and that was made. Of course, because the Mitchel case was ongoing, he had already had his initial appearance and he was going forward, that affidavit at some point was going to become unsealed, but at that period of time after this Thursday e-mail, that is the event that took place.

MR. WALDEN. But is that sort of standard procedure in these types of cases?

MS. FISHER. Eventually, yes. The complaint and the affidavit--if there is a complaint and an affidavit, they are unsealed as to the defendant because the defendant gets to know the charges against him.

MR. WALDEN. Sure.

MS. FISHER. And then as the case progresses, sometimes it is 30 days, sometimes it is immediate, sometimes it is a little bit later, those documents are unsealed because the case is going on and the defendant is making further appearances, and of course, our court proceedings are public.

MR. WALDEN. Okay.

MS. FISHER. But let me assure you, Congressman, because I think this gets at the issue. There would never be a deliberate attempt by the Justice Department to put a victim or a cooperating witness in harm's way. There certainly was no attempt to do that here. We want to protect our victims and we want to protect our investigation and our case.

MR. WALDEN. Sure, but when Mr. Ryan asked that it be resealed, why was it--that just didn't matter at that point?

MS. FISHER. It is not that it didn't matter at all. Unfortunately, it was already in the public realm and so resealing would have been ineffective, so the judgment was made at the time by the people on the ground to offer him protection.

MR. WALDEN. Okay. And when you say it is already in the public realm, does that mean that it was at one time open and available but could it--I am not an attorney, so you are going to have to work with me on this. But resealing it, would that take it out of the public realm?

MS. FISHER. Well, when I said it was already in the public realm, the press in Roanoke already had a copy of the affidavit and had called the U.S. Attorney in Roanoke, according to my conversations with the U.S. Attorney in looking into this. And so it was already in the public realm, and of course, it had been made--



MR. WALDEN. But it was like one reporter in Roanoke had it?

MS. FISHER. I believe that is right but I am not sure that they knew that at the time. But I think that when they were considering whether resealing would be effective, and of course, it would only have remained resealed for a certain period of time--

MR. WALDEN. How long would that be, normally, in a case?

MS. FISHER. It would depend on the local rules in the courthouse down there. Sometimes it is 15 days, sometimes it is longer. It depends on your relationship with the court and the motions that are filed. But this was not done on purpose. We want to protect our victims. I am sorry that it happened. I believe everybody is sorry that it happened.

MR. WALDEN. Okay.

Mr. Roldan, what is the current budget for the Innocent Images Unit?

MR. ROLDAN. Sir, I can break it down for you, but--

MR. WALDEN. You need to turn your mic on there if you would. Thank you, sir.

MR. ROLDAN. I can break it down for you, sir, but right now it is a little bit less than \$20 million.

MR. WALDEN. And is it--

MR. ROLDAN. Including personnel.

MR. WALDEN. And has the Unit's budget been the same since its inception?

MR. ROLDAN. No, sir. It started in 1998 and we received 60 positions equivalent to \$5.8 million.

MR. WALDEN. That was in '98?

MR. ROLDAN. In 1998. We also received--

MR. WALDEN. And what is it today?

MR. ROLDAN. Total in personnel or non-personnel. I will give you the whole--1998, 60 positions, equivalent \$5.8 million.

MR. WALDEN. Okay.

MR. ROLDAN. In addition, non-personnel \$4.2 million. In 1999, 45 positions equivalent to \$5.2 million.

MR. WALDEN. So it has gone down?

MR. ROLDAN. No, in addition. This is reoccurring. So in addition to the 60 positions, we received an additional 45 positions.

MR. WALDEN. You got an additional 45 positions.

MR. ROLDAN. Yes, sir.

MR. WALDEN. Okay.

MR. ROLDAN. And in 2005, in addition to the \$4.2 million non-personnel, we received an additional \$3 million non-personnel. No additional positions, but we received \$3 million in non-personnel. So now we are up to \$7.2 million reoccurring. It will reoccur every year.

And then in 2006, we received an additional 22 positions, which is approximately \$2.69 million.

MR. WALDEN. Okay. Do you believe that is adequate to keep up with the volumes we are hearing about here?

MR. ROLDAN. We could use more resources in this particular matter, obviously, from the numbers we are getting.

MR. WALDEN. All right.

Within the cyber crimes section, what priority is placed on Innocent Images investigations as opposed to intellectual property crimes, such as downloading music from the Internet, for example? How many positions do you have on these intellectual property cases?

MR. ROLDAN. Minimal, sir. As a matter of fact, the Innocent Images program is just below the intrusion matters, which address counterterrorism and counterintelligence.

This was just recently changed, too, by the way.

MR. WALDEN. When?

MR. ROLDAN. Most recently, we started working on a national strategy approximately a year ago or a little less than a year ago, and that national strategy was recently signed. That is where the changes were made.

MR. WALDEN. Okay, because it used to be like third in your priority, didn't it?

MR. ROLDAN. Yes, sir, you are correct.

MR. WALDEN. After intellectual property cases, after hacking, and after intrusion?

MR. ROLDAN. Yes, sir, you are correct.

MR. WALDEN. Okay. All right.

Ms. Fisher, one final question on this affidavit issue. Have you ever resealed an affidavit in a case?

MS. FISHER. No, sir. I have not had occasion to do so.

MR. WALDEN. Does it ever happen in--I meant the Justice Department in general, not necessarily you personally.

MS. FISHER. The Justice Department, I couldn't say for the entire Justice Department. I think it unusual, but I would never say that it couldn't happen or wouldn't happen. It would be up to the court, obviously.

MR. WALDEN. All right.

MS. FISHER. Could I clarify one thing--

MR. WALDEN. Sure.

MS. FISHER. --Mr. Chairman? I think I mentioned the cyber crime treaty earlier as something that could be done and could be worked on that is in the Senate right now, and I mentioned it in regards to data retention. It actually helps us with international cooperation and

information sharing, not data retention, so I apologize for that. I just wanted to clarify that for the record.

MR. WALDEN. All right. Thank you, Mr. Chairman. My time is expired.

MR. WHITFIELD. Thank you, Mr. Walden.

At this time, I recognize Dr. Burgess for 10 minutes.

MR. BURGESS. Thank you, Mr. Chairman. I apologize for being out of the room for a while during part of the testimony.

When evidence comes to light that some of this activity has been going on, but it comes to you late, does it reach a point where the evidence is just too stale to pursue an investigation or a search warrant?

MS. FISHER. There could be a staleness problem with regard to search warrants, but as far as the investigation goes, I would defer that to Mr. Swecker.

MR. SWECKER. Can you repeat that question?

MR. BURGESS. If you don't catch something right away, is there an expiration date on the ability to investigate it and pursue a search warrant?

MR. SWECKER. The answer is yes, because data can become stale and you can't use it in a search warrant, for example, because it is not current enough. We often get information that is a year, 2 years old, and unless you can update that information and get it to the point where it is fresh enough to get a search warrant, you can't act on it without just knocking on the door and doing the knock and talk that I think Raul discussed earlier.

MR. BURGESS. So then what happens? Does the case just get dropped?

MR. SWECKER. No. I mean, if you have a list of subscribers that are 2 years old, for example, you continue with the investigation. It goes into a database. If you do get to the names of the subscribers and you get the information on it, that goes into the Innocent Images database and usually we run across these folks again.

So it doesn't just die, I mean, the investigation continues on.

MR. BURGESS. Is there any tool that we could give you here that would help you with the staleness problem? Is there any legislative tool that Congress could supply you?

MR. SWECKER. I will defer to Justice on that one. I mean, we like data retention. It is a question of how long and how much data is going to be retained. There is an issue with our regional forensic labs, frankly. There is a bottleneck there. Innocent Images cases, as we refer to them, have to take a backseat to terrorism exploitation with respect to our computer forensic examinations. There are only about nine labs, I believe, forensic labs around the country right now, and these are labs

that are shared by State and local and FBI and other Federal agencies. There are times when we can't get to this information because of the press of terrorism, counterintelligence cases, and other cases that the Director has stated, and rightfully so, that are higher priorities. So more forensic labs would help.

MR. BURGESS. I have a hard time differentiating between this type of terrorism and some of the other types that you pursue, but I understand what you are saying.

So you will try to pursue a case even though some of the information has become quite dated?

MR. SWECKER. Yes. Arnold, can you elaborate on that a little bit?

MR. BELL. Yes, sir.

Even when we receive dated information, we have several databases that are contained in house. In addition, we have databases that are available to us at the National Center for Missing and Exploited Children. We will take the names of the individuals that we have, we will take whatever information we have, and we will bounce it off those databases. Sometimes we find people that we have encountered before, sometimes we find people that we already have active investigations on, or when we go through the National Center, some other agency may have active investigations on. The information that we have, if someone else has an investigation, our information generally will bolster some other investigation or allow us to continue on with investigations we might already have ongoing on a particular subject. For example, on a website case we might have 10,000 such leads, but all that information might be 2 or 3 years old. We bounce that off of all the databases that are available to us.

MR. BURGESS. So you have someone who is continually working on those?

MR. BELL. We do those regularly.

MR. BURGESS. Do you have any--I mean, are there success stories from successful prosecutions from that?

MR. BELL. You know what, I can't think of any that came specifically from some data of that age right now. I am sure there are. I can get back to the committee if it is necessary.

MR. BURGESS. Well, I am sure all of you were in the room when we heard the testimony from the pervious panel. I have just got to tell you, I am really bothered by human traffickers masquerading as adoption agencies. I mean, I had no idea that that sort of thing could even happen.

Is there any role for the Department of Justice or the FBI in working up these cases and pursuing these individuals? I mean, that is really at the heart of what we are talking about, from the standpoint of the Internet. The Internet has put all of this stuff on steroids. At the heart of

it, you had a pedophile go overseas and adopt a baby, and went through three agencies in order to do it. Is that possible?

MS. FISHER. It was such a sad and horrific story that she told, and she is such a brave girl.

I was thinking that same thing as she was testifying, is there something--

MR. BURGESS. Well, are you guys investigating--

MS. FISHER. --for the Department--

MR. BURGESS. Go ahead--aspects of those adoption agencies? I mean, I don't want to come down hard on international adoption agencies that are doing good work and providing people the children they have always longed for, but this is so heinous. Surely, the FBI is investigating adoption agencies, international adoption agencies, after seeing this kind of information, because as someone on the previous panel said, there have got to be other Mashas out there. We just haven't found them yet.

MR. SWECKER. Can I address that?

MR. BURGESS. Sure, I wish you would.

MR. SWECKER. You hit it right on the head. It is a human trafficking case, and we address human trafficking cases. We have a pretty sizeable inventory of human trafficking cases. We can get back to you as to how many of those that would involve adoption agencies. As you know, we played a role in this case, although it was first scoped out by a local officer. He came to the FBI for some additional help in getting the search warrant put together and actually conducting the raid.

But to answer your question, we do have a role to play.

MR. BURGESS. Are any of the people who were involved in this case that was before us today, any of the adoption agency people in jail, on trial, awaiting trial? Has anyone been punished for what happened to this 5-year-old?

MR. SWECKER. Not that I am aware of.

MS. FISHER. Other than the defendant, her adoptive father who is in prison, I am not aware of any others.

MR. BURGESS. And I mean, the failures are--her teachers, I don't know whether she got medical care during her 5 years with this guy. I don't know whether he took her in for her immunizations. If she went to school, I presume she had immunizations. I presume she was weighed by a nurse and someone should have noted that her weight was lower than the 20<sup>th</sup> percentile for a 10-year-old. I mean, it is just hard to imagine how this was missed over and over and over again. The failings of our system are just rampant in this case.

The Toronto police department spent considerable time and resources to find this child, only to learn that her identify had been--or

that she had been found 2 years earlier by the FBI working with the Chicago police department. Do you have things in place internationally now to try to help that? What is being done amongst Federal law enforcement agencies and the Justice Department?

MR. SWECKER. The answer is yes. Our database has been merged with the National Center for Missing and Exploited Children database, which is actually when the match was made in this case two years after she was recovered. NCMEC has put out a list of protocols that need to be followed in these types of cases, and as a last resort, placing the child's picture out on the public domain. That protocol wasn't followed in this case, and I will let Arnold follow up on that, but we can't force other international law enforcement agencies to follow those protocols. They are really advisory in nature. Most countries do.

MR. BURGESS. How do our efforts compare with that of other countries? Are we keeping up?

MR. SWECKER. We do. We have recovered--in comparison to the international law enforcement agencies, we have recovered 124 children versus the combined efforts of 181 other countries in the recovery of about 257 children. So one agency has recovered 124; combined, 181 agencies have recovered 250. So we compare, I mean, we lead the world in these types of investigations in terms of recovered children.

MR. BURGESS. Is there any idea how big the universe of children who are exploited by child predators is? I mean, how does that figure of 187 compare with--

MR. SWECKER. We tried to take a stab at that a little earlier, and we think it is hundreds of thousands internationally, probably tens of thousands--

MR. BURGESS. Probably not a great figure.

MR. SWECKER. --nationally.

MR. BURGESS. Mr. Chairman, it has been a long day. This is an emotionally exhausting topic. I am going to yield back the balance of my time.

MR. WHITFIELD. Thank you, Mr. Burgess.

Once again, I want to thank the panel. We look forward to continuing to work with you as we continue efforts in this area. The record will remain open for 30 days and the documents and these records will be submitted in to be formally a part of the record.

[The information follows:]

109TH CONGRESS  
2D SESSION

# H. R. 4703

To provide meaningful civil remedies for victims of the sexual exploitation of children.

---

## IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 7, 2006

Mr. GINGREY (for himself and Mr. TIERNEY) introduced the following bill; which was referred to the Committee on the Judiciary

---

## A BILL

To provide meaningful civil remedies for victims of the sexual exploitation of children.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. CIVIL REMEDIES.**

4 (a) IN GENERAL.—Section 2255(a) of title 18,  
5 United States Code, is amended—

6 (1) in the first sentence—

7 (A) by striking “(a) Any minor who is”

---

8 and inserting the following:

9 “(a) IN GENERAL.—Any person who, while a minor,  
10 was”;

1 (B) by inserting after “such violation” the  
2 following: “, regardless of whether the injury  
3 occurred while such person was a minor,”; and

4 (C) by striking “such minor” and inserting  
5 “such person”; and  
6 (2) in the second sentence—

7 (A) by striking “Any minor” and inserting  
8 “Any person”; and

9 (B) by striking “\$50,000” and inserting  
10 “\$150,000”.

11 (b) CONFORMING AMENDMENT.—Section 2255(b) of  
12 title 18, United States Code, is amended by striking “(b)  
13 Any action” and inserting the following:

14 “(b) STATUTE OF LIMITATIONS.—Any action”.



**UNITED STATES CODE – TITLE 42****Section 13032. Reporting of child pornography by electronic communication service providers**

## (a) Definitions

In this section -

- (1) the term "electronic communication service" has the meaning given the term in section 2510 of title 18; and
- (2) the term "remote computing service" has the meaning given the term in section 2711 of title 18.

## (b) Requirements

## (1) Duty to report

Whoever, while engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce, obtains knowledge of facts or circumstances from which a violation of section 2251, 2251A, 2252, 2252A, or 2260 of title 18, involving child pornography (as defined in section 2256 of that title), is apparent, shall, as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children, which shall forward that report to a law enforcement agency or agencies designated by the Attorney General.

## (2) Designation of agencies

Not later than 180 days after October 30, 1998, the Attorney General shall designate the law enforcement agency or agencies to which a report shall be forwarded under paragraph (1).

## (3) Failure to report

A provider of electronic communication services or remote computing services described in paragraph (1) who knowingly and willfully fails to make a report under that paragraph shall be fined -

(A) in the case of an initial failure to make a report, not more than \$50,000; and

(B) in the case of any second or subsequent failure to make a report, not more than \$100,000.

## (c) Civil liability

No provider or user of an electronic communication service or a remote computing service to the public shall be held liable on account of any action taken in good faith to comply with this section.

## (d) Limitation of information or material required in report

A report under subsection (b)(1) of this section may include additional information or material developed by an electronic communication service or remote computing service, except that the Federal Government may not require the production of such information or material in that report.

## (e) Monitoring not required

Nothing in this section may be construed to require a provider of electronic communication services or remote computing services to engage in the monitoring of any user, subscriber, or customer of that provider, or the content of any communication of any such person.

(f) Conditions of disclosure of information contained within report

(1) In general

No law enforcement agency that receives a report under subsection (b)(1) of this section shall disclose any information contained in that report, except that disclosure of such information may be made -

(A) to an attorney for the government for use in the performance of the official duties of the attorney;

(B) to such officers and employees of the law enforcement agency, as may be necessary in the performance of their investigative and recordkeeping functions;

(C) to such other government personnel (including personnel of a State or subdivision of a State) as are determined to be necessary by an attorney for the government to assist the attorney in the performance of the official duties of the attorney in enforcing Federal criminal law; or

(D) as permitted by a court at the request of an attorney for the government, upon a showing that such information may disclose a violation of State criminal law, to an appropriate official of a State or subdivision of a State for the purpose of enforcing such State law.

(2) Definitions

In this subsection, the terms 'attorney for the government' and 'State' have the meanings given those terms in Rule 54 of the Federal Rules of Criminal Procedure.



**U.S. Department of Justice**  
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 20, 2006

The Honorable J. Dennis Hastert  
Speaker  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Mr. Speaker:

As you may be aware, this morning the Attorney General announced that today the Administration would transmit to Congress a new legislative proposal, the Child Pornography and Obscenity Prevention Amendments of 2006. This proposal, which is attached for your convenience, will help to ensure that electronic communications providers report the presence of child pornography on their systems by strengthening the criminal penalties for failure to report it. It will also prevent people from inadvertently stumbling across pornographic images on the Internet.

If we can be of further assistance, please do not hesitate to contact this office. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this package.

Sincerely,

A handwritten signature in cursive script that reads "William E. Moschella".

William E. Moschella  
Assistant Attorney General

Attachment

**A BILL**

To enhance prosecution of child pornography by strengthening section 13032 of title 42, United States Code, to ensure that child pornography is effectively reported, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SEC. 1. SHORT TITLE.**

- (1) Short Title- This Act may be cited as the 'Child Pornography and Obscenity Prevention Amendments of 2006'.
- (2) Table of Contents- The table of contents for this Act is as follows:
  - Sec. 1. Short title.
  - Sec. 2. Findings.
  - Sec. 3. Strengthening section 13032 of title 42 to ensure that child pornography is effectively reported.
  - Sec. 4. Requiring that warning labels be placed on commercial websites containing sexually explicit material.
  - Sec. 5. Prohibiting the embedding of words or images on a website in order to deceive individuals into viewing obscenity or material harmful to minors.

**SEC. 2. FINDINGS.**

Congress makes the following findings:

- (1) The importance of electronic communications service providers reporting the presence of child pornography on the Internet to the CyberTipline at the National Center for Missing and Exploited Children:
  - (A) A substantial interstate market in child pornography exists, including not only a multimillion dollar industry, but also a nationwide network of individuals openly advertising their desire to exploit children and to traffic in child pornography. Many of these individuals distribute child pornography with the expectation of receiving other child pornography in return.
  - (B) The interstate market in child pornography is carried on to a substantial extent through the mails and other instrumentalities of interstate and foreign commerce, such as the Internet. The advent of the Internet has greatly increased the ease of transporting, distributing, receiving, and advertising child pornography in interstate commerce. The advent of

digital cameras and digital video cameras, as well as videotape cameras, has greatly increased the ease of producing child pornography. The advent of inexpensive computer equipment with the capacity to store large numbers of digital images of child pornography has greatly increased the ease of possessing child pornography. Taken together, these technological advances have had the unfortunate result of greatly increasing the interstate market in child pornography.

- (C) Ensuring that electronic communication service providers effectively report violations of the child pornography laws to the CyberTipline at the National Center for Missing and Exploited Children, which in turn will forward that report to law enforcement agencies designated by the Attorney General, will reduce both supply and demand in the interstate market for child pornography and will enhance the prosecution of such offenses.
- (2) The importance of requiring that warning labels be placed on commercial websites that contain sexually explicit material:
- (A) The World Wide Web contains a substantial amount of sexually explicit content that is inappropriate for children to view.
  - (B) Many such commercial websites may accidentally be visited by children or other individuals who do not wish to view sexually explicit content.
  - (C) The provision of information on each page of a commercial website that contains sexually explicit material indicating that such material is present will enable filtering software and other tools identify web sites to place on their list of sites to be blocked by the software to more effectively protect children and other individuals from inadvertently viewing material that they do not wish to view.
  - (D) Requiring websites to provide information about the presence of sexually explicit material on their "home page" will allow individuals to make an individualized decision about whether to view such material and will protect them from inadvertently being subjected to such material.
- (3) The importance of prohibiting the embedding of words or images on a website in order to deceive individuals into viewing obscenity or to deceive minors into viewing material harmful to minors:
- (A) Many websites containing sexually explicit material attempt to lure unsuspecting victims, primarily children, into visiting these sites by embedding commonly used search terms or phrases within the source code of the website.

- (B) Luring unsuspecting victims to such commercial websites is a form of fraud that has a substantial impact on interstate commerce.
- (C) Prohibiting the use of such misleading and deceptive words or images will serve to reduce the instance of such fraudulent activity.

**SEC. 3. STRENGTHENING SECTION 13032 OF TITLE 42 TO ENSURE THAT CHILD PORNOGRAPHY IS EFFECTIVELY REPORTED.**

Section 13032 of title 42 of the United States Code is amended—

- (1) By amending paragraph (4) of subsection (b) to read as follows:
  - (4) Failure to report.
    - (A) A provider of electronic communication services or remote computing services described in paragraph (1) who knowingly and willfully fails to make a report under that paragraph shall be fined—
      - (i) in the case of an initial failure to make a report, not more than \$ 150,000; and
      - (ii) in the case of any second or subsequent failure to make a report, not more than \$ 300,000.

**SEC. 4. REQUIRING THAT WARNING LABELS BE PLACED ON COMMERCIAL WEBSITES CONTAINING SEXUALLY EXPLICIT MATERIAL**

Title 15 of the United States Code is amended by adding the following—

**§ 7801. Requirement to place warning labels on commercial websites containing sexually explicit material.**

**(1) In general**

No person who operates a website located on the Internet where such website is primarily operated for commercial purposes, in or affecting interstate or foreign commerce, may knowingly, and with knowledge of the character of the material, place on that website sexually explicit material, and—

- (A) fail to include on each page of the website that contains sexually explicit material, the marks and notices prescribed by the Commission under this subsection; and

- (B) fail to provide that the matter on the website that is initially viewable, absent any further actions by the viewer, does not include any sexually explicit material.

**(2) Prescription of marks and notices**

Not later than 90 days after the enactment of this section, the Commission shall, in consultation with the Attorney General, provide by regulation clearly identifiable marks or notices to be included in the code, if technologically feasible, or if not feasible on the pages, of websites that contain sexually explicit material in order to inform the viewer of that fact and to facilitate the filtering of such pages.

**(3) Inapplicability to carriers and other service providers**

This section shall not apply to any person to the extent that person is—

- (A) a telecommunications carrier engaged in the provision of a telecommunications service;
- (B) a person engaged in the business of providing an Internet access service;
- (C) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication made by another person, without selection or alteration of the content of the communication, except that such person's deletion of a particular communication or material made by another person in a manner consistent with any applicable law or regulation shall not constitute such selection or alteration of the content of the communication.

**(4) Definitions**

For the purposes of this section, the term—

- (A) "Commission" means the Federal Trade Commission;
- (B) "website" means any collection of material placed in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol except that the term does not include any collection of material where access to sexually explicit material is restricted to a specific set of individuals through the provision of a password or through another access restriction mechanism;
- (C) "sexually explicit material" means any material that depicts sexually explicit conduct (as that term is defined in subsection (2)(A) of section 2256 of title 18), unless the depiction constitutes a small and insignificant

part of the whole, the remainder of which is not primarily devoted to sexual matters;

- (D) "Internet" means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit information;
  - (E) "Internet access service" means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.
- (5) **Penalties**
- (A) Whoever violates paragraph (1) shall be fined under title 18, or imprisoned not more than 5 years, or both.

**SEC. 5. PROHIBITING THE EMBEDDING OF WORDS OR IMAGES ON A WEBSITE IN ORDER TO DECIEVE INDIVIDUALS INTO VIEWING OBSCENITY OR MATERIAL HARMFUL TO MINORS.**

Title 18 of the United States Code is amended by adding the following—

**§ 2252C. Misleading Words or Digital Images on the Internet.**

- (a) Whoever knowingly embeds words or digital images into the source code of a website with the intent to deceive a person into viewing material constituting obscenity shall be fined under this title or imprisoned not more than 2 years, or both.
- (b) Whoever knowingly embeds words or digital images into the source code of a website with the intent to deceive a minor into viewing material harmful to minors on the Internet shall be fined under this title or imprisoned not more than 4 years, or both.
- (c) For the purposes of this section, a word or digital image that clearly indicates the sexual content of the site, such as "sex" or "porn", is not misleading.
- (d) For the purposes of this section, the term "material that is harmful to minors" means any communication, consisting of nudity, sex, or excretion, that, taken as a whole and with reference to its context—



- (1) predominantly appeals to a prurient interest of minors;
  - (2) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
  - (3) lacks serious literary, artistic, political, or scientific value for minors.
- (e) For the purposes of subsection (d), the term "sex" means acts of masturbation, sexual intercourse, or physical contact with a person's genitals, or the condition of human male or female genitals when in a state of sexual stimulation or arousal.
- (f) For the purposes of this section, the term "source code" means the combination of text and other characters comprising the content, both viewable and non-viewable, of a web page, including but not limited to any website publishing language, programming language, protocol or functional content, as well as any successor languages or protocols.

**Brief Section-by-Section Summary of Proposed Legislation:****Child Pornography and Obscenity Prevention Amendments of 2006****Section 1:**

Sets forth the short title and table of contents for the legislation.

**Section 2:**

Makes findings regarding the importance of: (1) reporting the presence of child pornography on the Internet; (2) requiring the placement of warning labels on commercial websites containing sexually explicit material; and (3) prohibiting the embedding of words or images that are intended to deceive individuals into unintentionally viewing sexually explicit material.

**Section 3:**

Section 3 would amend existing provisions of the law that require certain providers of electronic communications services to report violations of the child pornography laws. Current law provides that a provider who knowingly and willfully fails to report such violations shall be subject to a criminal fine of up to \$50,000 for the initial failure to report and \$100,000 for each subsequent failure to report. Prosecutors and law enforcement sources report that this criminal provision has been virtually impossible to enforce because of the particular mens rea requirement and the low amount of the potential penalty. This legislation would triple the criminal fines available for knowing and willful failures to report, making the available fines \$150,000 for the initial violation and \$300,000 for each subsequent violation.

**Section 4:**

Section 4 requires all websites that are operated primarily for commercial purposes to include specific marks and notices on every page of the website that contains sexually explicit material. The legislation also requires that the material initially viewable by any individual on a website not contain any sexually explicit material absent further actions (e.g., an additional click) by the viewer. Sexually explicit material is defined as material depicting sexually explicit conduct as that term is defined in the criminal code (i.e., sexual intercourse; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person). Websites where access to sexually explicit material is restricted to specific individuals (e.g., password protected websites) are not covered by this legislation. The specifications for the relevant marks and notices are to be provided by the Federal Trade Commission in consultation with the Attorney General. The legislation employs language similar to that of the CAN-SPAM Act, 15 U.S.C. § 7704(d), in order to require the placement of warning labels on websites. The legislation provides for a criminal fine and up to five years in prison, or both, for violations of this provision.

**Section 5:**

Section 5 would prohibit the practice often engaged in by certain sexually explicit websites of hiding innocuous terms in a website's hypertext markup language so that a search for those terms on the Internet yields links to the sexually explicit websites. For example, the owner of a website called, say, "pornphotos.com", can hide the words, "Disney," "Bob the Builder," and "Barbie" in the computer code used to program the website, so that a search through Google for sites about Disney, Bob the Builder, or Barbie would bring up "pornphotos.com" in addition to "disney.com," "bobthebuilder.com" or "Barbie.com." A child or other individual who was not interested in or expecting to come across pornography would then unwittingly be directed to such material. The text of the section is similar to that of 18 U.S.C. § 2252B, the Misleading Domain Names Act, which prohibits use of domain names, such as "www.dinseyland.com" and "www.bobthebiulder.com," that are intended to draw children and others to sexually explicit sites if they make typing errors when searching for a site. The legislation would prohibit an individual from knowingly acting with the intent to deceive another individual into viewing obscene material and provides for a criminal fine and up to two years in prison, or both, for violations of this provision. The legislation would also prohibit an individual from knowingly acting with the intent to deceive a minor into viewing material harmful to minors and provides for a criminal fine and up to four years in prison, or both, for violations of this provision.

NANCY GRACE

Sit-Down With A Molestation Survivor;

Aired January 18, 2006 - 20:00:00 ET

THIS IS A RUSH TRANSCRIPT. THIS COPY MAY NOT BE IN ITS FINAL FORM AND MAY BE UPDATED.

NANCY GRACE, HOST: Tonight, a prime-time live exclusive. In all my years of criminal law, I've never seen anything like it. She was raised with nothing in an obscure Russian orphanage, abandoned by her own mother. But then, suddenly, an adoptive father comes to the rescue.

Tonight, the story of a little girl adopted through a legitimate U.S. adoption agency to an American pedophile. From ages 5 to 10, she endured nightly molestation, and then being photographed by her adoptive father, making her one of the most popular child porn stars on the Internet. But this story doesn't end in tragedy.

Tonight, the miracle girl who beat the odds. The little girl who survived is with us live.

Good evening, everybody. I'm Nancy Grace.

I want to thank you for being with us tonight.

Tonight, an unprecedented live exclusive with a child who has shown more courage in her short life than most of us show in a lifetime. Abandoned by her own mother, she escaped a Russian orphanage, where she kept all her worldly possessions under her pillow, to America.

Yes, she was adopted by an American -- an American pedophile. For five years, she lived through torture, starting at age 5. Horrible child porn of this little child plastered on the Internet.

Tonight, the American adoption agency that let it happen, the detective who never gave up, and the little girl who is no longer an anonymous face on the Internet porn sites. It's a story of survival of Masha Allen.

(BEGIN VIDEOTAPE)

UNIDENTIFIED FEMALE: Based upon all the evidence that we had seen, it does appear that the adoption was motivated by the defendant's interest in sexual activity, illegal sexual activity with children.

UNIDENTIFIED MALE: Once you've seen the images and you've seen the collection, this -- this set of pictures is, it breaks your heart.

MASHA ALLEN, CHILD PORNOGRAPHY SURVIVOR: My pictures that are on the Internet disturb me more than what Matthew did because I know that the abuse stopped but those pictures are still on the Internet.

UNIDENTIFIED FEMALE: I feel so much guilt for what happened. When I first found out that he adopted a little girl, I should have spoke up. I should have said something. I feel somewhat responsible.

(END VIDEOTAPE)

GRACE: Tonight, with us here in our Headline News studio, Masha.

Thank you for being with us.

ALLEN: Thank you.

GRACE: I know you. But you don't know me. But I have known about you for a really long time.

We have all been looking for you, trying to find you, along with the detectives and the police all over the world. And now here you are.

Thank you.

I want to start at the beginning. What was it like? Most of us don't understand what it was like to grow up in a Russian orphanage.

ALLEN: It was hard. Like, to me, it seemed like it was dark. You couldn't trust anybody. You didn't really have any of your own possessions.

GRACE: And it broke my heart when I learned you put all your possessions under your pillow every night.

ALLEN: If you didn't, they'd steal them or -- like, just a bad place to be.

GRACE: Did you think your mom, your mother was going to come get you?

ALLEN: She did visit me a couple times and said that she would come get me. But I waited and she never came. So eventually I just gave up hope that she would come and get me.

GRACE: When did you find out you had a family coming get you?

ALLEN: I was listening to the older people talking and they were saying names of children that were going to be adopted or that were going to leave, and they said my name. And I was excited. And I didn't really know what to think because I was confused. So I went and told all my friends there, told everybody there.

GRACE: You went and told your friends what?

ALLEN: That I was going to leave.

GRACE: Were you happy?

ALLEN: Yes, I was.

GRACE: What did you think it was going to be like?

ALLEN: Everybody there said it was going to be a great place, that I would get my own room and I'd get a mother and a father and a family and they would be all nice and happy.

GRACE: Did you know you were coming to America?

ALLEN: No. Not at the time.

GRACE: How did you find out you were coming to America?

ALLEN: I think Matthew told me. The second time he came...

GRACE: OK. Who is Matthew?

ALLEN: Matthew is the person that adopted me from Russia.

GRACE: Your adopted dad?

ALLEN: Yes. My adopted father.

GRACE: He told you what now?

ALLEN: He told me that I was going to the United States.

GRACE: So the first time you saw him was when, when he took you home?

ALLEN: No. He visited a couple times.

GRACE: Do you recall the day you went home, you flew home to America?

ALLEN: It was kind of a blur, but I don't remember -- like, I don't remember anything early in the day. I remember leaving the orphanage.. And -- well, this was before we left, but we went to his friend Sergei's (ph) house and stayed for about a month there.

GRACE: Why?

ALLEN: The day we left, we took two planes to...

GRACE: Did you -- were you -- what did you think when you found out you weren't going to have a mommy?

ALLEN: I did ask him. And he said he wasn't married. And I was sad, and I thought that was just natural to have a mother because I had a mother that abused me, and still I had a mother. And just -- it was sad.

GRACE: You said even though your Russian mom abused you, you still had a mother. But then -- now you wouldn't have one at all.

Did that make you sad or were you just happy to be adopted?

ALLEN: I was sad, but at the same time, I was -- I thought I shouldn't be sad over that. I should just be grateful that I'm adopted.

GRACE: So when you came to America with your new father, what happened when you first got home?

ALLEN: He took me home and we ate and he showed me around the house. And I didn't have a bedroom. And kids at the orphanage said I'd get my own room. And I was shocked. I didn't have my own bed.

GRACE: Did you ask him?

ALLEN: I did. And he said that -- he didn't really give me a straight answer. He just said that I wasn't going to need a bed. I felt...

GRACE: Where did you end up sleeping?

ALLEN: I slept with him.

GRACE: OK. Masha, do you recall your first night in your new home?

ALLEN: Yes. It was really hard. I couldn't get to sleep because he tried to touch me or tried to do something to me.

GRACE: What was he trying to do?

ALLEN: Trying to touch me. It didn't get really worse until after a couple of nights. And so it just kept getting worse, and it was hard because I wasn't getting a lot of sleep. And, like, after the first night, I knew that it wasn't going to be all that great.

GRACE: Did your adopted father molest you?

ALLEN: Yes.

GRACE: What happened?

ALLEN: He'd touched me or touched my private parts or make me touch his private parts or...

GRACE: Did you ever tell anybody?

ALLEN: No. I never told anybody.

GRACE: Did Mancuso, your adopted father, have sex with you?

ALLEN: Yes.

GRACE: And how old were you when that started?

ALLEN: When I was 5 or 6.

GRACE: And how long did that happen?

ALLEN: For the five years I was with him.

GRACE: Did you ever tell anybody?

ALLEN: No. He threatened me. He'd tell me not to tell anybody, or he would say something bad would happen. But he never told me what he would do.

And so, like, I'd be close to telling somebody, but then I'd always not because I'd get afraid of what might happen.

GRACE: What would he give you to eat, Masha?

ALLEN: I had, like, strict diet. I ate peanut butter sandwiches, I didn't eat cooked vegetables, not a lot of meat. I didn't eat that much junk food or candy.

GRACE: Do you know why he didn't feed you enough?

ALLEN: I do now, but at the time he said I was too fat and that I should stop eating as much as I was.



GRACE: You said you do now. Why do you believe now that Mancuso, your adopted father, did not feed you enough?

ALLEN: Well, now, I, like -- a lot of my friends told me that I was really skinny. And now that, like, I actually eat enough, I understand that it's OK to eat until you're actually full. And it's OK to eat the foods that you want eat. And you don't have to be afraid to get what you want to eat. So...

GRACE: Masha, do you remember -- do you have your first recollection of when Mancuso would take pictures of you without your clothes on?

ALLEN: At first it was with my clothes on, but then he'd take me -- he'd tell me to take my top off and just be in my underwear. And then it gradually got worse and I was naked. And...

GRACE: Baby, how old were you when this was happening?

ALLEN: Six.

GRACE: When you think now -- and I want to tell you, you're one of the bravest people I've ever met.

ALLEN: Thank you.

GRACE: When you think that pictures of you went out on the Internet, you must be furious.

ALLEN: I think it's really wrong. And I kind of thought that I was stupid for not figuring it out earlier. But...

GRACE: But you know better than that, right?

Joining me right now is a very special guest joining us out of Washington, D.C.

Elizabeth, do I have Senator Isakson?

Senator Johnny Isakson is from my home jurisdiction of Georgia.

Sir, thank you for being with us.

When you hear Masha speak out, how does it make you feel? And what are you doing about it?

SEN. JOHNNY ISAKSON (R), GEORGIA : Well, it makes me feel, Nancy, exactly like you are. It breaks my heart.

And I'm on tonight because Senator Kerry, who was the original sponsor of this legislation, is still in the Middle East. But John came to me and shared with me Masha's story, the fact that she was a resident in Georgia, and asked me to join with him in a bipartisan effort to bring about some changes.

Nancy, unbeknownst to me, and I think millions of Americans, it was a worse penalty to download music on the Internet illegally than to download child pornography. And what Senator Kerry's introduced and I've co-sponsored with him is legislation to triple the minimum that an individual victim can recover against someone who downloads these pictures on the Internet.

Secondly, it would have been illegal for someone who was violated and whose pictures were used to sue for any damages after they reached the age of majority because of the way the law was worded. So we have lifted that sanction to ensure that even if they go to the age of majority, if it's learned who they are, and those pictures on the Internet, they can sue and they can recover.

It's just a small effort to try to see to it that those victims of this horrible, heinous-type of crime can in some way be compensated and those who violate them can somehow be punished.

GRACE: Mr. Isakson, a lot of America really doesn't know what to make of politicians. Many of us have a bad taste in our mouths. But I have got to tell you, sir, what you and Senator Kerry are doing really restores our faith that someone, one person like Masha can make a difference thanks to you and Senator Kerry.

Everyone, tonight, with us, Senator Johnny Isakson, who has drafted along with Kerry and is pushing through Masha's Law.

Elizabeth, could you roll that sound of our Toronto police officer?

(BEGIN VIDEO CLIP)

UNIDENTIFIED MALE: It's horrific abuse of a very young, vulnerable, child. And you just -- once you have seen the images and you've seen the collection that this -- this -- this set of pictures is, it really breaks your heart.

(END VIDEO CLIP)

GRACE: Here in the studio with me also tonight is another special guest, an adoption lobbyist. She's a child advocate.

With me is Maureen Flatley.

Maureen, you have been on this case from the get-go. And I was especially galled when I learned what type of child Mancuso asked to adopt.

Explain.

MAUREEN FLATLEY, ADOPTION LOBBYIST, CHILD ADVOCATE: Well, he specifically asked for a blond-haired, blue-eyed 5-year-old girl.

GRACE: It's my understanding he asked for a Caucasian child, blond hair, blue-eyed. He was willing to consider a child with disabilities. Also, willing to take a child diagnosed with learning disabilities.

What do you make of him, Maureen?

FLATLEY: Well, I think it's very clear that he was specially ordering a sex slave. And I think that, in fact, the very serious mistake he made is he ended up with Masha, who is a child of enormous intellect and not someone who was going to be victimized without fighting back.

(BEGIN VIDEO CLIP)

SEN. JOHN KERRY (D), MASSACHUSETTS: What does it tell you about Washington's misplaced priorities that the penalty for downloading songs off the Internet is three times what the penalty is for downloading pornography, child pornography?

It's wrong, obviously, that we have tougher penalties for downloading music than that we do for the abuse of our children.

(END VIDEO CLIP)

(COMMERCIAL BREAK)

GRACE: Tonight, detectives in Orange County, Florida, want your help to identify a young girl they call a material witness in a child pornography case. They want to identify a girl seen in a series of sexually explicit photos taken at Walt Disney World and other locations.

The pictures have circulated over the Internet for the past three years. Where is this girl?

Authorities offering a \$5,000 reward for information leading to the girl. As part of the search, detectives released photos of a different girl whom they do not think was sexually exploited, but this photo is of interest because the backgrounds in the photos are incredibly similar.

If you have any information, please, call the Orange County Police, 1-866- 635-4357.

(BEGIN VIDEOTAPE)

GRACE: Tonight, a happy ending to one story that started off horribly wrong. This girl, the victim of over 200 sexually explicit photos on the Internet, we believe, is in foster care tonight. The alleged perpetrator behind bars.

And tonight, I'm looking for the mother.

(END VIDEO CLIP)

GRACE: Welcome back, everybody. That girl here in the studio with us.

The mother that put her up for adoption and abandoned her in Russia -- tonight, with her is her new adoptive mother, Faith (ph). And they're living here in the United States.

So, the end of the story hasn't really come yet. Masha tells me she wants to be a graphic designer, wants to go to school, and wants to bring her attacker to justice.

Straight out to detective Constable Bill McGarry, the lead investigator on this case for over two years.

Why did you become so obsessed with solving this case?

DET. CONSTABLE BILL MCGARRY, LEAD INVESTIGATOR ON CASE: Well, Nancy, Masha, she's not unlike any other child. She's indicative of -- she could be anybody's child.

To see these photographs of her, some over 200 images of her in some of the worst sexually abusive situations that you can imagine, it's just soul-destroying. And you can't not look at her eyes in these images and not want to do something.

GRACE: How did you go about -- and I remember we were trying to help you in your search. How did you go about figuring out where these photos were taken?

MCGARRY: Well, each one of the images -- you've heard the saying a picture tells a thousand words. Well in the backgrounds of these images, there are things that we've learned that we can identify and try to trace at certain geographic locations. And we've had lots of help.

And it's almost like this wasn't a case of finding a needle in a haystack. This was a whole hay field. And we just went through each haystack one at a time.

(BEGIN VIDEO CLIP)

UNIDENTIFIED FEMALE: Why do you have to hurt them to realize that this is your problem. Not a baby's. That these are human beings who have histories, that have personalities, that have potential that you can never imagine.

UNIDENTIFIED MALE: This is not a way to remember your child.

(END VIDEO CLIP)

(COMMERCIAL BREAK)

(BEGIN VIDEO CLIP)

ALLEN: My pictures that are on the Internet disturb me more than what Matthew did because I know that the abuse stopped but those pictures are still on the Internet.

(END VIDEO CLIP)

GRACE: Her perpetrator, her adopted father, American pedophile, living the good life here in a mental facility, Devons (ph) Prison Hospital.

Let's see that menu, Elizabeth. What's Mancuso got tonight? Baked chicken, rice and green beans.

You know, I'm going to relish the thought of Mancuso having a little baked chicken and canned green beans tonight. But what I don't understand, Kevin Rothstein, reporter, "Boston Herald," is why this guy is in a cushy medical center.

I mean, have you seen this place? It's got basketball courts, it's got a park. The inside looks pretty good. It's not a jail. This guy is not insane, Kevin.

KEVIN ROTHSTEIN, "BOSTON HERALD": He's -- no, he is not insane. He is in a federal medical center that also houses a program for sexual offenders. He's not in the hospital program where the insane and the physically ill go. But he is -- as you said, he's not in a penitentiary, and that's causing some people to take a second look, including senators Isakson and Kerry.

GRACE: Well, I don't understand how a guy -- first of all, what -- what is he convicted of?

ROTHSTEIN: He's serving a federal sentence for child pornography-related offenses. They are not abuse offenses, although he does have a sentence waiting for him when he finished his federal time on Pennsylvania charges of rape and incest. And that sentence will begin when he's released from Devons (ph).

GRACE: What I don't understand, why he is in a prison hospital and not a regular facility.

Do you know that, Kevin Rothstein?

ROTHSTEIN: Well, there's a lot of questions being raised about that right now. The...

GRACE: I've got a lot of questions about that myself. It's not as if this guy pled incompetency or insanity. He pled nolo -- nolo contendere. He didn't even have the guts to say "guilty."

ROTHSTEIN: He -- I think the reason that he is there is that the Federal Bureau of Prisons decided that there's where he belonged, in this federal sex offender management program.

GRACE: Kevin, how did he come to adopt Masha?

ROTHSTEIN: Well, there's -- I think it's safe to say there were a lot of checks that were supposed to stand in his way from -- that weren't checked. There's a lot of questions...

GRACE: Weren't checked? It's my understanding the adoption agency, Maureen Flatley, never even did another home study. They never came out to the home.

Don't you think they would notice there's only one bedroom and no mommy?

FLATLEY: Yes. We are really, really troubled by the content of the home study. It does appear that they went through some kind of superficial perfunctory process. It doesn't appear that they made any best effort to talk to his daughter.

GRACE: And what about the grown adopted sister?

FLATLEY: Exactly.

GRACE: Didn't -- wasn't she molested and never spoke up?

FLATLEY: Absolutely. And no one ever went to talk to her. It could have prevented the abuse.

(COMMERCIAL BREAK)

(BEGIN VIDEO CLIP)

UNIDENTIFIED FEMALE (voice-over): In 2003, an undercover agent posing as a young girl online was contacted by Mancuso to swap child porn. Pittsburgh agent Denise Holt (ph) and her partner tracked the Web address right to Mancuso's home. They secured a search warrant, and they went in.

UNIDENTIFIED FEMALE: Well, it was kind of surreal that day.

UNIDENTIFIED MALE: When we walked up to the door, approaching Mancuso and the child come walking from the backyard to us.

UNIDENTIFIED FEMALE: And right then, we both said to each other, you know, this is not good. We had to separate the two of them so that we could talk to him about why we were there, that we had a search warrant to, you know -- a search warrant to search his home. And we wanted to get her away from the scene so she was not traumatized.

UNIDENTIFIED FEMALE: Separated and safe, the little girl broke down.

UNIDENTIFIED FEMALE: To this day, we don't really know why she started talking to us that day, but maybe she just had enough. I don't know. But very short period after she sat down with the other female agent, she said, "I have a secret," and she just disclosed.

(END VIDEO CLIP)

GRACE: That little girl, adopted from a very obscure Russian orphanage at age 5 to a brand-new family in America, but to an American pedophile. For the next years of her life, age 5 to 10, she was sexually abused nearly every night, raped. And not only that, her abuser plastered the Internet with child porn.

But that's not the end of the story. Tonight, with us, this little girl who survived, Masha.

You know, Masha, when I hear that story about the detectives coming to the house, about child pornography, they didn't even know you were there. Do you remember the day they came?

MASHA, ADOPTIVE FATHER RAPED AND ABUSED HER: Yes.

GRACE: What happened?

MASHA: I got back from school, and we were just out on the back porch. And a car drove up. And we just thought it was just somebody that got the wrong address. So he went to talk to them, and they said they needed to talk to him.

And so an FBI agent came and talked to me. And she explained that they were there because of the pornography and that they didn't know that I was there. And so we went out on the front porch, and I just told her everything.

GRACE: Why did you -- that day, you hadn't told anybody at school, no teachers, no grown-ups, nobody. Why, that day, did you suddenly tell a lady, a stranger you didn't even know?

MASHA: I don't know. It just -- something inside me told me that that day was going to be the day that it all stopped and that I didn't have to hide it anymore.

GRACE: Did you feel like you were hiding something?

MASHA: Yes, I did.

GRACE: Why do you think you felt that way?

MASHA: Because I was, and I didn't tell anybody.

GRACE: Did you feel that you were doing something wrong?

MASHA: No. But, then again, I felt wrong that I didn't tell anybody.

GRACE: Why do you believe you didn't tell anyone?

MASHA: Because he threatened me. And I know that. And...

GRACE: When the two detectives came, the lady and the man, to your house, is it true that Mancuso, your adoptive father, was yelling out at you not to talk?

MASHA: Yes. We walked past the window, and he yelled out the window. He was like, "Masha, don't tell these people anything," and I just kept walking.

GRACE: Did you ever see him again?

MASHA: No, I didn't.

GRACE: Not in court?

MASHA: I saw him in court, yes.

GRACE: There's a shot we're showing right now of Matthew Mancuso in court. Are you afraid of him?

MASHA: Not anymore. I was, but...

GRACE: You know he's never going to get out?

MASHA: Yes. It just feels like he should be afraid of me now, not the other way around.

MASHA: Honey, I'm sure he is. I am sure he is.

Maureen -- before I go to Maureen, I want to go to a special lady with us tonight. It's Masha's new mom, her adoptive mother, who is herself a crime victim. Faith is with us.

You had to go through H-E-double-L to adopt this child. Tell us about it.



FAITH, MASHA'S NEW ADOPTIVE MOTHER: Well, I had caseworkers, a case manager from the foster care agency. They came out to my house three times a month. I had a caseworker once a month. A case manager twice a month came out to my house the entire time she was with me in foster care.

After that, they did a complete home study, looked through my house. Yes, they did a complete home study. They took a picture of Masha in her room at her bed.

GRACE: What I don't understand how he could waltz into some adoption agency, who, by the way, Elizabeth, called tonight, to try to speak to them. They would not come on the show.

Elizabeth, let me see the Liz-cam for a second. Isn't it true, when you called this adoption agency in Jersey, they said, "Oh, no, that's not us"? Right. Right. They are denying they had anything to do with Masha ending up for five years of her life, age 5, pre-K, with an American pedophile. "No, no, no. We didn't have anything to do with that." But you know, we know what happened.

Maureen Flatley, what did happen?

FLATLEY: Well, first of all, there's no federal regulation of adoption at all in the United States.

GRACE: Well, hold on. Wait, wait, wait, wait, wait. Right there. Senator Isakson, are you still with us?

SEN. JOHNNY ISAKSON (R), GEORGIA: I am.

GRACE: Senator, I'm so proud of you and Kerry pushing through Masha's Law and putting it out there. Now, I don't mean to push, but why is it that it is not a federal law that there has to be home studies? I mean, this child was adopted into a home to a single man who was divorced with a daughter he had molested, a grown daughter. They never even did a home study, Senator, nothing. The law does not require them to continue doing follow-ups. What can you do for us?

ISAKSON: Well, first of all, be proud of Masha. Masha has done a great service to children for years to come. She's brought about a terrible problem, brought it to light. She's courageous. Senator Kerry and I are carrying that torch, but she's the one that brought it forward.

You're correct. We are looking into the adoption issue because of the very thing that happened with Masha and, quite frankly, working with the Bureau of Prisons because of what's happened in the assignment of Mancuso to the Boston facility in Massachusetts.

So the tentacles of this case go far beyond Masha. But what happened to Masha was the most important thing for us to begin to try to find a way to rectify as best we could. That's what Senator Kerry's doing; that's what I'm doing.

GRACE: And, you know, another thing, Senator Isakson, is I can't even imagine how many couples, how many people wish that they had a baby, wish that they had a child like Masha that they could love. And this whole scandal jeopardizes American adoptions from other countries. Who wants to let an American adopt when they could be a pedophile?

ISAKSON: Well, that's why we need to find out where the bad actors are and get them out of the business, because they're hurting the people that do such a marvelous job all around this country, in terms of adoption.

GRACE: That video we were just showing you is a shot inside a Russian orphanage. There are thousands of children waiting to find a home.

Hey, Elizabeth, do you have shots of the children we were going to highlight tonight that need a home? Let's roll that for the viewers, if we could, before we go back to Masha. Thanks, dear.

This is Christopher, age 9, resident, Georgia. He loves movies. He loves music. He loves hamburgers, and he wants to be a dentist.

This is Shamone, age 3, out of California. The little thing likes to walk, run and ride his rocking horse.

Let's see the next one, Elizabeth. There you go.

Valentino is age 10. He likes music. Valentino has cerebral palsy, but he has not let it stop him from playing baseball.

Jorge, age 14, out of Pennsylvania. He loves horses and cats. He gets all A's and B's. And he loves the Dairy Queen.

Christine -- isn't she a beauty? -- 15, loves to talk on the phone.

(COMMERCIAL BREAK)

(BEGIN VIDEO CLIP)

UNIDENTIFIED FEMALE: He definitely is a monster. And just by the look on him in the courtroom, what I saw was a monster. And I hope that he stays in there. He cannot hurt no one ever again.

(END VIDEO CLIP)

GRACE: Welcome back, everybody. With us tonight, Masha, a child adopted to an American pedophile, who lived through years of abuse. The important part is she lived, as she has brought her attacker to justice, her own adopted father.

I want to go back to her new mom, her new adoptive mom. They're out of the Georgia jurisdiction now. Faith is with us.

Faith, it's amazing to me that you got this girl and that you, too, are a crime victim. What happened?

FAITH: Well, when I was like 4 or 5 years old, my stepdad started molesting me. And then, when I got older, my mom and dad got divorced when I was like 10. Then she had boyfriends, and they started abusing me and my sister. And my mom actually knew about it and allowed it to happen.

GRACE: That must have left you with an incredible feeling of helplessness, that no one helped you, but now you can help her. And I've learned, as a crime victim myself, that knowing that somebody else has been through the same ordeal, and they survived, and they triumphed, that helps me. And I know that you're doing this for Masha.

Now, she saw him in court, right?

FAITH: Yes.

GRACE: What happened?

FAITH: When he came into court, she wanted to see him, because she wanted to see him walk in, in the shackles around his feet and the handcuffs on his hands. So I allowed her to do that. And when he walked in, she saw him and she actually laughed at him as he walked in the courtroom in these shackles and chains. And, I, you know, let her know that it was OK to do that.

GRACE: You know, so many child molestation victims that I have talked to -- let's go to Dr. Patricia Saunders, clinically psychologist -- it's just not only the molestation that haunts them as they grow up; it's the feeling that nobody did anything.

DR. PATRICIA SAUNDERS, CLINICAL PSYCHOLOGIST: And that nobody would listen, if they did speak out. No, I think Masha's kind of unusual, Nancy. And I don't want our viewers to think that all children who are molested at a very young age and continuously molested over years are as well put-together as Masha appears.

She's -- well, she's one of my new heroes tonight. But this new lady has a kind of resilience that's rare, and I would guess that Faith, her mom, has it, too. And it's really very special to see them helping each other.

GRACE: You know, it is rare, Doctor, because so many molestation victims that I see, as they grow up, they can't function anywhere than the level that Masha is now, still as a child.

Also joining us, James Marsh. This is Masha's attorney. James...

JAMES MARSH, MASHA'S ATTORNEY: Hi, Nancy.

GRACE: Hi, friend. What are we going to do about this adoption agency that helped facilitate Masha coming from Russia, straight into the hands of an American pedophile?

MARSH: Well, I guess, unfortunately, or fortunately for Masha, we have a lot of potential defendants in this case, because it wasn't just one adoption agency that helped facilitate this. There were many cooperating agencies involved. This was the agency that did the home study. There's the agency that...

GRACE: Or the lack thereof.

MARSH: Or the lack thereof, what I called the promotional piece for Mr. Mancuso.

GRACE: Any idiot could see there was one bedroom and one father and no mom.

MARSH: Well, I think what we've seen in this case is that -- you know, we talked to law enforcement. And what really led to Masha's rescue was a gut feeling that something was wrong here. And what we didn't have in the adoption context was any gut feeling...

(CROSSTALK)

GRACE: Are you suing? Are you suing?

MARSH: We are suing, absolutely.

GRACE: Who are you suing?

MARSH: We are suing the agency that did the home study. And we're still trying to sort out which agency was responsible for the placement. We have two names. They're pointing the fingers at each other.

GRACE: That's right.

MARSH: And we're going to get to the bottom of this for Masha.

GRACE: You know, Elizabeth, do you have the application we found that Mancuso made for her where it cites what kind of child he would like to bring home? If you could put that up, and highlight the part I want to show the viewers that we talked about.

Maureen Flatley is an advocate for children. What I don't understand is how, in this country, children like Masha can be adopted with basically no home study.

There we go. Mancuso wants a child, a girl, between 5 and 6, Caucasian. He is willing to consider a child with minor disabilities. I detect a child diagnosed with learning disabilities.

Now, what does that say to you? Why was this allowed?

FLATLEY: Well, again, there's no federal regulation of adoption of any kind. And worse yet, there are very different standards to adopt an American foster child. Fortunately for Masha, ironically, she entered the American foster care system, which actually has the highest standards for adoption, which is why Faith's home study was so much tougher.

But if you're adopting from a foreign country, the standards are extraordinarily low, really almost non-existent, in some cases, state to state. So we really believe strongly that we have to develop a single national standard to protect children wherever they come from.

GRACE: Back to Kevin Rothstein with "The Boston Herald," Kevin Rothstein, again, Mancuso behind bars tonight, not in a maximum facility prison where he belongs. He's in a cushy mental health facility. Tell me, what kind of privileges does he have there at Devens Prison Hospital?

ROTHSTEIN: Well, what he doesn't have are those restrictions and the top security of a federal penitentiary. We know there's a recreational facility, facilities that he can use there, although...

GRACE: Like what?

ROTHSTEIN: Not quite clear right now...

GRACE: Track, basketball court, baseball, soccer, treadmills -- treadmills? Treadmills! And board games. Board games? This guy has a recreational facility.

When you hear that, Masha, if you could speak out to him tonight, what would you tell him?

MASHA: He doesn't belong there. Whoever put him there or how he got there is wrong. And while I'm sitting here having nightmares and still suffering even after he's gone, he's sitting there playing games and comfortable? That's not right.

GRACE: Senator Isakson, I hope you can hear us.

ISAKSON: I can.

GRACE: We'll all be right back.

(COMMERCIAL BREAK)

(BEGIN VIDEO CLIP)

MASHA: There are people that can help them. And they should tell somebody, even if they are afraid to talk about it. The sooner they tell someone, the sooner it will get better. And they should have courage and be strong about it, because it's not going to last forever.

(END VIDEO CLIP)

GRACE: This is the first birthday party that Masha ever had. Sitting here on the set in the break, she told me that her adoptive father molested her on Christmas Day. She was adopted by him. She lived with him ages 5 to 10.

To Detective McGarry, what are you doing to make sure this does not happen to other children?

MCGARRY: We're going through every picture that we come across -- we literally seize millions of images. We're trying our best to go through every single one of them and glean every clue we can.

GRACE: And you need an army for that, Detective. But I've got to tell you, everybody, if you don't believe heroes exist, take a look at Detective Constable Bill McGarry. We have flown him in from Canada for working tirelessly to help solve this case.

But the real star in my mind is this child who survived.

Sweetie, if you could speak out to children tonight, what would you tell them?

MASHA: To not be afraid to tell somebody, because there are people you could go to and trust. And eventually, it will get better and stop. But people shouldn't be afraid to talk about it.

GRACE: And you're happy now with your new mom?

MASHA: Very.

GRACE: Thank you.

I want to thank all of my guests and to this child, Masha, for giving other children a voice and courage to speak out. But our biggest thank you is to you for inviting us and Masha and her story into your home. I'm Nancy Grace signing off for tonight. I'll see you right here tomorrow night, 8:00 sharp Eastern. Until then, good night, friend.



Copyright 2005 American Broadcasting Companies, Inc.  
ABC News Transcripts

SHOW: Primetime Live 10:04 PM EST ABC

December 1, 2005 Thursday

**LENGTH:** 4022 words

**HEADLINE:** MASHA'S CASE;  
PEDOPHILE ADOPTS RUSSIAN ORPHAN

**ANCHORS:** JOHN QUINONES

**BODY:**

CORLOC

TOPIC: CHILD PORNOGRAPHY

CONTENT: NAAMBLA

JOHN QUINONES (ABC NEWS)

(Off-camera) Good evening. Welcome to "Primetime." I'm John Quiñones. Somewhere a nameless little girl is being forced to pose for thousands of strangers on the internet. Who's taking those explicit pictures? As our mystery continues, somebody has to know who that little girl is and how she got there.

JOHN QUINONES (ABC NEWS)

(Voiceover) Her name is Masha and her journey to hell and back begins at the age of four. Here in the small industrial city in the south of Russia where coal mining was once king but where unemployment and alcoholism now rule. Masha doesn't remember her father. Her mother told her he was dead. But then again Masha says her mother seemed to live much of her life in a bottle.

JOHN QUINONES (ABC NEWS)

(Off-camera) Did she hit you or abuse you?

MASHA (ABUSE VICTIM)

She stabbed me.

JOHN QUINONES (ABC NEWS)

(Off-camera) Stabbed you?

MASHA (ABUSE VICTIM)

She got mad at me and she was drunk. She stabbed me in the back of my neck.

JOHN QUINONES (ABC NEWS)

(Voiceover) So Russian police came to the rescue, and it would be one of the last times Masha would ever see her mother.

MASHA (ABUSE VICTIM)

She said goodbye or whatever. So I was like, okay. I didn't know what was going on.

JOHN QUINONES (ABC NEWS)

(Off-camera) You must have been scared.

MASHA (ABUSE VICTIM)

I was scared and confused, yeah.

JOHN QUINONES (ABC NEWS)

(Voiceover) They brought Marsha here, to orphanage number one, where many children from troubled homes live in refuge. She would be among the nearly 700,000 Russian kids who live in state-run homes, more than any other country in the world. Masha is only 4 years old.

MASHA (ABUSE VICTIM)

I didn't really know anybody, and I remember I had to keep my stuff under my pillow or people would come and steal it.

JOHN QUINONES (ABC NEWS)

(Off-camera) All your belongings under a pillow?

MASHA (ABUSE VICTIM)

I didn't have that many belongings.

JOHN QUINONES (ABC NEWS)

(Voiceover) In Russia, very few families adopt orphans. So Marsha was destined to live here until she turned 18. Her mother visited now and then and kept promising that when the leaves turned green, she would come back for Masha. But the seasons changed. The little girl turned 5, and her mother never



returned. And then one day...

**MASHA (ABUSE VICTIM)**

They were saying the names of some kids that were going to be adopted. And they said my name. And I was like, okay.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) So when you heard that you might be adopted, what went through your mind?

**MASHA (ABUSE VICTIM)**

They were saying that someone was going to come and get me. And I was like, at first I thought it would be one of my family members, but then I found out it wasn't.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) The person coming to adopt Masha was Matthew Mancuso, a divorced 41-year-old engineer from the US. At first, he seemed like a little orphan's dream come true. The international adoption went smoothly, arranged by this woman, Jeanine Smith, who now runs an adoption agency in Cherry Hill, New Jersey. Mancuso paid her thousands of dollars.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) When Matthew Mancuso contacted Smith here at her home office, he told her he was looking to adopt a 5 to 6-year-old Caucasian girl. They sent him a videotape, and he specifically picked Masha.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) In a letter to the agency, Mancuso wrote, "after months of preparation and what seemed like a mountain of paperwork, it was finally time for me to go to Russia and meet my new daughter. Yippee. And not a moment too soon. I practically wore out the VHS tape of her from watching it so many times."

**JOHN QUINONES (ABC NEWS)**

(Off-camera) Did he seem like a nice man?

**MASHA (ABUSE VICTIM)**

Yeah, he was there. And, like, he'd bring candy and stuff.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) And yet there was something missing.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) Did you wonder why there wouldn't be a mother, a wife of his?

**MASHA (ABUSE VICTIM)**

I did. I think I remember asking him if I was going to get a mother, and he just - he'd say that he wasn't married and that he didn't think I would. So I was like, okay.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) The adoption was finalized. And on the long transcontinental flight from Moscow to New York, Masha slept peacefully, far away from everything she had ever known. But she was leaving more than her orphanage. Masha was leaving her childhood behind as well.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) This would be Masha's home in the US, a modest ranch-style house in a middle-class neighborhood on the outskirts of Pittsburgh. Ordinary in many ways, but to a little Russian orphan, it must have seemed like a mansion, a palace that quickly turned into a house of horrors the very first night Marsha slept here.

**MASHA (ABUSE VICTIM)**

People in the orphanage say that I was going to get my own room, my own bed. And when I didn't, I was like, hmm, there wasn't a bedroom for me.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) So then it's time to go to bed and he says what?

**MASHA (ABUSE VICTIM)**

He told me sleep with him. I was kind of nervous, and I thought it was kind of weird.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) Remember, this was a 5-year-old girl who spoke no English, alone in this strange house in a new country. The only person she knew was now her captor.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) What did he do?

**MASHA (ABUSE VICTIM)**

He touched my leg or something or he touched my chest like a couple nights after that. He'd started touching my private parts.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) He didn't have clothes on himself?

MASHA (ABUSE VICTIM)

Uh-uh.

JOHN QUINONES (ABC NEWS)

(Off-camera) And you knew this didn't feel right, of course.

MASHA (ABUSE VICTIM)

Yeah, I knew it was wrong. No, I tried to tell him stop or whatever, but he wouldn't usually listen to me. So just wait till it was over.

JOHN QUINONES (ABC NEWS)

(Voiceover) We interviewed Marsha, now 13, in the presence of her new adoptive mother, her therapist, and an adviser, all of whom hope that airing this little girl's story might help her heal. And there is so much healing to be done, because back in Pittsburgh, just a few days went by before Mancuso started raping her repeatedly.

MASHA (ABUSE VICTIM)

I'd make myself think of other things when it was happening, but it always came back to me. Couldn't stop it.

JOHN QUINONES (ABC NEWS)

(Voiceover) Not only that, Mancuso then starts taking sexually explicit pictures of her.

JOHN QUINONES (ABC NEWS)

(Off-camera) How did he explain it?

MASHA (ABUSE VICTIM)

He just said he wanted my pictures. He just said that I was pretty and stuff like that. So he'd just take them. Like he tried to bribe me sometimes. He'll say, if you let me take your picture, I'll buy you something.

JOHN QUINONES (ABC NEWS)

(Voiceover) Mancuso used rewards and threats to keep her silent so that she wouldn't tell her teachers and classmates after she was enrolled in school.

MASHA (ABUSE VICTIM)

He wouldn't tell me what it would be, but he'd just say something bad would happen. So I just didn't tell anybody because I was afraid.

JOHN QUINONES (ABC NEWS)

(Voiceover) By now, Mancuso was starving her to keep her from reaching puberty, but she told no one.

MASHA (ABUSE VICTIM)

And now I regret not telling anyone sooner, but I guess I really couldn't.

JOHN QUINONES (ABC NEWS)

(Off-camera) You were too scared to tell anyone.

MASHA (ABUSE VICTIM)

Mm-hmm.

JOHN QUINONES (ABC NEWS)

(Off-camera) And he threatened you.

MASHA (ABUSE VICTIM)

Yes, he did.

COMMERCIAL BREAK

ANNOUNCER

"Primetime." Here again John Quiñones.

JOHN QUINONES (ABC NEWS)

(Voiceover) Our investigation into a sexually exploited little girl named Masha takes us south of Chicago, where most days you'll find sergeant Mike Siglifa running a patrol shift for the Palos Heights police department. But somewhere toward the end of a long career in law enforcement, Sergeant Siglifa is startled by a crime that sickens him. Internet child pornography.

SERGEANT MIKE SIGLIFA (PALOS HEIGHTS POLICE)

Other than murder, I would say it's the most horrendous crime there is.

JOHN QUINONES (ABC NEWS)

(Voiceover) He joins a child exploitation task force and poses as a pedophile calling himself "billyboy7," and he enters the dark world of internet pornography, where obscene pictures of children

are traded like baseball cards. Believe it or not, there is a limited supply of child porn. So pedophiles are always looking for arousing new images. Masha's pictures, which were fresh and updated regularly, caused a feeding frenzy. Sergeant siglifa pretended to want them, too, leading to a chat-room conversation he'll never forget.

SERGEANT MIKE SIGLIFA (PALOS HEIGHTS POLICE)

He was wanting to trade pictures or videos of girls 8 to 12 years old engaged in sexual acts.

JOHN QUINONES (ABC NEWS)

(Voiceover) The person on the other end of his computer chat room goes by the name of 'nkdsister."

SERGEANT MIKE SIGLIFA (PALOS HEIGHTS POLICE)

I knew he had been around this block before. He knew all names of pictures that law enforcement has seen time and time again on the internet. He was well versed in child sex abuse images.

JOHN QUINONES (ABC NEWS)

(Off-camera) This is a text of some of the email conversations you had with him, most of it we can't even say on the air. But he did want full female body pictorials, he said.

SERGEANT MIKE SIGLIFA (PALOS HEIGHTS POLICE)

Yes.

JOHN QUINONES (ABC NEWS)

(Off-camera) Engaged in sexual acts. You knew he was serious.

SERGEANT MIKE SIGLIFA (PALOS HEIGHTS POLICE)

Yes.

JOHN QUINONES (ABC NEWS)

(Voiceover) His gut tells him to pursue this man.

SERGEANT MIKE SIGLIFA (PALOS HEIGHTS POLICE)

I just felt that there was something more.

JOHN QUINONES (ABC NEWS)

(Voiceover) So he traced 'nkdsisters'" internet address to Pittsburgh, Pennsylvania, and then contacted the FBI. May 27, 2003. At this lonely ranch house tucked away in the woods outside Pittsburgh...

DENISE HOLTZ (FEDERAL BUREAU INVESTIGATION)

It was around 4:15 in the afternoon that we arrived to execute the search warrant.

JOHN QUINONES (ABC NEWS)

(Voiceover) Armed only with information provided by Sergeant Siglifa, Federal agents Denise Holtz and Tom Clinton showed up at Mancuso's door looking for those photos he was advertising on the internet. But neither of them could have anticipated what they would find. There was a suspected pedophile but he was not alone.

JOHN QUINONES (ABC NEWS)

(Off-camera) He was with the little girl?

DENISE HOLTZ (FEDERAL BUREAU INVESTIGATION)

They were together. They had been in the back. We could see them when we pulled up, we could see them back there sitting on a pick picnic table.

JOHN QUINONES (ABC NEWS)

(Off-camera) You must have been blown away.

DENISE HOLTZ (FEDERAL BUREAU INVESTIGATION)

We looked at each other and we said, this is not good.

JOHN QUINONES (ABC NEWS)

(Voiceover) They leave Masha on the front porch with another FBI agent and take Mancuso inside.

TOM CLINTON (FEDERAL BUREAU INVESTIGATION)

He wasn't happy we were there. It was obvious to us that he wasn't. He looked concerned.

JOHN QUINONES (ABC NEWS)

(Voiceover) They find computer disks with child pornography. But the biggest discovery isn't the physical evidence of a crime, it's what they hear from the little girl sitting on this porch swing.

DENISE HOLTZ (FEDERAL BUREAU INVESTIGATION)

The little girl said, "is this about my secret?"

JOHN QUINONES (ABC NEWS)

(Voiceover) The secret that Masha had been hiding for five long years out of fear of her adopted father. In fact, even on the day of his arrest, Mancuso, who no longer lives here, tried to keep control of Masha by yelling at her from inside the house.

**MASHA (ABUSE VICTIM)**

"Masha don't tell these people anything I told you or anything I did." But I did anyways. Because it was like, I finally had someone to talk to. So once I said something, I said everything else. It just all came out.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) Finally, she's rescued at the age of 10.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) If they hadn't have caught him, where would you be right now?

**MASHA (ABUSE VICTIM)**

I don't know. I guess I'd still be waiting like I did for five years, waiting for someone to find me.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) Masha was not the only one waiting and keeping a terrible secret about Matthew Mancuso. Rochelle is his biological daughter, now 28 years old. She's asked us not to show her face. Her mother, Dourine McDade, is Mancuso's ex-wife.

**DOURINE MCDADE (EX-WIFE)**

We heard he adopted and I was angered. He had a biological daughter already that he paid no intention to, was not in contact with. Why do you want to adopt another little girl? You already have one.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) When you heard he was adopting, what went through your mind?

**ROCHELLE (DAUGHTER)**

I was very scared for the little girl after I found out it was a girl. I knew deep down inside why he probably had her.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) You knew.

**ROCHELLE (DAUGHTER)**

I had a gut feeling.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) As unbelievable as it sounds, Rochelle says **Masha** was not the only abused child. For five years, Matthew Mancuso, her biological father, molested her. Her mother is hearing much of this for the very first time.

JOHN QUINONES (ABC NEWS)

(Off-camera) How often would it happen?

ROCHELLE (DAUGHTER)

I know I remember my mother going out with her friends Friday nights. It would definitely happen every Friday night.

DOURINE MCDADE (EX-WIFE)

I'm sorry, honey.

ROCHELLE (DAUGHTER)

I know. Just whenever he had the opportunity was when it would happen. Anytime my mother wasn't around, he would take that as an opportunity. You know, after my mom and dad got separated and divorced, weekend visitations was free game then because there was nobody else there. And I know it hurts her to hear that, and that's why I really never said anything because I didn't want to hurt anybody.

DOURINE MCDADE (EX-WIFE)

Oh, honey, you're not hurting me. I'm hurting for you.

JOHN QUINONES (ABC NEWS)

(Off-camera) How hard is it for you to talk about it?

ROCHELLE (DAUGHTER)

I avoid it as much as possible because I feel so much guilt for what happened. When I first found out that he adopted a little girl, I should have spoke up. I should have said something. I feel somehow responsible.

ANNOUNCER

When "Primetime" returns, how could this have happened? A little girl handed over to a child molester.

JOHN QUINONES (ABC NEWS)

(Off-camera) Anyone would find this shocking. A 41-year-old pedophile goes to Russia and he buys himself a sex slave.



ANNOUNCER

Next.

COMMERCIAL BREAK

ANNOUNCER

"Primetime." Once again, John Quiñones.

JOHN QUINONES (ABC NEWS)

(Voiceover) For many years long before he molested Masha, Matthew Mancuso's biological daughter says he molested her, too.

ROCHELLE (DAUGHTER)

He was like a monster. For him to do this to me and then go and do it to another girl after that, I think that does categorize him as a monster.

JOHN QUINONES (ABC NEWS)

(Voiceover) If anyone involved in the adoption process had asked the most basic questions, they could have easily determined that Mancuso was a pedophile.

JOHN QUINONES (ABC NEWS)

(Off-camera) Anyone write you guys letters to verify anything?

DOURINE MCDADE (EX-WIFE)

Nothing.

JOHN QUINONES (ABC NEWS)

(Off-camera) A phone call?

DOURINE MCDADE (EX-WIFE)

No phone call.

JOHN QUINONES (ABC NEWS)

(Off-camera) Anyone visit your house?

DOURINE MCDADE (EX-WIFE)

No.

JOHN QUINONES (ABC NEWS)

(Off-camera) No one interviewed you about his adoption.

DOURINE MCDADE (EX-WIFE)

No.

JOHN QUINONES (ABC NEWS)

(Voiceover) Experts say those calls should have been made. It's all part of what is normally an extensive background check done on anyone planning to adopt. But in Masha's case, the New Jersey agency relied on a home study prepared by a Pittsburgh social worker who made none of those calls. Instead, the study reads flatly, "Mr. Mancuso is very capable, willing, and well-prepared to provide a stable and loving home."

MAUREEN FLATLY (LOBBYIST)

Well, I think it's fair to say that it was a fairly perfunctory process.

JOHN QUINONES (ABC NEWS)

(Voiceover) Maureen Flatly is a lobbyist who specializes in adoption and child welfare. She got involved in Masha's case in a desperate effort to find out how a pedophile could have adopted a 5-year-old little girl.

MAUREEN FLATLY (LOBBYIST)

It doesn't appear that they talked to anybody about Mancuso. That they simply took what Mancuso said to them at face value and placed the child with him.

JOHN QUINONES (ABC NEWS)

(Voiceover) Tom Atwood is president of the National Council on Adoption.

JOHN QUINONES (ABC NEWS)

(Off-camera) Did you get to see the home study that was performed?

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

I did.

JOHN QUINONES (ABC NEWS)

(Off-camera) What do you think of it?

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

The home study is fairly typical.

JOHN QUINONES (ABC NEWS)

(Off-camera) Typical?

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

Yes. It's a - I don't see anything in there that stands out as a giveaway that such a problem like this would occur.

JOHN QUINONES (ABC NEWS)

(Off-camera) Mr. Atwood, anyone would find this shocking. A 41-year-old pedophile goes to Russia and he buys himself a sex slave.

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

Well, he was not known to be a pedophile at the time.

JOHN QUINONES (ABC NEWS)

(Off-camera) But if proper investigation had been done, his own...

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

(Off-camera) What do you think would have been found? I mean, the...

JOHN QUINONES (ABC NEWS)

(Off-camera) They could have spoken to...

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

There was a criminal - again, I'm not here to defend this adoption, okay. Obviously something went wrong, clearly.

JOHN QUINONES (ABC NEWS)

(Voiceover) What troubles adoption experts is that, according to **Masha**, there were no home visits after she was adopted. It's common practice, and just one visit, experts say, should have turned up some disturbing problems like, where was **Masha's** bedroom?

MAUREEN FLATLY (LOBBYIST)

The adoption agency that was responsible for making the placement appears never to have supervised the placement once the child went to his home. Which is incredible. It's inappropriate by any standards.

JOHN QUINONES (ABC NEWS)

(Off-camera) They turned their back on this little girl.

MAUREEN FLATLY (LOBBYIST)

Right. They sold her to a complete stranger. And let her - and let her go.

JOHN QUINONES (ABC NEWS)

(Off-camera) Little Masha told us 'no one ever called, no one ever came to see me. I was all alone.'

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

If there were no visits from the social workers, then they were not following the rules, and they're letting her down.

JOHN QUINONES (ABC NEWS)

(Voiceover) But those rules are murky at best. While post-placement supervision is required in Pennsylvania for domestic adoptions, no such law exists for international placement. And yet there have been more than half a billion American dollars spent on Russian adoption since the fall of the Soviet Union. Because of that, adoption experts say there should be more regulation at every stage of the process.

MAUREEN FLATLY (LOBBYIST)

The policy seems to be, if the check clears, the kid is yours. There's very little indication that any significant number of people are turned away from this process.

JOHN QUINONES (ABC NEWS)

(Off-camera) When you wave a \$15,000 to \$20,000 check in the face of an adoption agency, there's very little incentive then to kill the deal, isn't there?

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

That question mischaracterizes the motives of people involved in...

JOHN QUINONES (ABC NEWS)

(Off-camera) That's what this man paid for this little girl.

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

People do not provide adoption service for money. They are motivated by desiring to help children have families.

JOHN QUINONES (ABC NEWS)

(Off-camera) So these adoption agencies throughout the country, you can sit here and tell me that all of them - none of them are doing it for the money?

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

What I can tell you is that the professional adoption agencies who provide services to children, the service of adoption placements, are motivated by a desire to benefit children.

JOHN QUINONES (ABC NEWS)

(Off-camera) Jeanine Smith, the woman who arranged the adoption here in New Jersey, would not talk to us on camera about the post-placement supervision or anything else about the adoption citing New Jersey law, which she says constrains her.

JOHN QUINONES (ABC NEWS)

(Voiceover) In fact, when we showed up at her agency this week to ask her about **Masha**, she instructed our camera crew to stay off her property and called the police. She also issued a statement emailed to "Primetime." "The unearthing of this horrific experience has further strengthened our resolve to advocate for policy and law enforcement tools to help prevent applicants with criminal motives from becoming adoptive parents in the future." For his part, Tom Atwood insists that post-placement reform requiring visits and reports starting at one month and then again at three months will go a long way to make sure this kind of thing will never happen again.

TOM ATWOOD (NATIONAL COUNCIL ON ADOPTION)

The adoption community in the United States is outraged and heartbroken over this case, **Masha's** case. We can and are doing things about it. I want your viewers to know that international adoption is a beautiful thing. The face of international adoption is 49,000 children adopted from Russia since 1992, living happy, healthy lives in America. And these tragic, deplorable incidents should never happen. But it would be even more tragic if we were to shut down adoptions in - as a result of them.

JOHN QUINONES (ABC NEWS)

(Voiceover) Two weeks ago, Matthew Alan **Mancuso** crumbled in the face of multi-count criminal indictments, pleading guilty as charged.

REPORTER (FEMALE)

Do you have any remorse? Is there anything you want to say to her? Anything?

**MASHA** (ABUSE VICTIM)

He never apologized to me. Never.

JOHN QUINONES (ABC NEWS)

(Off-camera) How long should he stay in prison?

**MASHA (ABUSE VICTIM)**

For the rest of his life.

**ROCHELLE (DAUGHTER)**

And not some kind of easy country club-like jail.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) But you know what they say happens to child molesters in jail.

**ROCHELLE (DAUGHTER)**

I don't care. I think he would deserve it. Let him get what is due to him for doing what he did to us.

**JOHN QUINONES (ABC NEWS)**

(Voiceover) **Mancuso** has been sentenced to a minimum 35 years in prison. This on top of 15 years on the Federal charges. And prosecutors from the state of Florida have announced they, too, will try him for crimes they say he committed against **Masha** at Disney World. In a sense, **Mancuso** continues to victimize **Masha**. Those pictures he took of her are still out there in pedophile cyberspace and can never be retrieved. But **Masha** is bravely putting all that behind her. Now 13, she lives in a quiet suburb of another American city with her new adoptive mother. Living out the childhood that was stolen from her and dreaming big dreams. Someday she says she'd like to return to her homeland and devote her life to helping other Russian orphans.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) As hard as it is, **Masha**, why do you speak up?

**MASHA (ABUSE VICTIM)**

Because I think that it's wrong what he did. Some kids just give up and they don't have any faith. And a lot of the times nobody ever tells anybody, even if they are afraid to tell somebody, no matter what they think is gonna happen, it's gonna be for the better, because if they tell somebody, it's gonna change.

**JOHN QUINONES (ABC NEWS)**

(Off-camera) It does get better. It did for you.

**MASHA (ABUSE VICTIM)**

Yes.

**ANNOUNCER**

Next, would you ride what train insiders call a coffin car? Where is it, what it is and why did our cameras get shut down when we just asked about it.

CHRIS CUOMO (ABC NEWS)

(Off-camera) Isn't that ironic that you're worried about security in the unsafe car?

ANNOUNCER

When "Primetime" returns.

COMMERCIAL BREAK

ANNOUNCER

Next, video that could make you change seats on your next train ride to work. "Primetime" continues after this from our ABC stations.

COMMERCIAL BREAK

ANNOUNCER

"Primetime." Now Chris Cuomo.

**LOAD-DATE:** December 2, 2005

---

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI  
EASTERN DIVISION

**FILED**  
AUG 16 2001

UNITED STATES OF AMERICA, )  
 )  
Plaintiff, )  
 )  
v. )  
 )  
ALOIS LARRY WOLK, JR., )  
 )  
Defendant. )

U. S. DISTRICT COURT  
E. DISTRICT OF MO.

No. 4:01 CR 258 SNL  
DDN

**ORDER AND RECOMMENDATION  
OF UNITED STATES MAGISTRATE JUDGE**

This action is before the Court upon the pretrial motions of the parties which were referred to the undersigned United States Magistrate Judge pursuant to 28 U.S.C. § 636(b). An evidentiary hearing was held on August 2, 2001. Defendant ordered a transcript of the evidentiary hearing and the parties filed post-hearing memoranda.

**1. Motion in limine.**

Defendant Alois Larry Wolk, Jr., has moved in limine to preclude introduction of irrelevant, prejudicial, inadmissible evidence, prosecutorial misconduct, and improper prosecutorial comment (Doc. No. 13). This motion is premature. It asserts an objection to an expected offer of evidence at trial, which evidence may not be offered at trial. The undersigned will deny the motion without prejudice to defendant reasserting it at trial for consideration by the district judge in the context of the trial evidence.

**2. Motion to dismiss.**

Defendant has moved to dismiss (Doc. No. 14) upon three grounds. First, defendant alleges that certain described

34



constitutional rights were violated. At the hearing on this matter, defendant offered no evidence or argument to support his allegations. Second and third, respectively, he argues that, if the court sustains his motions to quash the search warrant and to suppress evidence, the government would be left without legally sufficient evidence to sustain a guilty verdict at trial. These arguments are best deferred to the district judge for ruling at trial.

### 3. Suppression issues.

The government has moved for a pretrial determination of admissibility pursuant to 18 U.S.C. § 3501 (Doc. No. 11). Defendant Wolk has moved to suppress evidence and statements (Doc. No. 15) and to quash the search warrant and to suppress evidence (Doc. No. 18).

From the evidence adduced at the hearing, the undersigned makes the following findings of fact and conclusions of law:

#### FACTS

1. On November 9, 2000, Federal Bureau of Investigation Special Agent Gerald Bell applied for and received a search warrant from Magistrate Judge Lawrence O. Davis for the residence at 6 Shadow Lane, St. Peters, Missouri, and for computers and computer media found therein. Gov. Exhs. 1 and 2. The affidavit submitted to Judge Davis by Agent Bell recounted the investigation conducted by Palos Heights, Illinois, Police Sergeant Michael Zaglifa. The affidavit stated that on September 22, 2000, Sgt. Zaglifa participated in an undercover investigation on the Internet using his police computer. In this investigation he posed as a 13-year-old girl from Chicago under the name of "Ashley\_S13" (Ashley) and entered an electronic chat room. In that capacity he was invited into a file server of someone who identified himself as "^fish-^"

(Fish) using Internet Protocol address 204.184.55.3. "Fish" instructed "Ashley" how to access the graphic image files in his file server and "Ashley" downloaded photographs of late teenage girls and photographs of child pornography. The Internet connection session was interrupted and reestablished with "Fish" assigned to Internet Protocol (IP) address 204.184.55.66. Further investigation by Sgt. Zaglifia determined that "Fish" was using the Internet access provider Westplex Information Network (Westplex) in St. Peters, Missouri. The officer then contacted Danny Hughes, the Westplex System Administrator, who ultimately determined and advised that the Internet access account with which Sgt. Zaglifia communicated on September 22, 2000, belonged to a Larry A. Wolk at 6 Shadow Lane, St. Peters, Missouri. The affidavit submitted by Agent Bell further described expert technical automation opinions which established the need to access the computer facilities at 6 Shadow Lane in a secure fashion to seize evidence of the illegal transmission of the child pornography which was observed by Sgt. Zaglifia. The affidavit also stated that the records of the Missouri Department of Revenue were reviewed and listed two motor vehicles registered to Larry A. and Melynna L. Wolk at 6 Shadow Lane. The search warrant affidavit and the search warrant itself described the place to be searched as the residence at 6 Shadow Lane, St. Peters, Missouri, 63376, and the computers and computer media found in the residence. A two-page attachment to the warrant and the affidavit specifically described the items sought. After considering the affidavit, at 2:10 p.m. on November 9, 2000, Judge Davis issued his search warrant.

2. On November 16, 2000, the search warrant was executed at 6 Shadow Lane by seven law enforcement personnel. Federal law enforcement personnel, led by Special Agent Bell, took the leading roles in executing the warrant. Also participating in the search activity were F.B.I. Special Agents Michael R. Johnson and Scott

Skinner, Postal Inspector Dale Roberts, St. Peters Police Lt. Brad North, Police Det. Todd Roth, and Officer Malawy (the only officer in uniform). At approximately 9:30 a.m., the officers arrived at the residence in several government vehicles, one of which was a marked police car. The officers first knocked on the front door of the residence. Melynna Wolk answered the door. The officers identified themselves and stated that they were there to execute a search warrant for child pornography. Mrs. Wolk allowed the officers to enter the residence without objection. Although none of the officers had a weapon drawn, she could see that they were armed.

3. All of the officers entered defendant's two-story residence. Mrs. Wolk was the only person at home. The officers first made a cursory observation of each room in the house for the officers' safety. Nothing was found that appeared to risk the officers' safety.

4. The officers asked about the location of defendant. Mrs. Wolk said her husband was at an employment training session. Because she believed he should be there with her, at 9:40 a.m. she attempted to call his pager. She did so by going into the kitchen and using the telephone there. Her husband, later identified as defendant Alois Larry Wolk, did not respond to her several calls. At 9:45 a.m. the officers began to execute the warrant. At this time, Agent Bell asked Mrs. Wolk where exactly her husband was; the officers wanted to advise him of the search warrant execution. She said he was at a training seminar given by H & R Block at a location not far from the house. Lt. North and Postal Inspector Roberts left the residence to locate defendant.

5. After making the telephone calls, Mrs. Wolk remained in the kitchen-dining room area of the home with Police Officer Malawy. There they conversed on topics that included her craft work. Mrs. Wolk also was asked where the computers in the home

were located. She gave the agents this information. Agent Skinner went through the home and located and inspected the several computers there.

6. Lt. North and Inspector Roberts drove approximately one mile to the H & R Block facility in an unmarked vehicle. The officers entered the H & R Block office and saw several people seated around a table. Lt. North asked whether Mr. Wolk was there. When defendant identified himself, Lt. North asked him whether they could speak with him. Defendant agreed to accompany the officers outside. Outside the office the officers introduced and identified themselves with their badges and told him that the F.B.I. was at his home to execute a search warrant and that his wife asked that he come home. The officers told defendant that he was free to return home, if he wanted, and that, if he decided to go home, they would meet him there. Defendant decided to do so and drove home by himself in his own vehicle. The officers also returned to 6 Shadow Lane in their own vehicle.

7. Defendant arrived at 6 Shadow Lane at approximately 10:10 a.m., shortly thereafter followed by Lt. North and Inspector Roberts. Defendant entered the house and identified himself to Agent Bell. He was directed into the living room. There Agent Bell introduced himself and explained that the law enforcement officials were there to execute a search warrant regarding the distribution of child pornography. Defendant was then told that the officers would like to interview him, that any statement by him would have to be voluntary, that he was free to leave at any time, that he was not obligated to talk to the officers, and that he was not under arrest. Defendant responded by saying he was willing to talk with them. Agent Bell motioned for defendant to be seated and then took the lead in questioning him.

8. In the ensuing conversation, questions, and answers, defendant made several oral statements. Defendant was advised of

the specific nature of the investigation and the officers' information about defendant's involvement with child pornography. During this interview, defendant made incriminating statements. Defendant specifically answered the questions put to him and then expanded his answers in a narrative fashion. He identified certain photographs and wrote his initials on them. Defendant was asked about the location of his computer and CD ROMs to which he had backed up some data. Defendant led the officers to his den, which was adjacent to the kitchen area where his wife was located. There he pointed out the equipment. At one time, when discussing the multitude of pornographic images in his computer equipment, defendant broke into tears.

9. During the interview, Agent Bell asked defendant whether he would make a written statement. Bell stated that any such statement would have to be voluntary and that defendant did not have to write one. Defendant said he wanted to make a written statement. Agent Bell provided defendant with several pieces of blank paper and asked him to write about the matter under investigation. At the top of the first piece of paper Agent Bell hand printed the date and the following introductory paragraph: "I \_\_\_\_\_ voluntarilly (sic) give this written statement. I understand I am under no obligation to give this statement & I give it freely." Gov. Exh. 4. Agent Bell then handed the paper to defendant and asked him to describe what had happened and what his role in it was. Defendant wrote his name on the blank line and printed a statement on the rest of the first page. He signed his name on the second page. Id. Agent Skinner was present through most of the interview and witnessed defendant signing his name. Skinner, however, did not sign his name as a witness on the statement until several days later.

10. At no time during the interview, or during the oral or written statements, was any threat or promise made to defendant to

induce him to cooperate and to make his statements. Throughout the interview, defendant did not request an attorney; he was never handcuffed or formally arrested or physically confined. At no time did defendant state to the officers that he did not want to make a statement.<sup>1</sup> At no time on November 16, 2000, did the officers advise defendant of his constitutional rights to remain silent and to counsel as set out in Miranda v. Arizona.

11. During the search of the residence the agents seized three CD ROMs, one IBM Aptiva computer, one keyboard, one computer mouse, and one digital camera. Gov. Exh. 3. These items were within the categories of the items described in the Attachment to the warrant which listed the items to be seized. See Gov. Exh. 2 at ¶¶ 1 and 9. At 11:30 a.m. the search was concluded and all of the officers left the residence. Thereafter, F.B.I. forensic investigators reviewed the data on the equipment that was seized.

#### DISCUSSION

##### The search warrant

Defendant Wolk argues that the search warrant issued for his residence was not supported by probable cause and was not lawfully executed. The undersigned disagrees.

The search warrant for 6 Shadow Lane was lawfully issued. The issue before this court when reviewing the legal sufficiency of the basis for the issuance of a search warrant is whether the issuing judge had a substantial basis for concluding that probable cause existed for the issuance of the warrant. Illinois v. Gates, 462 U.S. 213, 238-39 (1983); United States v. Luloff, 15 F.3d 763, 768 (8th Cir. 1994).

---

<sup>1</sup>The undersigned does not credit the testimony of defendant that he told the officers that he did not want to make a written statement. Trans., filed August 7, 2001, at 157-59.

Under the Fourth Amendment, probable cause for the issuance of a search warrant exists when there is a "fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Horn, 187 F.3d 781, 785 (8th Cir. 1999), cert. denied, 529 U.S. 1029 (2000) (quoting Illinois v. Gates, 462 U.S. at 238). A "fair probability" is less than an absolute certainty. Mason v. Godinez, 47 F.3d 852, 855 (7th Cir.), cert. denied, 516 U.S. 840 (1995).

In this case the affidavit of Special Agent Bell described specific facts learned from Police Sgt. Zaglifa about his observations that "Fish" was involved in the Internet communication of child pornography. Agent Bell learned from Danny Hughes, the System Administrator of Westplex Information Network, that the Internet access account used by "Fish" at the time the child pornography was communicated belonged to a Larry Wolk who resided at 6 Shadow Lane. Agent Bell corroborated through the Missouri Department of Revenue the accuracy of the Hughes' information that identified Larry Wolk's name with 6 Shadow Lane. All of this information was sufficient to establish probable cause to believe that 6 Shadow Lane held evidence of the unlawful distribution of child pornography. Judge Davis clearly had a substantial basis for finding probable cause.

Defendant argues that the affidavit information failed to advise the issuing judge that Agent Bell had had no prior experience with Hughes or Westplex and that Bell conducted no investigation about whether Westplex had a security program in place to prevent someone from assuming a Westplex account holder's identity on the Internet. Defendant argues that this failure to investigate and report to the issuing judge about the possibility that someone other than defendant communicated with Sgt. Zaglifa demonstrates bad faith on the part of Agent Bell. The undersigned disagrees.

By this argument, defendant appears to be invoking the holding of Franks v. Delaware, 438 U.S. 154 (1978). Under Franks, a defendant may be entitled to the suppression of evidence seized pursuant to a search warrant, if the government intentionally included false material statements in its warrant affidavit, or included false material statements with that reckless disregard for the truth that is the legal equivalent of intentional falsehood. United States v. Garcia, 785 F.2d 214, 222 (8th Cir.), cert. denied, 475 U.S. 1143 (1986).

A facially sufficient affidavit may be challenged also on the ground that the affiant deliberately or recklessly omitted material information. United States v. Lucht, 18 F.3d 541, 546 (8th Cir.), cert. denied, 513 U.S. 949 (1994); United States v. Reivich, 793 F.2d 957, 960 (8th Cir. 1986). In this regard, defendant Wolke must prove

(1) that the police omitted facts with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading, . . . and (2) that the affidavit if supplemented by the omitted information would not have been sufficient to support a finding of probable cause.

United States v. Lucht, 18 F.3d at 546 (quoting United States v. Reivich, 793 F.2d at 960).

In this case, it is clear that the affidavit information provided by Agent Bell was not false, inaccurate, or misleading. Hughes' position as the administrator of the Internet access provider established the reasonable reliability of the information he provided. Nothing in the affidavit implied that there was no likelihood another location could have been involved in the communications with Sgt. Zaglifa. Nothing in the record reasonably indicated to Sgt. Zaglifa or to Agent Bell that the person with whom Zaglifa communicated in the chat room was other than the person to whom the Westplex account was registered and who resided at 6 Shadow Lane. In the circumstances of this case, the



speculative possibility that someone else was responsible for providing the child pornography did not diminish the probable cause to believe that 6 Shadow Lane was involved as reported by Danny Hughes.

Defendant argues that the search warrant did not specifically describe the place to be searched and the items to be seized. The undersigned disagrees. Under the Fourth Amendment the language of a search warrant must describe the items to be seized with particularity: "the language must be sufficiently definite to enable the searcher to reasonably ascertain and identify the things authorized to be seized." United States v. Saunders, 957 F.2d 1488, 1491 (8th Cir.), cert. denied, 506 U.S. 889 (1992). See also United States v. Horn, 187 F.3d at 788. The standard is one of "practical accuracy," recognizing that the specificity required hinges on the circumstances of each case. United States v. Strand, 761 F.2d 449, 453 (8th Cir. 1985). A warrant naming only a generic class of items may suffice if the individual goods to be seized cannot be more precisely identified at the time that the warrant is issued. Horn, 187 F.3d at 788.

In this case the search warrant affidavit and the search warrant itself sufficiently described the place to be searched as the residence at 6 Shadow Lane, St. Peters, Missouri, 63376, and the computers and computer media found in the residence. A two-page attachment to the warrant and the affidavit specifically described the items to be searched for.

Defendant argues that the officials seized items outside the scope of the search authorized by the warrant. The undersigned disagrees. The items seized by the agents were specifically within the categories of things authorized by the warrant to be seized.

The search warrant was constitutionally issued and executed.

Defendant's statements

Defendant argues that his statements should be suppressed because they were not voluntary and were not preceded by an advise of rights pursuant to Miranda v. Arizona, 384 U.S. 436 (1966). The undersigned disagrees.

The government has the burden of establishing the admissibility of a defendant's pretrial statements by a preponderance of the evidence. Lego v. Twomey, 404 U.S. 477, 489 (1972); United States v. Astello, 241 F.3d 965, 966 (8th Cir.), cert. denied, 121 S. Ct. 2621 (2001).

A defendant who was not given his Miranda warnings, such as defendant Wolk, may be entitled to the suppression of the statements he made in response to police interrogation while he was in custody. He is not entitled to such relief, if he was not "in custody" when interrogated. Miranda v. Arizona, 384 U.S. at 477-78; Illinois v. Perkins, 496 U.S. 292 (1990). In this case the parties dispute whether defendant Wolk was "in custody" when he was interviewed and made his statements on November 16, 2000.

Generally, a person is "in custody" "when he has been formally arrested or his freedom of movement has been restrained to a degree associated with a formal arrest." United States v. Goudreau, 854 F.2d 1097, 1098 (8th Cir. 1988). To be considered "in custody" for Miranda purposes, a person need not have been formally arrested. In Stansbury v. California, 511 U.S. 318 (1994), the Supreme Court held:

In determining whether an individual was in custody, a court must examine all of the circumstances surrounding the interrogation, but "the ultimate inquiry is simply whether there [was] a 'formal arrest or restraint on freedom of movement' of the degree associated with a formal arrest." California v. Beheler, 463 U.S. 1121, 1125 (1983) . . . .

511 U.S. at 322.

Our decisions make clear that the initial determination of custody depends on the objective circumstances of the interrogation, not on the subjective views harbored by either the interrogating officers or the person being questioned. . . . "[It is] the compulsive aspect of custodial interrogation, and not the strength or content of the government's suspicions at the time the questioning was conducted, which [has] led the Court to impose the Miranda requirements with regard to custodial questioning." [Beckwith v. United States, 425 U.S. 341, at 346-347 (1976)]. . . .

Id. at 323 (emphasis added).

. . . "the only relevant inquiry is how a reasonable man in the suspect's position would have understood his situation." [Berkemer v. McCarty, 468 U.S. 420, 442 (1984)]. . . .

Id. at 324.

. . . . Even a clear statement from an officer that the person under interrogation is a prime suspect is not, in itself, dispositive of the custody issue, for some suspects are free to come and go until the police decide to make an arrest. The weight and pertinence of any communications regarding the officer's degree of suspicion will depend upon the facts and circumstances of the particular case.

Id. at 325.

In United States v. Griffin, 922 F.2d 1343 (8th Cir. 1990), the Eighth Circuit enumerated six indicia of custody:

(1) whether the suspect was informed at the time of questioning that the questioning was voluntary, that the suspect was free to leave or request the officers to do so, or that the suspect was not considered under arrest; (2) whether the suspect possessed unrestrained freedom of movement during questioning; (3) whether the suspect initiated contact with authorities or voluntarily acquiesced to official requests to respond to questions; (4) whether strong arm tactics or deceptive stratagems were employed during questioning; (5) whether the atmosphere of the questioning was police dominated; and (6) whether the suspect was placed under arrest at the termination of the questioning.

Id., 922 F.2d at 1349. The presence of the first three factors tends to mitigate the existence of custody at the time of questioning; the last three factors tend to indicate custody. Id. See also United States v. Brown, 990 F.2d 397, 399 (8th Cir. 1993).

Other factors relevant to the issue of whether or not an interrogation was custodial are the length of the interrogation and the place and purpose of the interrogation. United States v. McKinney, 88 F.3d 551, 554 (8th Cir. 1996).

Defendant Wolk's first statements were made to the officers outside the H & R Block office. There defendant was clearly not "in custody." The officers identified themselves as such and put defendant on notice that they were involved in a criminal investigation of him. Although they communicated his wife's desire that he return home, they expressly told him he did not have to do so. Nevertheless, without coercion he returned home.

From the factual record, the undersigned finds and concludes that defendant also was not "in custody" when he made the oral and written statements inside his residence. Regarding the first Griffin factor, defendant was told and he understood that any statement he made would have to be voluntary, that he was free to leave at any time, that he was not required to speak with the officers, and that he was not under arrest. The first factor militates strongly against custody.

Regarding the second Griffin factor, the agents directed defendant into the living room of the residence. However, he led them from the living room into his den to point out some equipment. There is no evidence that defendant was prevented from otherwise moving about or leaving his house or that the officials in any way indicated to him that he could not do so. There is no evidentiary basis for finding that his freedom of movement, exercised by him when he drove his automobile home alone, was not extended to him inside his home. Regarding the third Griffin factor, the record is

clear that defendant told the officials that he was willing to speak with them. He knew he did not have to do so. Regarding the fourth Griffin factor, there is no evidence that the officials in any way used strong arm tactics against him or in any way deceived him during the interrogation. These factors militate against a finding of custody.

Regarding the fifth Griffin factor, there is no doubt that there was a substantial police presence inside his home when defendant made his statements. However, defendant knew the officers were there to execute a search warrant, which tended to indicate a reason for their presence other than to interview him. Further, he had been repeatedly told he did not have to go home or to give statements to them. In this context, this factor does not militate toward a finding of custody.

The sixth Griffin factor tends to indicate that defendant was not in custody for Miranda purposes. He was not arrested at the conclusion of the interrogation or at the conclusion of the search and he had been previously told he was not under arrest. Finally, the interview lasted no longer than one and one-half hours and occurred in the defendant's own residence.

Under the circumstances of defendant's interrogation, a reasonable man would not have understood or believed that he was in custody or that his freedom of movement was limited to the degree associated with a formal arrest or that he could not go about his own business rather than give statements to the officers.

Defendant argues that United States v. Hanson, 237 F.3d 961 (8th Cir. 2001), supports his position. Hanson was convicted of arson at an abortion clinic. On appeal, among other arguments, he asserted that he was in custody when interviewed by federal agents, but was not given his Miranda warnings. The Court of Appeals, over Judge Morris Arnold's dissent, agreed and reversed his conviction. The facts relied on by the Court of Appeals to warrant Hanson's

Case 4:01-cr-00258-USA Document 34 Entered on FLSD Docket 08/16/01  
INTERNAL RECORD KEEPING

AN ORDER, JUDGMENT OR ENDORSEMENT WAS SCANNED, FAXED AND/OR MAILED TO THE FOLLOWING INDIVIDUALS ON 08/16/01 by lkresko  
4:01cr258 USA vs Wolk

COPIES FAXED AND/OR MAILED TO THE PARTIES LISTED BELOW AND THE UNITED STATES PROBATION OFFICE AND UNITED STATES PRETRIAL SERVICE OFFICE. IF THIS IS A JUDGMENT IN A CRIMINAL CASE SEND CERTIFIED COPIES TO THE FOLLOWING:  
4 Certified Copies to USM  
2 Certified Copies to USP  
1 Copy to Financial  
1 Copy to O.S.U.

Carrie Costantin -  
Richard Veit - 4605

Fax: 314-539-7695  
Fax: 636-940-8348

SCANNED & FAXED BY:  
108 16 2001  
C. D. D.



Copyright 2003 The Hartford Courant Company  
Hartford Courant (Connecticut)

August 6, 2003 Wednesday, 7 SPORTS FINAL

**SECTION:** CONNECTICUT; Pg. B7

**LENGTH:** 819 words

**HEADLINE:** MAN ARRESTED IN CHILD PORN CASE;  
COLLECTION LARGEST SEIZED IN NEW BRITAIN

**BYLINE:** KATIE MELONE; Courant Staff Writer

**DATELINE:** NEW BRITAIN --

**BODY:**

A laid-off trash collector, arrested Tuesday on 201 charges of possessing **child pornography**, amassed thousands of images of adults sexually abusing children as young as 3, according to court records unsealed after his arrest.

Rogelio Medina, 32, a father of two young boys, told police that in 2002 he began hopping in and out of **child pornography** chat rooms.

It soon became an addiction, court records state. Police claim Medina started a **child pornography** server on a computer in his Gold Street apartment and began trading photographs depicting young girls -- sometimes infants and toddlers -- engaged in sex acts with adults.

He used the screen name "Wizard of Oz," downloading traded files when his wife was not home. It ended in June, when a tip from an Illinois cop tipped New Britain police about the "Wizard."

Medina, of 93 Gold St., Apt. 2S, admitted to police in June that he ran the server. On Tuesday he turned himself in to police.

The arrest and investigation brought police the largest seizure of **child pornography** in the New Britain Police Department's history.

"This is the largest I've seen in this jurisdiction if not in this state," said Assistant State's Attorney Lou Luba.

Bail for Medina was set at \$75,000 after his arraignment Tuesday afternoon. Luba said the case has been forwarded to the FBI for review of federal charges.

Police charged Medina only over those pictures that depicted children they were able to identify. One showed a man performing a sex act on a girl thought to be under 3.

Medina, who in June admitted to running the server, has sought treatment at the Wheeler Clinic, his

attorney, Assistant Public Defender Todd Edgington, said Tuesday.

Medina could repair computers and often improved his Gateway using parts he found on his trash-hauling job, said a neighbor who lived in his three-story Gold Street apartment building. Once granted access to his server, online visitors were able to download roughly three photographs for every one photograph they added, Det. James Wardwell said.

"It was quite an operation," Luba said.

An Illinois detective working on a state child exploitation task force caught Medina in June when he entered a chat room and noticed a person using the screen name "WizardOfOz" displaying a banner ad for a **child pornography** file server. The detective, Det. Sgt. Michael Zaglifa, entered the server and discovered hundreds of pornographic files. He linked the screen name to Medina through Comcast, Medina's internet provider.

"These pictures are very serious," Zaglifa said. "All those pictures represent child abuse in progress. They're not just pictures."

Medina's server was the first such computer system discovered by the New Britain police, Capt. Michael Sullivan said. He said the department has typically nabbed individuals who buy or acquire pornography, and not those who distribute it.

The arrest surprised neighbors. "Wow," said Jose Cruz, at his Gold Street doorstep, corralling his toddler son into his apartment, which is feet away from Medina's.

"He didn't look like anybody bad," said Catherine Merced, a 12-year-old who lives upstairs from Medina. "He was sweet with his kids."

Catherine said Medina once fixed her family's home computer, and often gave her rides to school when she missed the bus. She once attended church with Medina and his wife, she said.

Authorities were able to identify several of the children depicted in the photos using a newly developed database at the National Center for Missing Exploited Children. The victims range in age, he said, because some of the photographs are between 15 and 20 years old. In most cases, the adults abusing the children in the photographs have been arrested and detained, Luba said.

Investigators went to lengths to identify the victims in the wake of an April Supreme Court ruling that, in effect, deems computer-generated **child pornography** legal. To bolster their case in light of the ruling, investigators set out to prove the children depicted in Medina's cachet of photos were real children, and not computer-generated or morphed images.

"In this case, we're dealing with a distributor, so we wanted to cross the t's, dot the i's," Wardwell said.

Police seized Medina's computer June 25 when he was away from home. Later that day, Medina visited detectives and admitted establishing the server to distribute **child pornography**, according to the arrest warrant. He started small, Medina told the police that day, and "just got deeper and deeper" into it. Soon he became addicted to the images, he told police.

He also told police that days before the seizure he reformatted his hard drive in an attempt to get himself "away" from **child pornography**. He told police he used an encryption program to disguise



his files to prevent his wife from learning of his hobby.

He expressed remorse for his actions, according to the warrant.

**LOAD-DATE:** August 6, 2003

---

MR. WHITFIELD. Mr. Roldan, I think Chairman Barton indicated he would be getting a question to you, and we would appreciate an answer on that.

I hope you all enjoyed being with the Energy and Commerce Oversight Subcommittee this afternoon. With that, the hearing is adjourned.

[Whereupon, at 7:25 p.m., the subcommittee was adjourned.]

RESPONSE FOR THE RECORD BY THE HON. ALICE S. FISHER, ASSISTANT ATTORNEY  
GENERAL, CRIMINAL DIVISION, UNITED STATES DEPARTMENT OF JUSTICE

Responses to Questions Presented to  
Assistant Attorney General Alice Fisher  
following the May 3, 2006 hearing of the  
Committee on Energy and Commerce  
“Sexual Exploitation of Children Over the Internet: What Parents, Kids, and  
Congress Need to Know About Child Predators”

**Questions from the Honorable Bart Stupak**

**1. In your testimony, you stated that the Attorney General had established an expert working group to look at the issue of data retention by Internet Service Providers. Would you provide the names of the members of that group, the issues they have been directed to address, and the timeframe for the completion of their work?**

**Answer:**

At the Attorney General’s direction, the Assistant Attorney General for the Office of Legal Policy convened a working group of experts within the Department of Justice to examine the issue of data retention in consultation with industry and to provide the Attorney General with proposed recommendations. The working group comprises representatives from the following Department components:

- Office of the Attorney General
- Office of the Deputy Attorney General
- Office of Legislative Affairs
- Office of Legal Policy
- Criminal Division
  - Computer Crime and Intellectual Property Section
  - Child Exploitation and Obscenity Section
  - Counterterrorism Section
  - Office of Enforcement Operations
- United States Attorney’s Office for the Middle District of Alabama
- Federal Bureau of Investigation
- Executive Office for United States Attorneys
- Office of Intelligence Policy and Review
- Office of Intergovernmental and Public Liaison
- Office of Public Affairs
- Office of Privacy and Civil Liberties

The working group has been tasked with examining the issue of data retention by communications service providers and to provide the Attorney General with proposed recommendations. The Attorney General has not limited the issues that the working group could consider, leaving the working group to define all the issues it believes to be relevant to its consideration of data retention.

The working group has provided the Attorney General with an initial set of issues to address with respect to data retention. The working group expects to provide the Attorney General with further information and to make recommendations with respect to data retention over the summer.

**2. You stated that search warrants had been issued that took down the commercial website that was being used by Justin Berry and his partners. Please provide the date those search warrants were executed, the court that issued the search warrants, and the supporting affidavits for those warrants. If those affidavits remain sealed, please provide that information.**

**Answer:**

The search warrants at issue remain sealed.

**3. Is it an accurate statement that local law enforcement departments whose personnel are working with the Federal Cyber Crimes Task Force, which is where child pornography cases are pursued, are not paid for their overtime, but are reimbursed for overtime of personnel working on the Terrorism and Violent Crimes Task Forces? If so, please explain the basis for stating that child pornography cases are a priority when local law enforcement departments can no longer afford to work with Federal agencies?**

**Answer:**

The Attorney General's Project Safe Childhood initiative demonstrates the priority the Department of Justice attaches to child exploitation cases. The initiative charges United States Attorneys with convening Federal, State and local law enforcement, including Internet Crimes Against Children (ICAC) task forces, and other leaders to develop strategic plans for each judicial district to coordinate efforts on national investigations, pursue leads from the National Center for Missing and Exploited Children's Cybertipline and advance public awareness. In May 2006, the Department published a Manual on Project Safe Childhood that provides guidance to and identifies resources available to support Federal, State, and local law enforcement efforts to implement the Project Safe Childhood initiative. In his May 2, 2006, letter prefacing the Manual, President Bush stated that "[m]y Administration is committed to protecting our children from abuse and exploitation by online predators." In his May 17, 2006, letter in that Manual, the Attorney General stated that "I have made it one of the highest priorities of the Department of Justice to protect children from...computer-facilitated sexual abuse and exploitation."

The Department provides financial and other support to State and local law enforcement investigating computer-facilitated crimes against children through the ICAC program, which is administered by the Office of Justice Programs' (OJP) Office of Juvenile Justice and Delinquency Prevention (OJJDP). This program funds 46 ICAC task forces nationwide. OJJDP created the ICAC Task Force program to help State and local law

enforcement agencies enhance their investigative response to offenders who use the Internet, online communication systems, or other computer technology, to sexually exploit children. OJJDP's grant program helps State and local law enforcement agencies acquire the necessary knowledge, equipment, and personnel resources needed to prevent, interdict, or investigate ICAC offenses.

Consistent with that mandate, the investigation of Internet crimes against children has been and continues to be a priority for the FBI. Cybercrime ranks behind only counterterrorism and counterintelligence in the Bureau's Strategic Plan. The FBI-led Cyber Crime Task Forces (CCTFs) are multi-jurisdictional entities comprising personnel assigned primarily from Federal, state, and local law enforcement and criminal justice agencies. Both the CCTF Standard Operating Procedures (June 2004) and the CCTF Memorandum of Agreement typically executed by the participating agencies provide that overtime may be paid to CCTF members by their employing agencies in accordance with the applicable overtime provisions of those agencies. While Congress has provided FBI funding for overtime compensation for some task forces (for example, the FBI has been funded by Congress to reimburse state and local agencies for the overtime worked by full-time members of Safe Streets Task Forces), funds have not been appropriated for CCTF overtime. Consequently, the funding of CCTF overtime is generally at the discretion of a task force member's employing agency.

RESPONSE FOR THE RECORD BY JAMES R. MARSH, ESQ.

Marsh Menken & Weingarden pllc

---

81 Main Street, Suite 305  
White Plains, New York 10601  
P – 914-686-4456  
F – 914-206-3998  
www.mmwlaw.us  
James.Marsh@MMWLaw.us

July 7, 2006

The Honorable Bart Stupak  
Ranking Member  
U.S. House of Representatives  
Committee on Energy and Commerce  
Washington, DC 20515-6115

Re: **Sexual Exploitation of Children Over the Internet Subcommittee Hearing  
Response to Additional Questions**

Dear Congressman Stupak,

It was an honor to appear at the Subcommittee on Oversight and Investigation's May 3, 2006 hearing on the Sexual Exploitation of Children Over the Internet. Your interest in this vital issue will greatly contribute to the emerging national consensus that much more can and must be done to protect our children by regulating the wide and unmitigated distribution of child pornography on the internet.

Please find the following answers in response to your additional questions arising from the hearing:

Question 1

Please provide copies of the home study done of Matthew Mancuso prior to his adoption of Masha in 1998 and the home study done of Faith Allen prior to her adoption of Masha in 2004 and describe the major differences.

Answer 1

Exhibit 1 – Mancuso Home Study  
Exhibit 2 – Allen Home Study

The major difference between these two documents is that the Allen home study is child-centered and the Mancuso home study is parent-centered. By this I mean that the Allen home study is focused on the unique needs and individual circumstances of the child, Masha Allen, while the Mancuso report is a public relations document written by the social worker and director of the Family Health Council, Inc.'s Family Adoption Center, Nancy Simpronio, on behalf of Matthew Mancuso.

The Allen home study specifically identifies dates and the names of the individuals contacted as primary or collateral sources of information [p. 2-02]. The "very thorough [Mancuso] home study process" [p. 1-01], while obliquely referring to his un-named "mother" and several siblings [p. 1-04], is based exclusively on "intensive interviews with Mr. Mancuso" [p. 1-02]. So, while the Mancuso report relies on one self-interested source for all the information contained therein, the Allen home study utilizes no less than 10 independent sources, including Masha herself.

The Mancuso home study is comprised largely of conclusory statements based on information taken directly from the subject of the report. There were no interviews with collateral sources such as Mancuso's estranged daughter, his ex-wife, neighbors, friends and support networks. There was no attempt to contact his mother and sister for their opinion of Mancuso as a father. There was no verification of his parenting abilities or community resources.

In reality, Mancuso raped and molested his birth daughter and his computer screen name was "IFuckedMySister." The fact that "the interviews were conducted by a Master's degree licensed social worker with over fourteen years adoption experience" [p. 1-02] is meaningless. Mancuso's reference to "his travels throughout the world" [p. 1-06] should have prompted a review of his passport since child sex tours are common for wealthy pedophiles like Mancuso.

In addition, Mancuso's report that he "had spent a considerable amount of time researching adoption and discussing adoption with adoptive parents for the past six months" [p. 1-06] should have led to collateral contacts with these individuals to ascertain their impressions of Mancuso. Obviously, Mancuso's preference for "a girl between the ages of five and six of the Caucasian race" [p. 1-06] was additional cause for concern which should have led the social worker to consider alternative motivations for the adoption.

Mancuso's statements about "parenting," "adjustments," "professional assistance," "child care," and "faith" [p. 1-07], while highly relevant, are largely without substance in the absence of collateral contacts and added detail. There is no discussion about who, what, where and when Mancuso would do anything for a young girl speaking a foreign language from a foreign culture.

There is also the acknowledgement that Mancuso did not even have a bedroom for Masha since "currently the room is a mix-match of furniture which he plans on replacing with appropriate furnishing for a young girl" [p. 1-08]. In reality, Masha slept in Mancuso's bed for over four years where she was raped and molested nightly. She never had her own room or even a bed. The agency's vow to "provide post-placement reports for a period of three (3) years" [p. 1-01, 1-09] apparently did not include either home visits or meeting with Masha.

The statement that “Mancuso is close to his nearest neighbors including one with four daughters” is chilling given his lifelong history as a pedophile. There is no indication that this neighbor or these girls were contacted. The section of the home study devoted to references [p. 1-08] merely parrots the cursory written testimonials which were provided by the office manager at Mancuso’s place of employment, a subordinate at his place of employment, and a former co-worker [pp. 1-11-13]. Again, there is no indication that these individuals were questioned at all by the social worker writing the home study.

Finally, there is no basis for the Ms. Simpronio’s conclusion that Mancuso is “a highly moral individual who will provide not just a financially stable home but the ability to parent a child with values” [p. 1-09]. The reality could not be further from this asinine endorsement.

#### Question 2

Is there any procedure for Masha to copyright all the images of her made by Mr. Mancuso and then pursue remedies under copyright law for any illegal distribution, or does the civil cause of action under 18 USC 2255 provide a more efficient and useful remedy?

#### Answer 2

“Works of the visual arts are protected under United States copyright law. Visual arts include original pictorial, graphic, and sculptural works in two and three dimensions. As with other types of copyrightable works, copyright protection for works of the visual arts is automatic upon creation. The work is created as of the moment it is fixed in media for the first time.” *E-Copyright Law Handbook*, Laura Lee Stapleton, Aspen Publishers (2003) § 6.02[A].

Although Masha’s images are per se copyrightable since they are works of the visual arts, the ability to obtain and assert copyright protection over them is unworkable if not impossible. As a practical matter, it is illegal for anyone—including Masha and her parent and attorney—to possess the pornographic images of her, making it difficult to even identify the items subject to copyright. It is also illegal for anyone outside of law enforcement to go looking for her images such as by visiting pedophile chat rooms or joining websites featuring child pornography. Masha would, therefore, have a difficult time obtaining and asserting any copyright interest in her images.

It is also unlikely that the courts, on public policy grounds, would allow anyone to possess and enforce copyright protection over images which are per se illegal.

The civil cause of action provided by 18 USC 2255 is a valuable but imperfect source of relief for victims of child pornography. The provision of statutory liquidated damages is a great benefit to victims who do not have to prove they were injured by the unlawful possession of their images.

The utility of 18 USC 2255 is limited, however, for the same reason that asserting copyright protection is impractical; victims must rely on law enforcement and notices under the federal Victims of Crime Act to identify and locate their images. Without law enforcement involvement and cooperation, victims will be unable to utilize the recourse provided by 18 USC 2255. Without proactive law enforcement identification and notification, an individual may not even know they are a victim of child pornography.

Currently, only federal law enforcement agencies are required to notify victims of child pornography, leaving the huge number of state prosecutions for child pornography out of reach for child victims otherwise eligible for relief under 18 USC 2255. In our experience, federal notification is spotty at best. To date, we have only received Victim of Crime Notices from 4 out of 94 federal judicial districts (4%) even though Masha's images are recovered in over 50% of all prosecutions for child pornography.

One possible enhancement of current law would allow the Digital Millennium Copyright Act of 1998 (DCMA) to be utilized to combat child pornography. The DCMA requires anyone who reproduces, distributes or displays copyrighted work without prior permission to pay significant damages as specified under the act including injunctive relief, actual damages and profits of the infringer, statutory damages of \$750-\$30,000 per infringed work or up to \$150,000 per infringed work in cases of willful infringement, and attorney's fees.

The DCMA grants limited shelter to online service providers for potential infringements occurring on their networks and systems, as long as they are unaware of the infringement, but providers must act expeditiously to remove or block access to copyrighted material once infringement is alleged. The DCMA has an extensive section on remedies which includes impounding any device involved in a violation and in the custody and control of the alleged violator, damages, recovery of court costs, recovery of attorney's fees, and destruction of any device involved in a violation which is in the custody or control of an alleged violator or which has been impounded.

Perhaps the greatest use of the DCMA for child pornography victims would allow them to demand that ISPs "takedown" the illegal images which might be residing on their network. Another useful provision would allow child pornography victims and law enforcement to contact website registrars to demand that known or potential child pornography websites – even foreign sites – be effectively "de-listed" from the world wide web, rendering access to those sites impossible.

### Question 3

Are there any legislative changes that should be made, in addition to Masha's Law, to encourage all Internet service providers (ISPs) to more carefully police their sites for illegal child pornography and remove it more rapidly? Is it effective to work only with the largest Internet service providers, or are pedophiles using less well-known ISPs?



Answer 3

Using current technology and the databases of known child pornography at the FBI, ICE and NCMEC, ISPs can and should be required to scan their networks for known child pornography and block access to those images. All internet access is dependent on a limited number of Tier 1 ISPs over which a majority of the world's internet traffic flows. Simple scanning of this network traffic could easily eliminate access to known child pornography. This is akin to placing drug sniffing dogs in the post office or metal detectors in airports. Utilizing the database of known child pornography images will address any First Amendment concerns since actual child pornography enjoys no Constitutional protection and is per se illegal and is subject to seizure and destruction.

Question 4

You testified that pedophile networks are actually creating parallel networks to the Internet that the public is familiar with. Access and images are tightly controlled by a few people, and there is no central server and no Internet service provider (ISP). Does current law and law enforcement efforts reach those networks? What must be done to control them?

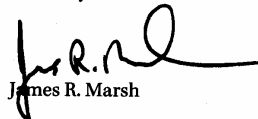
Answer 4

The networks I was referring to are accessed using the same ISPs that everyone else uses to access the Internet. What is different about them is that they are encrypted and widely distributed peer-to-peer networks with no central server and no central access control mechanism. Files and other content are broken into small bits and distributed over hundreds and even thousands of computers world wide. These packets are regularly moved among and between computers and only reassembled when a requester presents a key relating to that specific file.

In my discussions with law enforcement, they are aware of and have begun to penetrate these networks. Since there is currently no search mechanism on these networks, person-to-person relationships must be established to gain access to files and other content. Technologically limiting these networks is probably impossible and only traditional law enforcement surveillance and infiltration methods will be effective in both understanding and controlling these networks.

Please do not hesitate to contact me for further explanation or discussion of these answers and this important public policy issue.

Sincerely,



James R. Marsh

**EXHIBIT 1**



960 Penn Avenue • Suite 600 • Pittsburgh, PA 15222 • (412) 288-2138



RECOMMENDATION OF FAMILY ADOPTION CENTER

RECOMMENDATION OF MR. MATTHEW A. MANCUSO

PASSPORT NUMBER: 091081336

Through a very thorough home study process, I am happy to favorably recommend Mr. Matthew A. Mancuso, a U.S. Citizen who resides at 158 Shearer Road, New Kensington, PA 15068 be approved for adoption through Russia. I recommend approval for Mr. Mancuso to adopt one child between the ages of five and six, either male or female. I also recommend Mr. Mancuso for the adoption of a child with a medical special need if he so chooses.

Mr. Mancuso is very capable, willing and well-prepared to provide a stable and loving home. He has begun to make preparations for the arrival of a child. Mr. Mancuso is prepared to help his child develop an educated awareness and understanding of Russian culture and will help the child to identify with his/her heritage. He is committed to raising a child.

I have a Master's degree in Social Work and over fourteen years experience doing adoptions. I have the authority to conduct home studies for Family Adoption Center, a licensed adoption agency/home study agency in the State of Pennsylvania.

This agency hereby agrees to provide post-placement reports for a period of three (3) years.

*Robert M. Matthews*  
Name and Degree

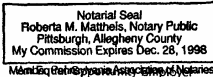
*Director*  
Title

State of *Pennsylvania*  
County of *Allegheny*

Sworn and subscribed to before me this *21* day of *November*, 19 *97*.

*Robert M. Matthews*  
Notary Public

My commission expires: *12/28/98*





Family Health  
Council, Inc.

960 Penn Avenue • Suite 600 • Pittsburgh, PA 15222 • (412) 288-2138

Family Adoption Center 

1-02

HOME STUDY - MATTHEW ALAN MANCUSO  
PREPARED NOVEMBER 20, 1997

Matthew Alan Mancuso - Born July 3, 1958  
158 Shearer Road  
New Kensington, PA 15068  
Home phone - (412) 335-3189  
United States Citizen  
Passport Number: 091081336

This home study is being performed at the request of Mr. Mancuso. He is in the process of adopting a child through an international adoption. The placing agency is a licensed agency in New Jersey, Families Through International Adoption. The phone is (609) 321-0777 and the contact is Ms. Jeannene Smith.


The home study is being prepared by Family Adoption Center, a licensed adoption agency. The interviews were conducted by a Master's degree licensed social worker with over fourteen years of adoption experience. The study was conducted in the office of Family Adoption Center and in Mr. Mancuso's home. It consisted of a written application, a medical statement from his physician, child abuse and criminal record checks, three reference letters, financial and income tax statements and intensive interviews with Mr. Mancuso.

PHYSICAL DESCRIPTION

Mr. Mancuso is a Caucasian male of Italian heritage. He is five feet, seven inches tall with a medium complexion, dark hair and hazel eyes. He weighs 145 pounds with an athletic build.



Family Health Council, Inc.

Family Adoption Center 

960 Penn Avenue • Suite 600 • Pittsburgh, PA 15222 • (412) 288-2138

RECOMMENDATION OF FAMILY ADOPTION CENTER

RECOMMENDATION OF MR. MATTHEW A. MANCUSO

PASSPORT NUMBER: 091081336

Through a very thorough home study process, I am happy to favorably recommend Mr. Matthew A. Mancuso, a U.S. Citizen who resides at 158 Shearer Road, New Kensington, PA 15068 be approved for adoption through Russia. I recommend approval for Mr. Mancuso to adopt one child between the ages of five and six, either male or female. I also recommend Mr. Mancuso for the adoption of a child with a medical special need if he so chooses.

Mr. Mancuso is very capable, willing and well-prepared to provide a stable and loving home. He has begun to make preparations for the arrival of a child. Mr. Mancuso is prepared to help his child develop an educated awareness and understanding of Russian culture and will help the child to identify with his/her heritage. He is committed to raising a child.

I have a Master's degree in Social Work and over fourteen years experience doing adoptions. I have the authority to conduct home studies for Family Adoption Center, a licensed adoption agency/home study agency in the State of Pennsylvania.

This agency hereby agrees to provide post-placement reports for a period of three (3) years.

*Wendy S. ...*  
Name and Degree

*Director*  
Title

State of *Pennsylvania*  
County of *Allegheny*

Sworn and subscribed to before me this *21* day of *December*, 19*97*.

*Robert M. Matthews*  
Notary Public

My commission expires: *12/28/98*

Notarial Seal  
Robert M. Matthews, Notary Public  
Pittsburgh, Allegheny County  
My Commission Expires Dec. 28, 1998

**BACKGROUND INFORMATION**

Mr. Mancuso was born on July 3, 1958 in Pittsburgh, Pennsylvania. He is the second of four children. Eugene, Jr. is the oldest with Mary Angela and Christopher being the younger siblings. They are two years apart from each other.

Mr. Mancuso's mother was a registered nurse and his father owned and operated an Italian bread business. When Mr. Mancuso was a toddler the family moved to Verona, PA. Mr. Mancuso appears to have very positive memories of his childhood which included playing with his siblings and having extended family members only a few blocks away from their home.

Mr. Mancuso stated his home life was typical for children in the 60's and the family considered themselves middle class.

As a child, Mr. Mancuso enjoyed taking art classes along with music lessons. He was an accomplished accordion player as a young child due to his grandfather's influence. As a teenager he played the organ, trumpet, guitar and the drums. Mr. Mancuso played the drums for a high school rock group with his cousin and brother. They successfully had one paying job before breaking up the band.

Holidays and family gatherings were always important as well as fun events for the Mancuso family.

During Mr. Mancuso's preteen and teenage years the family made a series of moves due to his father's involvement in various businesses. There was a time they moved out of Pennsylvania to Chicago. They did return to Pennsylvania after several months. Mr. Mancuso stated that he and siblings adapted to the moves and learned to make friends and navigate new schools and communities during this time.

Mr. Mancuso stated he enjoyed his childhood and has fond memories of his youth.

Presently, Mr. Mancuso's mother is a healthy, active woman with her own business. She is sixty five years old and stated a pet kennel. She has also published a book on dog training. Christopher works with their mother in the pet business. Eugene and Mary Angela also live close to them. Mr. Mancuso's father died suddenly in 1986 due to brain aneurysm and that was a great loss for everyone.

Mr. Mancuso stated that his strengths are his ability to think logically, he is resourceful and creative. He stated that he views himself as being loyal and an easy-going personality. He stated he feels at times his shyness gets in the way of socializing with new people. He prefers to spend time with long time friends or his family.

He enjoys cooking for friends, playing with his computer, working on his investments. Riding his motorcycle is also a favorite pastime.

#### MARRIAGE

Mr. Mancuso met his former wife through his cousin. She was from his home town of Verona and was a year younger. They shared many people and experiences in common. They dated during Mr. Mancuso's last year of high school and it was after his graduation that they discovered they were pregnant. Both families were upset when they told their respective parents of the situation. Mr. Mancuso's parents were the most upset and stated that they did not want to see him again. Mr. Mancuso's siblings also distanced themselves from him. Mrs. Mancuso's parents took them in and they eloped to Cumberland, Maryland where they got married. Mr. Mancuso lost his job at Keibler Industries when his father fired him.

The newly married Mancusos moved into Mrs. Mancuso's parents home and Mr. Mancuso found a job at a toy warehouse on a part time basis. Eventually in October of 1976 Mr. Mancuso's father called and offered him his former job full time at the plant.

In January of 1977 Mr. and Mrs. Mancuso moved into a small apartment in a nearby community. Mr. Mancuso worked, took a few classes at the Penn State extension campus in their community and drove his wife back to high school in Verona so she could graduate.

In March that same year their daughter Rachelle was born. After an initial period of adjustment that Mr. Mancuso admits to being stressful for both of them, he and his wife settled into a regular routine and home life with their daughter.

Mrs. Mancuso completed high school and Mr. Mancuso was offered a better position at the plant. This enabled them to return to Verona and be close to her parents. At the same time, Mr. Mancuso had stopped taking classes due to the added responsibilities of being a parent and the money needed to pay for tuition. Keibler Industries proposed a tuition plan for Mr. Mancuso and he returned to college majoring in mechanical engineering.

Mr. Mancuso has very strong memories about being a father to Rachelle and enjoyed his role. He continued to grow with responsibilities in the company and receive promotions.

In 1984 he and Mrs. Mancuso built their home where he still resides. He and Rachelle appreciated the rural setting while Mrs. Mancuso did not participate in the various adventures they would take such as walking in the woods behind their home or visiting the neighbor's horses.

When Rachelle was ten years the differences between Mr. and Mrs. Mancuso became more apparent. He stated he was always more of a "homebody" while she preferred the social scene. Mr. Mancuso stated he requested a divorce when he determined she was having a relationship with another man. They did attempt marital counseling for several months however she discontinued it and Mr. Mancuso learned that she had continued the affair during the time they were involved in counseling.

The divorce was finalized in March of 1987 and they had been married almost eleven years. Mr. Mancuso remains positive about the marriage until the end. He immersed himself in his work to cope with the loss. By mutual agreement, Mrs. Mancuso returned to Verona to be near her family and to raise Rachelle. Mr. Mancuso paid generous support and had weekend visits with his daughter.

As Rachelle entered her teenage years the weekend visits became fewer and fewer. She wanted to be near her school friends and participate in activities with them. At first, Mr. Mancuso would invite a friend or two to spend the weekend with them however Rachelle spent her time with her friends rather than her father. As she got older the closeness began to fade and by the time she graduated high school they only saw each other on birthdays and holidays.

This lack of relationship has been very difficult for Mr. Mancuso and he feels strongly that he will always be available to Rachelle. He paid for her education at a culinary school. At this time she is twenty years old and has a live-in relationship with a man.

#### ADOPTION

Mr. Mancuso wants to adopt a child as he strongly misses the parenting role that he had with his daughter. He very much wants to provide a strong home life for a child in need. Along with his desire to be a parent and his travels throughout the world have given him an appreciation of other cultures and the ability to help a child without a home.

Mr. Mancuso had spent a considerable amount of time researching adoption and discussing adoption with adoptive parents for the past six months.

He has discussed adopting a child with his family and they are supportive.

#### THE CHILD

Mr. Mancuso would like to adopt a girl between the ages of five and six of the Caucasian race. He is willing to consider a child with minor disabilities that can be corrected. He is also willing to take a child diagnosed with learning disabilities.



Mr. Mancuso feels that as a single parent adopting a young child and not an infant would be the best situation. He would prefer a daughter since he has experience with parenting a girl as he did with his daughter. He understands the adjustments that will be necessary in his life and he is prepared to make the changes to accommodate a young child.

Mr. Mancuso also understands that adoption brings challenges and issues that parents who give birth to a child do not have to manage. He is willing to seek professional assistance if necessary to aid him with the placement. Mr. Mancuso is eager to become a parent and has considered making changes in his work schedule to spend more time with the child he adopts. Some of his work he can do from his home office along with computer and fax support. He has already spoken to a local child care center that can provide extended day coverage while he is working.

#### RELIGION

Mr. Mancuso is of the Catholic faith. He no longer is an active member of a church at this time. He understands the importance of exposing a child to a religious faith and plans on doing this with the child he adopts.

#### EDUCATION / EMPLOYMENT / MILITARY SERVICE

Mr. Mancuso never served in the military.

Mr. Mancuso attended public grade and high school. He stated he has very fond memories of both grade and high school.

In high school Mr. Mancuso played football and was on the wrestling and track teams. He also was a member of the chess club. He took academic courses and would take the higher level math and science classes, often he was ahead of his other classmates. His grades were above average and upon graduation had taken calculus, physics, nuclear science, chemistry, biology and anatomy. At that time Mr. Mancuso was planning to attend college and becoming a chiropractor.

During high school Mr. Mancuso began working at the same company where he is now employed with the janitorial department. His job consisted of sweeping the floor, emptying the trash and scrubbing the bathrooms. Eventually he worked with other departments, the weld shop, the machine shop, the paint shop, the maintenance shop and the parts warehouse. He saved his money and before he graduated high school Mr. Mancuso had bought and paid for his first car, a used 1969 Firebird.

Mr. Mancuso is close to his nearest neighbors including one with four daughters.

Any child he would adopt would have their own room. Currently the room is a mix-match of furniture which he plans on replacing with appropriate furnishings for a young girl.

#### PETS

Mr. Mancuso does not own any pets. Mr. Mancuso did state that he considers himself sharing the neighbor's cat as the cat visits Mr. Mancuso on a regular basis and often leaves "gifts" for him.

#### CRIMINAL RECORD/CHILD ABUSE CHECKS

Mr. Mancuso submitted the required criminal record and child abuse checks for review. Both were negative and are included with this report.

#### REFERENCES

Mr. Mancuso submitted three references from friends and family members who have known him for years and can testify to his personality and ability to parent. All the references were very positive and favorable to Mr. Mancuso. All the references stated they believed Mr. Mancuso should be permitted to adopt. The references are included with this report.

#### MEDICAL

Mr. Mancuso is under the care of Dr. Perviz Heyat of the New Kensington Health Center. Dr. Heyat examined Mr. Mancuso on July 14, 1997 and determined he is in good general health with no problems to indicate that he should not be an adoptive parent. Mr. Mancuso's medical history and physician's statement are included with this report.

#### FINANCIAL STATUS

Mr. Mancuso's 1996 income tax return showed a total income of \$111,699. He included a financial breakdown of his assets and expenses. He carries no debts as his home is paid off and has no car payments. He has a four wheel drive vehicle and a motorcycle.

Mr. Mancuso carries medical insurance through his employer that provides comprehensive coverage with Blue Cross/Blue Shield/Select Blue program. He has life insurance along with significant pension and financial portfolio savings.

His employer Keibler Thompson Corporation submitted a letter stating Mr. Mancuso's current salary is \$115,000.00 per year.

The addition of a child to Mr. Mancuso's income will not be a hinderance financially to Mr. Mancuso. He lives well within his means and has significant holdings for his future.

All financial information is included with this report.

#### SUMMARY AND RECOMMENDATION

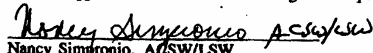
It is the recommendation of this licensed social worker that Mr. Matthew Mancuso be approved for the international adoption of a young child.

He is a caring, loving man who misses the parenting role that he had with his daughter. He is a highly moral individual and will provide not just a financially stable home but the ability to parent a child with values. He is committed to having a family and is willing to make the necessary adjustments to his home and to his lifestyle to insure that the best interests of a child are paramount.

Mr. Mancuso understands that at times as a single parent he may require the assistance of other support people. His mother and sister are willing and able to assist. One situation Mr. Mancuso needs to establish is to have a will written and provide guardians for his child he adopts. He has given this matter some thought and plans on asking long time friends of his who he admires for their parenting skills.

Mr. Mancuso is committed to contacting professionals if needed for help with either parenting or adoption issues.

Family Adoption Center is willing to conduct the required supervisory visits along with being a local support for Mr. Mancuso during the adoption process.

  
Nancy Simpronio, A/MSW/LSW  
Director  
PA License # 000561-E

**F** Family Health Council, Inc.

Family Adoption Center 

960 Penn Avenue • Suite 600 • Pittsburgh, PA 15222 • (412) 288-2138

I, Nancy Simpronio, do hereby swear and affirm that the facts contained in the foregoing Home Study are true and correct to the best of my knowledge, information and belief.

Nancy Simpronio ACSW/LSW  
Nancy Simpronio, ACSW/LSW

Sworn to and subscribed before me

this 11<sup>th</sup> day of  
November, 1997

Roberta M. Mattheis  
Notary Public

My Commission Expires: 12/28/98

Notarial Seal  
Roberta M. Mattheis, Notary Public  
Pittsburgh, Allegheny County  
My Commission Expires Dec. 28, 1998  
Member, Pennsylvania Association of Notaries



**KEIBLER THOMPSON CORP.**

130 ENTRANCE DRIVE • LOGANS FERRY HEIGHTS • NEW KENSINGTON, PA 15068 PHONE: (412) 335-9161 / FAX: (412) 335-6189

August 20, 1997

This letter hereby verifies that Matthew A. Mancuso has been a full time employee of Keibler Industries, Inc. since November 1, 1976. It should also be noted that Mr. Mancuso was a part time employee for two years prior to that date.

Mr. Mancuso is currently a company Vice President in charge of Engineering and Equipment Sales. His average income for the last three years is \$115,000.00 per year.

*Carol Goulding*  
Carol Goulding  
Office Manager

State of Pennsylvania  
County of Westmoreland

Before me, the undersigned Notary Public in and for the County and State, hereby certify that before me personally appeared, Carol Goulding, who acknowledged that the facts contained herein are true and correct.

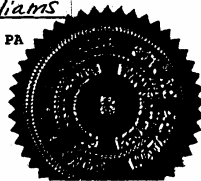
WITNESS my hand and notarial seal, this 17<sup>th</sup> day of Dec., 1997.

My commission expires:

March 13, 2000

*Bonnie S. Williams*  
Notary Public  
Printed: Bonnie S. Williams  
Residence of Notary Public  
Westmoreland County, PA

Notarial Seal  
Bonnie S. Williams, Notary Public  
New Kensington, Westmoreland County  
My Commission Expires March 13, 2000  
Member, Pennsylvania Association of Notaries



Richard Dale Knopsnider  
267 Pine Hill Rd.  
White, PA 15490

September 12, 1997

Attn: To Whom It May Concern  
Subj: Letter of Recommendation

It gives me great pleasure to recommend Matt Mancuso to become an adoptive parent.

I have known Matt for over eight years now. He was my immediate supervisor for six years, while I worked as a Design Engineer at Keibler Thompson Corp. and now as I work with Matt in an ongoing business relationship. He is a well-rounded individual, displaying intelligence, dedication, responsibility and also a sense of humor. Traits that are required to be successful not only in the business world, but also as a parent.

As the father of three young boys, I believe I have a good idea of what it takes to be a good parent. I think Matt would provide the same kind of lifestyle and atmosphere for a child that I would desire for my children, if someone else were to rear them.

Sincerely,

  
Richard Dale Knopsnider

**Sakala Stone Products**

7230 Guyer Road • Lower Burrell, PA 15068  
(412) 339-2224

September 13, 1997

To Whom It May Concern:

This letter is written in reference to Matt Mancuso, a long-time friend and colleague, who desires to adopt a child. We have known Matt for over 20 years, having met him through Keibler-Thompson Corporation, where he and Paul worked.

We believe that Matt would make an excellent parent for an adopted child. First, he is financially secure, has a nice home and a good job. Secondly, Matt's demeanor and personality are well-suited for children. He is a quiet, easy-going man who has the time and patience for children. But most importantly, we believe that Matt has a lot of love to give a child. We know that Matt is sincere about his commitment to adopt a child and is able to give a child lots of love and attention. He is able to provide a secure, comfortable, stable and loving environment to a lonely boy or girl.

Please feel free to call us if you have any questions regarding our comments.

Sincerely,

*Paul and Cindy Sakala*

Paul and Cindy Sakala

MEDICAL CERTIFICATE FOR PROSPECTIVE ADOPTIVE PARENT

1-14

This examination is made in order that we may determine whether the applicant's physical health will permit him/her to adopt a child. The applicant's present, as well as future health, is of paramount importance and should be given serious consideration. For the most part, we ask that the physician use his or her own discretion as to the appropriateness of bloodwork, x-rays, or other tests. This form may be returned to the parent or mailed directly to the Alliance.

1. Patient's name: Matthew Mancuso DOB: 7-3-58 Ht: \_\_\_\_\_ Wt: 148 1/2
2. General appearance: Good
3. Heart: KRR. no murmur Blood Pressure: 118/86 Lungs: Clear
4. Hearing: Good Vision: Good Dental: 12
5. Heart disease: No Diabetes: No Venereal disease: No  
 Infectious disease: No Alcoholism/other addiction: No  
 Seizure disorder: No Nervous disorder: No  
 Allergies: Bee sting - not anaphylactic HIV-AIDS test (date and results): 7/16/97 NEGATIVE
6. Abnormal findings (please explain): No
7. Has the patient any chronic disease that in your opinion would be detrimental to the supervision and care of children? No If yes, please explain: \_\_\_\_\_
8. Is there anything in the patient's present state of health that would tend to shorten his/her life span? No If yes, please explain: \_\_\_\_\_
9. In view of your finding, do you consider the patient physically competent to adopt a child(ren)? Yes
10. If the applicant has children, what is, to your knowledge, the state of health of each child? Has one daughter in good health

7/14/97  
Date of Examination

Periz Heyat  
Physician's Signature

PERVIZ HEYAT  
Physician's name (please print)  
New Kensington Health Ctr.  
Address  
1260 Martin Ave City/State/Zip  
(412) 339-6641 New Kensington, PA  
15068  
 Telephone



**EXHIBIT 2**

**Child Profile Report**

for

**MASHA**



prepared by Michele A. Cunko

October 7, 2003

Every Child, Inc.

**STATEWIDE ADOPTION NETWORK  
CHILD PROFILE**

<b>Child's Name:</b>	<b>Maria "Masha" M.</b>
<b>DOB:</b>	<b>8-25-92</b>
<b>Gender:</b>	<b>Female</b>
<b>Race:</b>	<b>Caucasian</b>
<b>Date of Profile:</b>	<b>October 7, 2003</b>
<b>Prepared by:</b>	<b>Michele A. Cunko, MAC HR Consulting, LLC</b>
<b>CYFS Adoption Worker:</b>	<b>Wendy Krauss</b>

**A. SOURCES OF INFORMATION**

Information was gathered on August 28, 29 and September 12, 13, 30 and October 2, 3 and 6, 2003 through examination and analysis of the Allegheny County Children Youth and Family Services (CYFS) records and interviews with CYFS caseworker Wendy Krauss, CYFS intake worker Diane Goble, adopted maternal grandmother Ann, FBI agent Denise Valentine, attorney Stanley Greenfield, Keith Wallace, Family Through International Adoption, Jeannine Smith, Reaching Out Through International Adoption, The Children's Institute and foster mother Lynn Ginn. In addition, a visit with Masha and Ms. Ginn was conducted at their home on September 22, 2003.

**B. INTRODUCTION**

Masha is an attractive, slender youngster who has chin-length, fine, light brown hair and blue eyes. She wears prescription eyeglasses. Maria is the name on Masha's original and adopted birth certificates although she goes by Masha. According to sources at the agency that handled Masha's adoption from Russia, Masha is a variation of the name Maria, as Shelly is a name for Rochelle in the USA.

Masha has been in foster care in the USA since 5-03 and she was adjudicated dependent in 6-03. The CYFS goal for Masha was changed to adoption in 6-03.

**Residential Time Line**

<b>Dates</b>	<b>Resource</b>
8-25-92 to 1-31-97	birth mother/hospital in Russia
1-31-97 to 6-26-98	Russian orphanage
6-26-98 to 5-27-03	adopted father Matthew
5-27-03 to date	Families United Network foster home of Lynn Ginn

**C. HISTORY****Birth**

Masha was born in the Novoshakhtinsk District, Rostovskaya Region in the Republic of Russia. There is no information in the CYFS files regarding the details of Masha's birth although Masha advised that she believes she was born prematurely. Jeannine Smith of the Reaching Out Through International Adoption agency advised that her records from processing Masha's adoption from Russia show that Masha was born very prematurely and her birth weight was 900 grams. These records also indicate that Masha was the fourth pregnancy for her birth mother.

**Developmental**

There is no information in the files regarding Masha's developmental history.

**Social**

CYFS first became involved with this family in 5-03 when Masha's adopted father Matthew was arrested on charges related to child pornography. The court issued a finding of aggravated circumstances and there were no Family Service Plan Goals established for adopted father Matthew to work toward reunification with Masha.

A referral for Masha to again be adopted was made in 6-03.

**Abuse/Neglect**

Masha was subjected to physical maltreatment. Masha was subjected to sexual maltreatment and sexual exploitation beginning when she was around age 6 and continuing until 5-03. Masha has been reported to be very small for her age, possibly as a result of her having not received adequate nutrition.

**Residential History**

8-25-92 to 1-31-97

Masha is presumed to have been in the care of her birth mother for the first four years of her life. Masha's birth mother was reported to have stabbed Masha in the neck when Masha was around four or five years old and Masha bears a scar from this injury. Foster mother Ms. Ginn advised that she was told that Masha was hospitalized after having been stabbed in the neck by her birth mother and that Masha was placed in an orphanage when she was released from the hospital.

1-31-97 to 6-26-98

Masha lived in an orphanage in Russian for about eighteen months while agencies sought an adoptive home for her.

6-26-98 to 5-27-03

In 6-98 a divorced, retired American businessman named Matthew traveled to Russia and adopted Masha. Matthew brought his adopted daughter Masha to the Pittsburgh, PA area to live. Masha lived alone with her adopted father Matthew for almost five years. In 5-03 Matthew was arrested on charges related to child pornography and Masha was placed in foster care.

5-27-03 to date

Masha made a very good adjustment to her placement with her foster mother Lynn Ginn and she asked Ms. Ginn to adopt her. Ms. Ginn is planning to adopt Masha.

**Medical**

Health care is provided by Alma Illery Medical Center, 7227 Hamilton Avenue, Pittsburgh, PA 15208 and dental care is provided by Dr. Grimes, Mossie Boulevard, Monroeville, PA 15146.

Masha reported that she was hospitalized (in Russia) when she was around four years old but that she did not know the reason for this hospitalization. Foster mother Ms. Ginn advised that she was told that Masha was hospitalized after having been stabbed in the neck by her birth mother and that Masha was placed in an orphanage when she was released from the hospital.

Records from the agency that handled Masha's adoption indicate that Masha had chronic tonsillitis in 9-97 and that she was diagnosed with flat feet in 9-97. Masha also had a diagnosis of secondary cardiopathy (sic) in 1997. In 2-98 an oculist (an

optometrist or ophthalmologist) diagnosed Masha as having convergent comitant (sic) squint.

Masha wears prescription eyeglasses due to the condition of "lazy eye", a right esotropia. Vision care is provided by Pediatric Ophthalmology, Murrysville, PA 15668 and Masha had a prescription change to her eyeglasses in 9-03.

Masha underwent a medical assessment and consultation at Children's Hospital of Pittsburgh, 3705 Fifth Avenue, Pittsburgh, PA 15213 when she was first placed in foster care in 5-03. She was reported to be in good health aside from a low body mass index. Testing was conducted for various sexually transmittable diseases and there was a recommendation that Hepatitis B and C, RPR and HIV testing be conducted as soon as possible, that these tests be repeated in three months and a final repeat testing be performed in six months. Foster mother Ms. Ginn advised that as of 9-03 these tests had not been performed due to the difficulty she has had obtaining Masha's Social Security card and medical insurance verification but that she arranged to have this testing to take place on 9-23-03. The results of these tests were not available as of the date of this report.

In 6-03 Masha was noted to be about 15 pounds underweight and there was a recommendation that she be evaluated for an eating disorder. Foster mother Ms. Ginn advised that Masha was scheduled to undergo this evaluation on 9-23-03 with psychologist Dr. Patricia Pepe. The results of this evaluation were not available as of the date of this report.

Masha advised that when she goes swimming, she has a sensitivity to chlorine and that may have an allergy to chlorine.

Overall, Masha has enjoyed good health and there are no reports of any other medical issues or concerns.

Medical records show that Masha received the following immunizations and tests in Russia on the dates listed:

Pirket test: 4-20-93, 3-29-94, 5-24-95, 3-15-96, 4-17-97, 9-6-97 All results negative

Vaccination against tuberculosis (BCG) 4-20-92

Parotitis	11-30-93						
Polio	7-17-92	9-2-92	10-19-92	3-13-93	6-29-93	5-19-94	8-6-94
Diphtheria/ whooping cough	2-14-92	9-2-92	10-19-92	5-19-94			
HEPB	7-15-98						
Tetanus	9-23-93						

The record of Masha's immunizations in the U.S. was not in the CYFS files. Foster mother Ms. Ginn advised that as of 9-03 Masha's immunizations are up to date.

#### **Educational**

Masha attended Pivik Elementary School, 100 School Road, Plum, PA 15239 for kindergarten through fourth grade. In the fall 2003 Masha began to attend fifth grade at Mosside Middle School, 2609 Mosside Boulevard, Monroeville, PA 15146. She has done very well academically.

#### **Psychological/Psychiatric**

Records from the agency that handled Masha's adoption indicate that a Russian psychiatrist provided a diagnosis of astnic (sic) neurosis during 1997.

Masha has been described as a very affectionate, pleasant and well-mannered child who does not exhibit any behavioral problems.

Masha underwent an initial mental health evaluation through A Second Chance Wellness Center on 5-30-03. Dr. Sharon conducted this assessment and there was a recommendation that Masha undergo a psychiatric evaluation and attend therapy. The report from Dr. Sharon's evaluation was not in the CYFS files nor is there any documentation that these recommendations were followed.

Foster mother Ms. Ginn advised that Masha requested that she have a Christian therapist and that she attends counseling once per week at the Bethany Baptist Church.

There are no other reports of any psychological or psychiatric issues or concerns.

#### **D. CURRENT FUNCTIONING/RELATIONSHIPS**

Visits may be arranged with adopted maternal grandmother Ann if Ann and Masha wish to have visits. According to foster mother Ms. Ginn, Ann is to initiate arrangements for visits. Ms. Ginn advised that Ann has had only occasional contact with Masha since Masha's 5-03 placement in her care. Masha interacts well with her foster sister, ten-year-old Ashley, and they enjoy playing together.

Masha is a very pleasant, soft-spoken and intelligent youngster who quite readily engages in conversation. Masha said that she understood a lot more than people thought she did about her life. Masha said that she has had some very real dreams and, on occasion, she is not sure if things were real or dreams.

Masha likes attending school and her favorite subjects are reading and math. She enjoys reading books and some of her favorite books are the Harry Potter books, mysteries and chapter books.

Masha's favorite color is purple. Her favorite food is chocolate ice cream. Masha also likes to eat vegetables, spaghetti, rice, fish, hamburgers and French fries. Masha said that she knows how to cook eggs, spaghetti, sandwiches and soup in the microwave oven. Masha said that she does not like cheese, any sauces, cooked vegetables or pizza. Foster mother Ms. Ginn advised that Masha had not been exposed to a wide variety of foods while she was in the care of her adopted father Matthew and that Matthew had Masha on a restricted diet. Ms. Ginn has worked to introduce Masha to new foods.

Although Masha does not like to play sports, she enjoys playing catch with her foster sister, ten-year-old Ashley. Masha has an interest in gymnastics and would very much like to take gymnastics classes. She enjoys going to the park and playing on the swings and jumping rope.

Masha said that she would like to become a teacher, a doctor or a nurse when she is grown up.

Playing board games is a favorite pastime. Masha likes to play Bible Bingo, Full Armor of God and a nail polish board game.

Masha enjoys drawing, painting, sculpture and all kinds of crafts. She recollected that she had a box in her adopted father's home that she kept all of her art projects in. Masha's adopted father had given her his old digital camera and she enjoyed going outdoors to photograph nature, plants and animals. Masha said that she has taken some perfect pictures including a photograph of a butterfly that was in perfect focus and that this butterfly photograph was hanging in her adopted home.

Masha loves all kinds of animals but her favorite animal is a cat. She recollected that her adopted paternal aunt Mariangela used to have a pet motel and that she was allowed to walk the dogs that stayed there. Masha used to have a pet cat named Kitty. Foster mother Ms. Ginn is allergic to cats but she plans to allow Masha to have a pet cat when the family moves into a house and she plans to have the cat live in the basement.

Masha enjoys listening to music, singing and dancing. She would very much like to take dance lessons. Masha sings in her church choir and school chorus and she is to be a part of a performance on October 10, 2003 with the Pittsburgh Symphony. Masha likes music that has words and music, and other types such as orchestra music, that does not have words.

Masha enjoys watching the Disney and Nickelodeon channels on television and she likes all Disney movies.

On a typical weekday, Masha wakes up at 7:15 AM. She dresses, makes her bed, brushes her teeth and hair and gets ready for school. At 7:45 AM, Masha catches her bus for school. She eats breakfast at school. Masha arrives home from school at 3:10



PM. She says hello to whoever is at home, gives her foster mother Lynn a hug and checks to see what homework she has to do and does her homework. Masha watches television and plays with her foster sister Ashley when Ashley arrives home from school. Dinnertime is between 5:00 and 6:00 PM. Masha does the dishes and watches television after dinner. On Wednesday night, the family attends church. On other nights, Masha takes a shower between 7:00 and 8:00 PM and gets her clothes out for the next day. Masha's bedtime is 9:00 PM.

#### **Readiness for Adoption**

Adopted paternal grandmother Ann and Masha's adopted paternal aunt Mariangela were reported to have expressed some interest in obtaining custody of Masha, but Masha has told them that she wants to be adopted by her foster mother Ms. Ginn.

Masha developed a close attachment to her foster mother Lynn Ginn and Masha asked Ms. Ginn to adopt her. Masha appears to be very ready for adoption and Ms. Ginn is planning to adopt her. Masha addresses Ms. Ginn as Mumsy, a name she made up for Ms. Ginn.

### **E. BIRTH FAMILY INFORMATION**

#### **Birth Parents**

Masha's birth parents were reported to be alcoholics. There is no further information in the CYFS files regarding Masha's birth parents. Masha advised that her birth mother's name is Olga and that she had an older brother and an older sister. Masha believes that her birth mother had cancer and that she abused drugs and alcohol. She said that there is a box of information about her birth family at the home of her adopted father Matthew but efforts to retrieve this information were not successful.

#### **Adopted father**

Matthew was married to Doreen. They were separated by 1987 and subsequently divorced. Matthew and Doreen had a daughter named Rachel. Rachel lives out of the Pittsburgh area and has not had contact with her birth father Matthew for many years.

Matthew was employed as vice-president in a company affiliated with steel plants and, by the time he came to the attention of CYFS, he was retired from this position.

In 5-03 Matthew was incarcerated.

#### **Adopted father's attitude toward adoption**

Matthew is not expected to contest the adoption.

2-09

**Siblings**

Foster mother Lynn Ginn advised that she was informed that Masha's birth mother had three pregnancies before Masha was born but there is no information in the CYFS files regarding Masha's siblings. Masha advised that she has an older brother and an older sister and that she once knew their names but they were Russian names and she has forgotten them.

**F. SUMMARY**

Masha was reportedly placed in a Russian orphanage after suffering a stab wound inflicted by her birth mother. She was adopted from this Russian orphanage by an American man named Matthew. Family Through International Adoption in Cherry Hill, New Jersey handled this adoption. Masha was removed from the care of her adopted father Matthew after he was arrested and incarcerated in 5-03. Masha has lived with her foster mother Lynn Ginn since 5-03 and she asked Ms. Ginn to adopt her.

Masha wears prescription eyeglasses due to the condition of "lazy eye", a right esotrophia. Masha has a low body mass index and she was scheduled to undergo an evaluation in 9-03 to determine if she has an eating disorder. Masha is in need of testing for Hepatitis B and C, RPR and HIV that was recommended in 6-03. Masha was subjected to physical maltreatment, sexual maltreatment and sexual exploitation and possible inadequate nutrition. She has attended counseling.

Masha has an established bond with her foster mother Ms. Ginn and the adoption will provide permanency for Masha.

Submitted by MAC Human Resource Consulting, L.L.C., Michele A. Cunko, Principal, through Every Child, Inc. on October 7, 2003.

by Michele A. Cunko

Accepted by: \_\_\_\_\_

RESPONSE FOR THE RECORD BY FAITH ALLEN

*Faith Allen*

August 10, 2006

The Honorable Bart Stupak  
Ranking Member  
US House of Representatives  
Committee on Energy and Commerce  
Washington, DC 20515-6115

Re: Sexual Exploitation of Children Over the Internet Subcommittee Hearing  
Response to Additional Questions

Dear Congressman Stupak:

Thank you for inviting me and my daughter Masha to appear at the Subcommittee on Oversight and Investigation's May 3, 2006 hearing on the Sexual Exploitation of Children Over the Internet. We are heartened by your interest in and concern about this problem.

Here are the answers to your questions:

Question 1

In your daughter Masha's testimony, she mentioned that she had lost her Medicaid coverage recently. Frequently, adoptive parents of older children receive public assistance for medical and other care of those children until they are 18 years of age. Please describe whether you received any assistance from the States of Pennsylvania or Georgia to adopt Masha.

Answer 1

I did receive an adoption subsidy for Masha from the State of Pennsylvania which includes Medicaid. It has been difficult getting the same benefits in Georgia that I did in Pennsylvania since the subsidy is a Pennsylvania state subsidy which covers more things than Georgia.

There have also been problems getting and keeping Medicaid based on my inability to prove Masha's immigration status. When the FBI raided Matthew Mancuso's home they took everything, including documents about Masha's adoption and her Russian paperwork and US immigration papers. We really did not know what happened to Masha in terms of her adoption, including the agencies involved and information about her immigration, until our attorneys started investigating. The adoption agencies have refused to release anything about Masha's adoption to protect Mancuso's privacy. It is very difficult to get any public benefits, or even enroll Masha in school, without her social security card, immigration papers and other government and official documents.

Question 2

When a child has been abused as long and as severely as Masha, there are often medical and psychological conditions that require long-term treatment. What are the most significant challenges that you and Masha face? Do you have the financial resources for this treatment?

Answer 2

We have had a great deal of difficulty finding proper mental health treatment for Masha for two reasons. First is that Medicaid does not pay enough for most therapists and many therapists do not even take Medicaid. The second problem is that there are very few people able to treat a child like Masha with so many serious issues. Several providers have told me that they cannot handle a child with so many problems like Masha. Another issue is that there are very few therapists to begin with. And the therapists we have found who might help are hours from our home. We are considering relocating to be closer to the therapeutic help which Masha needs.

In terms of the money, if we can't find someone who takes Medicaid, the Pennsylvania victim's assistance program will pay up to \$10,000 lifetime for therapy. We are going to use that money, except they only provide reimbursement after we have spent the money. Masha does have a small trust which was ordered by the court for Mancuso to fund, but I am told by the person in charge of the money that they can only pay for education or the interest on the money which is not enough.

So we are frustrated that Mancuso, who is a millionaire, has done all this to Masha, is in prison at our expense probably for life, still has his millions and we are stuck with Medicaid, adoption agencies who are protecting HIM, no documents, and just scraping to get by. Even the victims of crime fund, which will give us something, will hardly pay for a year of Masha's treatment.

As a single working class mom who grew up in foster care, my financial resources will always be stretched. I just want and will do anything to get what is best for Masha. After everything she has survived, she really deserves the best treatment I can get for her.

Thank you for your interest in Masha and for all the help in passing Masha's law and making this such an important issue.

Sincerely,



Faith Allen  
Douglasville, Georgia

RESPONSE FOR THE RECORD BY RAUL ROLDAN, SECTION CHIEF, CYBER CRIME SECTION,  
CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF  
JUSTICE



**U.S. Department of Justice**  
Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

August 25, 2006

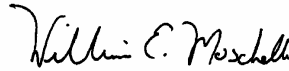
The Honorable Edward Whitfield  
Chairman  
Subcommittee on Oversight and Investigations  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

Attached are the responses to follow-up questions submitted to Mr. Raul Roldan, Section Chief, Cyber Crimes Section, Cyber Division, Federal Bureau of Investigation, U.S. Department of Justice, following the Subcommittee's May 3, 2006 oversight hearing entitled "Sexual Exploitation of Children Over the Internet: What Parents, Kids, and Congress Need to Know About Child Predators."

We hope that this information is helpful. Please do not hesitate to contact this office if we may be of further assistance.

Sincerely,

  
William E. Moschella  
Assistant Attorney General

Attachment

cc: The Honorable Bart Stupak  
Ranking Member

**Responses of the Federal Bureau of Investigation  
Based Upon the May 3, 2006 Hearing Before the  
House Committee on Energy and Commerce  
Subcommittee on Oversight and Investigations  
Regarding “Sexual Exploitation of Children Over the Internet”**

**Questions Posed by Congressman Stupak**

**1. In your testimony, you described in great detail a “typical sexual abuse website investigation” that appeared to involve the sale of child pornography. However, in numerous cases, such as the ones involving Matthew Mancuso and Alois Larry Wolk, and those described by members of the Internet Crimes against Children (ICAC) to the Committee at an earlier hearing, the focus of the investigation and the Federal search warrant was on the recipients or customers of child pornography images, not the website, itself. Often, there is no evidence of financial transactions among the participants.**

**Please describe a typical investigation in which a Federal Bureau of Investigation agent receives information that an individual is receiving, trading or purchasing child pornography on the Internet, as was the case with Matthew Mancuso.**

**Response:**

The FBI’s investigations of online child sexual exploitation are prioritized with the goal of having the greatest possible impact on the crime problem in light of finite resources. Our first priority is investigating online Electronic Groups (Egroups), web sites, and for-profit organizations that exploit children. Our second priority is to target the large-scale producers and manufacturers of child pornography. These crimes are serious because each individual image captures an act of sexual abuse against a child. Our third priority is “traveler” cases against individuals who indicate a willingness to travel interstate for the purpose of engaging in sexual activity with minors. “Travelers” also include individuals who entice, or attempt to entice, minors to travel interstate for that purpose. Our fourth priority is the possession of child pornography. Child pornography investigations that involve web sites as distribution mechanisms often yield thousands of subjects who fall into this category.

In addition to the website investigation discussed during the hearing, the FBI also investigates online child sexual exploitation in the peer-to-peer environment; this

includes chat rooms, file servers (Fservices), newsgroups, and Egroups. Although these investigations share similar aspects, each requires a different investigative approach.

The Mancuso investigation was the result of real-time law enforcement undercover activity. Mancuso engaged in a chat-room conversation with an undercover officer (UCO) whom he thought to be a like-minded person. During these conversations, Mancuso talked of his sexual desire for young children. Mancuso then provided an image of child sexual abuse to the UCO. Based on this transmission, the UCO was able to obtain an administrative subpoena for Mancuso's Internet protocol address to determine the origin of the image. Based on that information, the FBI's Pittsburgh field office obtained a search warrant for Mancuso's residence. During the execution of this search warrant, FBI agents found Masha Allen and learned from her that she had been the victim of continuous sexual abuse by Mancuso.

The Mancuso case provides an example of the FBI's use of undercover investigative techniques in online child sexual exploitation cases. The key to this case, and what makes the UCO investigative technique most effective, is the real-time communication between the offender and the UCO. Based on an offender's violation of federal law by transmitting or receiving child pornography, the FBI is able to obtain an administrative subpoena, attempting to accomplish this before the Internet service provider (ISP) destroys the information. Depending on the nature of the online dialog and the identification information provided by the ISP, the FBI may be able to obtain search and arrest warrants.

The FBI's use of UCOs posing as minors in chat rooms is another highly effective investigative technique. The FBI maintains a fairly constant covert online presence in various areas of the Internet to initiate cases of this type. During these investigations, pedophiles engage the UCO in sexually explicit conversations in the belief that they are talking to a child, and they often transmit pornographic materials as a means of lowering the "child's" inhibitions. These conversations and transmissions are recorded by the UCO. Because the pedophile's ultimate goal is to meet the child, these offenders often travel interstate and sometimes internationally. When the offender arrives, he is met by Federal agents and taken into custody.

The difference between the website investigation described during the hearing and a real-time investigation involving a UCO is the degree of impact the FBI can have on the overall crime problem. A web site investigation can potentially



identify thousands of pedophile-subscribers, derail and possibly ruin several for-profit mechanisms financing and otherwise supporting illegal enterprises, and most importantly, liberate numerous child victims from the exploitive and abusive situations ruining their lives. In contrast, a real-time undercover investigation will ordinarily result in the identification of one perpetrator and one child victim. Every day, the FBI employs investigative strategies and techniques designed to identify individual victims and to convict individual child sexual abuse offenders. In addition, resource limitations encourage the FBI to seek investigative vehicles that will contribute to the strategic goal of reducing the crime problem on the broadest possible scale. Web site investigations have proven to be effective and efficient in meeting this goal.

**2. You stated that a new national strategy established different priorities in the Cyber Crimes area. Please list the current priorities in order.**

**Response:**

The FBI Cyber Division's first priority is to safeguard our country's national security. Therefore, the Cyber Division's top investigative priority focuses on counterterrorism and counterintelligence matters, seeking to identify and neutralize the most significant individuals or groups conducting computer intrusions, disseminating malicious code, or otherwise threatening our national security interests. Our second priority is to identify and neutralize online predators or groups who sexually exploit and endanger children for personal or financial gain. Our third priority is to identify and neutralize operations targeting U.S. intellectual property, and our fourth priority is to identify and neutralize the most significant perpetrators of Internet fraud.

