AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

SEX CRIMES AND THE INTERNET

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 17, 2007

Serial No. 110–87

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

38–335 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SANCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

PERRY APELBAUM, *Staff Director and Chief Counsel*
JOSEPH GIBSON, *Minority Chief Counsel*

CONTENTS

OCTOBER 17, 2007

Page

OPENING STATEMENTS

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary 1
The Honorable J. Randy Forbes, a Representative in Congress from the State of Virginia, and Member, Committee on the Judiciary 1
The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Member, Committee on the Judiciary 2
The Honorable Ric Keller, a Representative in Congress from the State of Florida, and Member, Committee on the Judiciary 8

WITNESSES

Ms. Alicia Kozakiewicz
Oral Testimony 9
The Honorable Earl Pomeroy, a Representative in Congress from the State of North Dakota
Oral Testimony 13
Prepared Statement 15
The Honorable Nick Lampson, a Representative in Congress from the State of Texas
Oral Testimony 17
Prepared Statement 18
The Honorable Marilyn Musgrave, a Representative in Congress from the State of Colorado
Oral Testimony 19
Prepared Statement 21
The Honorable Christopher P. Carney, a Representative in Congress from the State of Pennsylvania
Oral Testimony 22
Prepared Statement 23
The Honorable Debbie Wasserman Schultz, a Representative in Congress from the State of Florida
Oral Testimony 23
Prepared Statement 25
The Honorable Cathy McMorris Rodgers, a Representative in Congress from the State of Washington
Oral Testimony 27
Prepared Statement 28
Mr. Michael A. Mason, Executive Assistant Director, FBI, Criminal, Cyber Response and Services Branch
Oral Testimony 30
Prepared Statement 32
Mr. Laurence E. Rothenberg, Deputy Assistant Attorney General, Office of Legal Policy, Department of Justice
Oral Testimony 35
Prepared Statement 37
Mr. Flint Waters, Wyoming Internet Crimes Against Children Task Force
Oral Testimony 44
Prepared Statement 46

Page

Ms. Michelle Collins, Director, Exploited Child Division, National Center for Missing and Exploited Children
Oral Testimony 61
Prepared Statement 62
Mr. Grier Weeks, Protect, Inc.
Oral Testimony 64
Prepared Statement 65
Mr. John Ryan, General Counsel, AOL
Oral Testimony 69
Prepared Statement 72
Ms. Elizabeth Banker, Assistant General Counsel, Yahoo
Oral Testimony 79
Prepared Statement 81

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Letter from Wayne Bowers, Board Member, Sex Abuse Treatment Alliance (SATA), dated October 16, 2007, to Rep. John Conyers 4
Article from *The New Jersey Star-Ledger,* dated August 14, 2005 105
Letter from the Honorable Joseph R. Biden, Jr., a U.S. Senator from the State of Delaware, to Robert F. Mueller, Federal Bureau of Investigation 118
Letter from James E. Finch, Assistant Director, Cyber Division, Federal Bureau of Investigation, to the Honorable Joseph R. Biden, Jr. 121

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Ranking Member, Committee on the Judiciary 135
Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary 136
Prepared Statement of the Honorable Steve Cohen, a Representative in Congress from the State of Tennessee, and Member, Committee on the Judiciary 137
Prepared Statement of Hemanshu Nigam, Chief Security Officer, Fox Interactive Media and MySpace 138

SEX CRIMES AND THE INTERNET

WEDNESDAY, OCTOBER 17, 2007

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 2:20 p.m., in Room 2141, Rayburn House Office Building, the Honorable John Conyers, Jr. (Chairman of the Committee) presiding.

Present: Representatives Conyers, Scott, Jackson Lee, Sánchez, Cohen, Johnson, Wasserman Schultz, Coble, Chabot, Lungren, Keller, and Forbes.

Staff Present: Perry Apelbaum, Staff Director and Chief Counsel; Mark Dubester, Majority Counsel; Joseph Gibson, Minority Chief Counsel; Michael Volkov, Minority Counsel; and Brandon Johns, Staff Assistant.

Mr. CONYERS. Good afternoon. Sorry for the delay.

The Committee will come to order.

Welcome, everyone. Without objection, the Chair is authorized to declare a recess of the Committee.

Today's hearing is on sex crimes and the Internet. The Internet has become a remarkable means of communication. It has also revolutionized commerce, the spread of information, but also unfortunately provides a venue for unscrupulous sexual predators to commit their crimes.

These predators use the Internet to infiltrate social networking sites to arrange meetings with minors where they use brute force to commit sexual offenses or worse. They use the Internet to join chatrooms and arrange sexual encounters with minors. They use the Internet to distribute images of child sexual exploitation and other child pornography.

So a goal of this hearing is to solicit input from all who are concerned about this issue, including my friends across the aisle, to make sure that any resulting legislation draws from all of the best ideas in strengthening the ability of the Federal and State law enforcement authorities to investigate and prosecute those who commit these kinds of crimes.

I am now pleased to recognize the Ranking minority Member of the Crime Subcommittee, the distinguished gentleman from Virginia, Mr. Randy Forbes.

Mr. FORBES. Thank you, Mr. Chairman.

Mr. Chairman, first, I would like to request unanimous consent to allow the statement of the Ranking Member Smith to be submitted.

Mr. CONYERS. Without, objection, so ordered.

Mr. FORBES. This is an important hearing.

Finally. The Judiciary Committee is finally focusing on a criminal justice issue of significant concern to the American public. The sexual offense epidemic in our country is well-documented. Each year an average of 366,000 individuals over the age of 12 are the victims of sexual offenses. It is estimated that nearly half of all of the sex offenders have attacked children under the age of 12. One in four women and one in seven men will be victims of sexual offenses in their lifetime.

The National Institute of Justice reported that rape costs $127 billion in victimization costs every year. But no statistic can truly capture the pain and suffering of the victims and their families.

The challenge is even greater when one considers the link between child pornography and sexual attacks on our children. We have seen an explosion of child pornography on the Internet. Offenders who possess or distribute child pornography are treated differently in our criminal justice system than those predators who prey on our children.

A recent study, the first in-depth survey of online sexual behavior, found that 85 percent of offenders who downloaded child pornography also committed acts of sexual abuse of children. The policy implications of this study are significant because they firmly link child pornography and sexual predators.

The challenge is for Federal, State and local law enforcement, legislators, and industry to work together even more than they have up to now to save children from these predators and to make the Internet safer.

The solutions require a combination of approaches. The Adam Walsh Act that we passed last Congress was an important step in the right direction. We need to continue this effort by using our common sense to protect the vulnerable and innocent children of our country from sexual predators, to provide law enforcement with the tools they need to protect our children, require the business community to cooperate with law enforcement when necessary, and make sure that the laws we pass are being carried out by the Justice Department and that judges are appropriately sentencing sex offenders.

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

Mr. CONYERS. I am now pleased to recognize the Chairman of the Crime Subcommittee, Mr. Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

I appreciate you holding this hearing on an important issue of sexual predators using the Internet for nefarious purposes. Protecting children from sexual predators is an important goal because the suffering caused by these crimes is a tragedy and we must do all we reasonably can to prevent such crimes.

However, even though these cases pull at our heart strings, that does not relieve us from the responsibility to legislate on a sound and effective basis.

There are many bills that have been introduced or will be introduced to require sex offenders to reregister their e-mail, instant message addresses, or types of Internet identifiers. The theory is with this information, law enforcement and others will be able to

track these offenders' e-mail activity. However, because of the nature of the Internet and the ease with which a person can create an online identity, it may be difficult, if not impossible, to keep track of a sex offender's e-mail traffic through this approach, such that all we will be doing is adding another charge that could be brought after the fact.

Furthermore, Mr. Chairman, the significant evidence is that of those who commit sex offenses using the Internet, only a negligible percentage are potentially subject to registration under any of the bills.

I would prefer that our attention be focused on efforts that are likely to reduce such offenses based on credible evidence. The evidence is that sex offender treatment programs will significantly reduce sex offender recidivism. Department of Justice figures indicate that 5 percent of sex offenders commit other sex crimes and that the recidivism rate for child molesters is about 3 percent within 3 years of release. That is compared to about 65 percent or more for other crimes.

Focusing resources on those who need treatment or other community assistance is far more likely to impact recidivism than relying on notions that we can track their Internet activity from a given e-mail address or other online identifier.

Of course where there are instances of offenses that are not being prosecuted through lack of staffing or other resources, such as apparently is the situation in peer-to-peer sharing of child pornography over the Internet, we should provide additional resources to not only prosecute such crimes but to also thwart attempts to commit them, and that would have a deterrent effect because people will know they are getting caught, which is right now not the case.

So, Mr. Chairman, I look forward to the testimony by witnesses on what we can do to actually address the problem of using the Internet to commit sex crimes against children and would ask unanimous consent, Mr. Chairman, that a letter to you from the Sex Abuse Treatment Alliance be entered in the record.

Mr. CONYERS. Without objection, so ordered.

[The information referred to follows:]

Oct. 16, 2007

Rep. John Conyers
2141 Rayburn House Office Building
Washington, DC 20515

Honorable Rep. Conyers:

Thank you very much for holding this hearing on Internet Sex Crimes. It is a complicated topic from a public health and criminal justice standpoint. Making the Internet a safer and more positive place to visit is the goal of all interested in prevention of sexual abuse.

Attached is a document that we wish to present to the House Judiciary Committee for consideration during your hearing and in research of this topic. The information has been compiled and submitted by a collective mind of a national coalition of advocates. Our organization is happy to join with this coalition in presenting the material to the committee.

A cross section of concerns and interest make up this coalition, including those who have been convicted of sex abuse or Internet charges, family and friends of those who have been convicted, victims who seek a more restorative approach to the issue, experts and citizens who wish to see a different approach.

Thank you again for addressing this issue. There are better ways to address this serious matter and our information, facts and research, if studied, shows present procedures are futile to the common good.

If there is a need for follow-up or discussion, please feel free to contact me at 405-639-7262.

Sincerely,

Wayne Bowers
Board Member

SEX ABUSE TREATMENT ALLIANCE
Programs: CURE-SORT • Communities of Concern
P.O. Box 761 Milwaukee, WI 53201-0761 • Phone: (517) 482-2085 • E-mail: sata@satasort.org • Web: www.satasort.org

Oct. 16, 2007

The laws governing sex offenses and sex offenders have resulted from myths and sound bytes. This committee must change direction seeking evidence based legislation.

1) Who is more likely to commit Internet Sex Crimes? (Registered offenders -or- someone not registered).

a) *Dateline's "To Catch a Predator" series*: Of the over 229 offenders who showed up or were prosecuted, *4 were registered sex offenders*, which is 1.7%.

b) *MySpace RSOs*: First 7,000 were removed, then 29,000 more Registered Sex Offenders (RSOs) were kicked off the MySpace social networking site. Following that, the Attorneys General from several states made a big to do over this, claiming they were possibly prowling for minors, and what did the AGs find? ***ONE RSO who had committed a MySpace type crime***; ONE! (http://tinyurl.com/2mxum5)

In reality what they found were RSOs who HAD ACCOUNTS on MySpace, and a few of them were on parole or probation, and had Internet restrictions. The fact that these supervised folks violated their supervised restrictions does not mean they committed an Internet Sex Crime, instead it was a TECHNICAL VIOLATION of Supervision; no crime.

c) *Newspaper reports of Internet crimes committed by public servants*: Currently we now have *stored over 145 cases of Internet Sex Crimes* that have been committed by folks who serve, or have served, the public in some capacity (/Crimes-Internet). (http://tinyurl.com/36g6zx)

In summary: Out of 36,229 RSOs only five committed an Internet Sex Crime. The recidivism percentage works out to .000138 or .0138%. That means legislation directed to registered sex offenders will do virtually nothing to address the over *99% of the predatory offenders who are committing Internet Sex Crimes*. Accordingly, these cases perpetrated by public servants, and those by recidivists, need to be addressed in legislation. Possibly through an enhanced graduated sentencing scheme.

2) Social Networking Website Act (New Legislation):

A) Congress needs to establish a new area of legislation, "The Social Networking Websites Act," (SNWA) and clearly define its limits and purpose; (Currently in society there are laws governing adult book stores and adult entertainment places.) Congress needs to enact SNWA likened to adult entertainment legislation to control SNW as to minors on their site:

B) Definitions:

i) "Social Network Website" (SNW) is a site which has a makeup similar to MySpace and operates as such, or is a site which permits a chat-room type conversation between two parties, or etc.,. (needs development)

ii) SNWs *do not include* sites such as News sites or blogs or other sites which would impede "Freedom of Speech," etc., and *are not covered by this SNWA* (Needs further development);

iii) Both SNWs and Chat-room only websites need to restrict minors to: 1) chat-rooms of just minors; 2) Accounts that are not publicly accessible but are accessible to other minors.

SEX ABUSE TREATMENT ALLIANCE
Programs: CURE-SORT • Communities of Concern
P.O. Box 761, Milwaukee, WI 53201-0761 • Phone: (517) 482-2085 • E-mail: sata@satasort.org • Web: www.satasort.org

C) Notifications to parents:

i) Require parents to approve their child's account, and notify them of their responsibility as to their child's actions;

b) Notify parents of the fines they will be subjected to if their child violates provisions: i.e., lying about age, etc. (Again needs further development)

3) Social Networking Website Operational Requirements:

A) Requirements as to SNW and minors on their website:

i) If a minor (person less than 18) sets up an account, it cannot be activated until a parent approves such. Parents would have to provide a valid credit card, or a driver's license as proof they approved of the account;

ii) Such minor accounts could not be accessed by adults (excepting the parents who have approved a minors account); minor accounts would be non public accounts automatically upon opening. They will only be accessible to other minor accounts;

iii) Minor accounts should be allowed to further restrict who they deal with. i.e., if there is someone they choose not to deal with and that person is a minor too, they should be allowed to stop contacts;

B) Social Networking Website Penalties:

i) If a minor is caught setting up an account as an adult (i.e., they lied about their age), the parents are reported to local police and they pay a fine; sort of a civil type penalty. That minor is then prevented from setting up another account for some period of time as a penalty to them.

ii) Social networking sites are fined for not following the law.

4) The Effects of current legislation runs contrary to public safety concerns:

a) Currently requiring RSOs to register e-mail addresses and other Internet ID's is a bootless exercise which shows Congress and State Legislators know little about how the Internet operates. e-mail addresses -if not used for a period of time- will become dormant and ISPs will -at some point, usually within a year- allow that e-mail address to be used by someone else. Hence, down the road -if a RSO registered that e-mail address, and someone else uses it in a manner prohibyted by law, then law enforcement will be arresting the wrong person. This causes a significant waste of law enforcement and the court's time and resources, and affect the RSO's arrest record.

b) The same is true of chat-room IDs, in fact, the same chat-room ID can be in use in hundreds of places around the world at the same time which could result in arresting the wrong person. i.e., the RSO who registered it when someone else is using the same chat-room ID in another chat-room

c) The stance that is being taken is to stop RSOs from participating in virtually all online activities. Current legislation tells ISPs and Social Networking sites to cut-off the RSO. This impedes the reentry of RSOs into the community by thwarting employment and educational opportunities, and affects the RSO's family as well. All this type of legislation makes RSOs and their families welfare recipients.

SEX ABUSE TREATMENT ALLIANCE
Programs: CURE-SORT • Communities of Concern
P.O. Box 761, Milwaukee, WI 53201-0761 • Phone: (517) 482-2085 • E-mail: sata@satasort.org • Web: www.satasort.org

d) Publishing RSOs' e-mail addresses, as well as other information, is causing them to be targets of hatred and they are being stalked harassed online and elsewhere. There are some who have been murdered!

5) Relevant studies for the committee to consider:

Very important to this committee is understanding the risks (sexual behaviors) today's youths engage in. The Center for disease Control's 2005 "Youth Risk Behavior Surveillance System" (YRBSS) (http://tinyurl.com/378o25) will show that 46.8% of students had had sexual intercourse during their life (Table 44). (pg-19). This must be considered when addressing youths on Social Networking Websites; unfortunately, today's youths are risk takers. (Additional information on YRBSS) (http://tinyurl.com/2m4jyy)

The following are relevant to Internet Sex Crimes. The committee should review them to filter out myths and misconceptions that prevail in the world of sex offenses and offenders. The more recent studies refute some of the findings of the older studies. Since the Internet is a constantly changing medium the Committee should place more reliance on the newer studies to debunk myths, sound bytes and factoids.

Teens and Online Stranger Contact (Pew / Internet & American Life Project), Oct. 2007 (http://tinyurl.com/2jnb3n)
Teens, Privacy & Online Social Networks: How teens manage their online identities and personal information in the age of MySpace (Pew / Internet & American Life Project), April 2007 (http://tinyurl.com/ysa4xy)

Internet Prevention Messages: Targeting the Right Online Behaviors, February 2007 (http://tinyurl.com/2zlbdg)

CREATING & CONNECTING // Research and Guidelines on Online Social — and Educational — Networking (National School Boards Association), July 2007 (http://tinyurl.com/2b327l) (*This study was comprised of three surveys: an online survey of 1,277 nine- to 17-year-old students, an online survey of 1,039 parents and telephone interviews with 250 school district leaders who make decisions on Internet policy.*)

Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study, May 2004 (http://tinyurl.com/yqectw)

Escaping or connecting? Characteristics of youth who form close online relationships, 2003 (http://tinyurl.com/26g4qr)

THE EXPOSURE OF YOUTH TO UNWANTED SEXUAL MATERIAL ON THE INTERNET: A National Survey of Risk, Impact, and Prevention (2003) (http://tinyurl.com/2cnp3g)

Internet Sex Crimes Against Minors: The Response of Law Enforcement, November 2003 (http://tinyurl.com/ywxgfh)

Internet Crimes Against Children (U.S Dep't of Justice) *December 2001 & 2005* (Youth Internet Safety Survey is included) (http://tinyurl.com/2z843e)
Just The Facts About Online Youth Victimization: (http://tinyurl.com/yq66s7) Researchers Present the Facts and Debunk Myths (Transcript), (http://tinyurl.com/ywuq7z) May 2007, this updates the 2000 "Online Victimization" report below.
Online Victimization: (http://tinyurl.com/28kqpw) A Report on the Nation's Youth (Crimes Against Children Research Center), June 2000

This is presented by the collective mind of a National Coalition of Advocates.
(All links were shortened using TinyURL.com http://tinyurl.com/)

SEX ABUSE TREATMENT ALLIANCE
Programs: CURE-SORT • Communities of Concern
P.O. Box 761, Milwaukee, WI 53201-0761 • Phone: (517) 482-2085 • E-mail: sata@satasort.org • Web: www.satasort.org

Mr. SCOTT. I want to site two statistics out of this. The first is that Dateline's "To Catch a Predator" series of over 229 offenders who showed up or were prosecuted, four were registered sex offenders, which is 1.7 percent. The other is out of 36,229 registered sex offenders, only five committed an Internet sex crime, and that works out to a percentage of 0.138 of a percent.

That means well over 99 percent of the predatory offenders who are committing Internet sex crimes would not be affected by this legislation.

Thank you, Mr. Chairman.

I yield back.

Mr. CONYERS. I thank the gentleman and recognize the distinguished gentleman from Florida, Mr. Rick Keller.

Mr. KELLER. Thank you very much, Mr. Chairman, for recognizing me, and I also want to especially thank you for holding this important hearing on sex crimes and the Internet.

The bottom line is that online child predators must be captured, prosecuted and locked away. The television show, Dateline's "To Catch a Predator," has raised public awareness about the seriousness of the problem we have in this country right now with online predators. Specifically, it shows us the problem we have with predators who communicate online with the child or someone who they believe to be a child and then travel to meet that person for the purpose of sexually abusing him or her.

It also shows us the problem we have with something called grooming, a behavior where predators pretend to be younger than they are and lie about their age in order to entice their victims. Currently, Florida is the only State in the Nation which has a law specifically targeting the criminal practice of grooming. I think that is an important issue to address, and, in fact, I will be introducing legislation with my colleagues on that issue.

I do have optimism that this is an issue that we can do something about.

On Monday, I joined with the Florida Attorney General Bill McCollum to cut the ribbon on the Child Predator Cyber Crime Unit in my hometown of Orlando which is staffed with six full-time employees who sit there much like on the TV show "To Catch a Predator" and coordinate with investigators, police officers and prosecutors to go out and capture the worse abusers.

This problem is so bad that all of us on both sides of the aisle need to drop what we are doing and address it. Seventy-seven million children in this country use the Internet daily, and one out of seven children in America between the ages of 10 and 17 are sexually solicited on line.

It is clearly a problem worthy of this important hearing, and I want to especially thank our witnesses, the Members of Congress, who have taken the time to draft thoughtful legislation and will be testifying today. And also I want to especially thank the second panel who will be made up of a broad cross-section of experts because we look very much forward to hearing your ideas.

And, Mr. Chairman, I will yield back the balance of my time.

Mr. CONYERS. I thank you very much, Mr. Keller.

And of course we will receive all other opening statements of Members.

We have two panels today plus a very important and distinguished speaker.

Our first speaker is Alicia Kozakiewicz. This brave young woman will describe her own personal experience with the issues that we consider today.

And I thank my colleagues, particularly the Ranking Member from Texas, Mr. Smith, for permitting us to call her out of turn because of her time schedule. She must leave immediately upon completing her testimony.

And there are several House Members who have introduced legislation on this issue who have agreed to briefly testify about their bills. We don't expect them to respond to questions, though they may be asked to answer written questions that will be submitted.

We will conclude with another panel from law enforcement and from the Internet provider industry.

Our lead-off witness can give a real voice to what this issue is all about, and I welcome her to the Committee. She is here today not only as a survivor, but she is sure to warn others of the dangers of the Internet to help us protect our kids.

Welcome to our hearing, and I would invite you to give us your testimony at this point.

TESTIMONY OF ALICIA KOZAKIEWICZ

Ms. KOZAKIEWICZ. Thank you, Mr. Chairman.

Hello. Thank you for inviting me to speak today.

My name is Alicia Kozakiewicz, a Pittsburgh resident. I am 19 years old and a sophomore in college. And for the benefit of those of you who don't know, don't remember those headlines, I am that 13-year-old girl who was lured by an Internet predator, transported across State lines to Virginia, in fact, not so very far from here, and enslaved by a sadistic pedophile monster.

The authorities told my parents that the odds were a million to one against my recovery. But I was the exception. I got the miracle. I was rescued.

So why me? Because I was blessed by the simple fact that I live in Pittsburgh, where one of the very best cyber crime task forces was created, and because I was enslaved in Virginia, where one of the best Internet Crimes Against Children taskforces, or ICAC, exists. Because they had the training, the knowledge and the expertise to find that needle in the haystack. That was—I was a lost little girl. That was me. Because they had the cooperation of another fine ICAC team here in Virginia, because they were there, I am here. They are the only reason that I am here in front of you today.

But I want you to know that I am not up here alone. Beside me there are so many young girls whose stories will never be heard because they are dead, possibly enslaved or just too terrified to speak out.

When I speak, what I say is for all of us who exist in pain and fear and sometimes even shame and for those of us who have been silenced by the grave.

So I guess you need to know how it happened, and why I let it happen to me. I want you to stop thinking that right now. I was a young girl and just because someone leaves without a struggle

doesn't mean that they left willingly. It has been 5 years, and I have just begun to answer that question myself.

I know that many of you perceive that those of us who have been lured via the Internet as being the stereotypical wild child, drugs, broken families, searching for love you can't find at home. Nothing could be further from the truth. Many of us were the shy children, the wallflowers, not necessarily the geeks or the freaks, just not the partiers, and sometimes, as in my case, those that were very shy.

The Internet provides a type of anonymity that allows a timid child to miraculously transform themselves. They are suddenly able to act without the fears that have constricted their daily lives. Take myself for an example.

So in an attempt to impart some clarity here, let me start at the beginning. Pick a teenage girl, any one of us, and we will be suffering agonies over at least one and probably more of these situations:

Imagine your 13th birthday was last month and for some ridiculous reason your parents still think you are a child. You are sitting home bored and lonely because your best friend decided that you are not so cool anymore and your other best friend has moved far away. That person you have an unbelievable crush on, they think you are the biggest geek. You have a D in algebra despite your best efforts and you won't be making the honor roll this semester. And nobody understands anything at all, nobody ever will. You are alone in this world and you are so bored, so lonely that you are online just chatting.

So let me start closer to the beginning. I was 13. I was a good student. I had a few good friends. I had the most wonderful, loving and supportive family a child could ever ask for, and yet at 13 we change. We question everything, especially ourselves. I was that typical bored, shy and lonely child just looking for something to do.

In the beginning, I chatted for months with Christeen, a beautiful red haired 14-year-old girl who just understood me all too well. We became the very best of friends. And we shared all of our thoughts, all of our intimate girlhood secrets. There was nothing that she didn't know about me, and we traded our school pictures.

Too bad that hers were fake. Yeah. Christeen was really a middle-aged pervert named John. And he had lots of practice at his little masquerade because he had it all down, the abbreviations, the music, the slang, the clothes. He knew it all. I never had a chance because these perverts, they congregate on the Internet. They pass their little girlfriends around to each other, and they share techniques and they boast in their conquests. John/Christeen was to introduce me to a great friend of hers. This man was to be my abductor, my torturer, and he was my dearest friend.

My relationship on line with Tyree grew slowly, over a period of about 6 months. He was courteous and interesting and subtle. He was thoughtful and gentle and nice, and of course entirely deceptive, and so we became friends.

Slowly and perceptively, he led me into more intimate conversations. I never even realized that our chats had become more intimate. So we just talked about everything. Not just about sex. He was interested in me as a person. My thoughts, my goals, my rela-

tionship with friends and family members. He gave me adult advice and always took my side, and 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 are not, and my family and I were very close but we didn't always see eye to eye about everything. Sometimes we just seemed to still think that I was still a child, but there was always my secret special friend, and I could count on him to see things my way.

He was my confidant, and I wanted to tell him personal things or parrot those things that they wanted to hear from me, whatever gibberish they were. And so I did. Always online, always ready to talk, always on my side. It was the most comforting thing imaginable, and soon I felt an obligation to return this time, to always be there for him to the exclusion of everything else.

He became that someone I believed I needed, the only one I could depend on to understand the real me. He had separated me from my support structures. I was alone.

Somehow in this process of grooming me, he had changed me. How he destroyed my ability of reason? Was I crazy? No. Was I brain washed? Entirely. Today I think, how could it have happened? What was my reason? Where was my sanity?

That girl who walked out into the coldest, iciest night of the year to meet the madman, that wasn't me, and yet somehow it was.

He took me apart and put me back together, and bit by bit, day by day, byte by byte.

I walked out the front door and found that the boogeyman is real and he lives on the Web. I know. I met him on the evening of January 1, 2002. He came for a 13-year old girl for a sex slave. He came for me.

Let me share these next words with you. I think they may be what you need to know to understand.

Imagine, it is below zero as you make your coatless way out the front door to meet this madman that you think is your friend. Maybe at this point you are afraid. Maybe there is something wrong here, but you can't stop yourself. So maybe you will think the game is over. When you get to the bottom of your driveway and you stand there shivering, cowering behind a bush on a dark night, the falling crystals sting your face, just curious to see if he will really show up. You are not really going to leave with him. Probably you won't even reveal yourself to him.

But he is your friend, your best friend. Maybe you will just be polite and say hi. But then somehow wait a minute, you don't remember walking over to the car, do you? And yet suddenly you are in the car, terrified, and he is grabbing on to your hand and crushing it and you cry out but there is no one to hear. And you know this is not your friend. It is some crazy, fat pervert who threatens to put you in the trunk if you make another noise, give him any trouble. So you stay quiet, real quiet.

And somehow you survive the long terrifying ride to the unknown. Each moment you get further away from your home from everyone who loves you, who might have saved you. You realize that you are about to die horribly. And you know on some level that there is only you now. You are totally alone, and you know if you want to live he has to believe that you will do anything for

him. And you decide that you will, that you are going to survive this no matter what it takes.

So you try to memorize road signs but nothing registers. You can't concentrate past the blinding fear. The signs on the road, no hope there. Where am I, you cry silently to yourself, and then hours later, eternities later, you arrive.

He opens the door, warning you yet again but somehow the words don't seem to make sense. They float into the air disappearing one by one as his fat sweaty hands holds tightly squeezing your hand as you stumble through this door, through the house and down, down into his basement. His disgusting dungeon.

Cold dark walls filled with nasty sex toys and a cage. Over the next days, he will use many of them on you. And between the beatings and the rapings, he will hang you by your arms while beating you, and he will share his prized pictures with his friends over the Internet.

He will attach clamps to your body, and he will use them to send bolts of electricity into your body. He will beat and overpower you and crush you as he violates every inch of your 90-pound body.

When he is finished with his fun, he will place a collar around your neck and attach a huge heavy chain to prevent your escape, and you know he will kill you if he even thinks you want to leave. So you wait and you pray.

And in your dreams, you begin to see that cold shallow grave waiting for your little lifeless body, and you cry silently, mommy, daddy, I am here. Please find me.

The last morning as he left for the office he grabbed my face and looking deep in my eyes he said, I think I am getting to like you a little too much. When I come home, we are going for a ride.

This was the 21st day that he had held me. My last meal I thought. And I knew that I would die today. Mommy, daddy, please hurry, I prayed.

I laid there crying holding his kitten, my tears wetting her fur waiting for death when I suddenly heard the loudest crash. Voices screaming, we have guns. We have guns. And dragging a heavy chain behind me as I huddled underneath the bed, terrified as the men swarmed the house, I saw the most beautiful letters in the alphabet: FBI, in bold yellow on the backs of their jackets, and I knew that I was safe, and that my prayers had been answered.

An agent covered my nakedness with a coat and cut the collar from my neck and took me from that evil house. The FBI, the ICAT, they are my angels. I like to say that they could walk on water, but they don't need to. Angels have wings.

I spent a lifetime in that house.

A year after my rescue, the Detective, Jim More, who had escorted the child that was me from that horror, drove me back to the house. It sits in a friendly little street, quietly cheerfully yellow. I walked up to the squeaky clean basement windows, the ones that had been painted black so that no passerby could peer in and stop his little games, and I see a toy. A playroom. And I stumble. I cry inside. I am mourning for the child that was me, the child that was stolen from me. And make no mistake, that child was murdered. I know that some parts of me are there forever; the

child I was is still chained in that room still suffering. And I am still trying to set her free and others like me.

This is why I am a psychology major and why my concentration is in forensics. My ultimate career goal is to become a part of the ICAT forces to rescue a child and help to recover its soul because even though I have been rescued, I fear that I will never be recovered.

Please support Congresswoman Debbie Wasserman Schultz's bill and Senator Joseph Biden's companion bill, S. 1738. Support the children. Save us from pedophiles, the pornographers, the monsters.

The boogeyman is real, and he lives on the Internet. He lived in my computer, and he lives in yours. While we are sitting here, he is at home with your children. ICAC has forces all over this country and are poised to capture him to put him in that prison cell with the man that hurt me.

They can do it. They want to do it. Don't you?

Thank you.

Mr. CONYERS. Thank you, Ms. Kozakiewicz. Your testimony is inspirational and moving, and it will guide us as we move forward. I commend you for your unique bravery and obviously the determination to use your experience to make sure that what happened to you will not happen to anyone else.

Thank you so much for joining us. The struggle continues, and the Committee will still be in touch with you, and we hope to be working forward in a rational way to put this problem on a national level and in perspective so that we can solve it.

Thank you very much for coming. And because of your time considerations, we will excuse you at this time.

Thank you.

Oh, and that is your mother besides you?

Mrs. KOZAHIEWICZ. It is.

Mr. CONYERS. Thank you for being here as well, ma'am.

Could I call the members of the panel forward?

Earl Pomeroy, Nick Lampson, Marilyn Musgrave, Chris Carney, Debbie Wasserman Schultz, Member of the Committee, Cathy McMorris-Rodgers. We thank you all for being here.

Earl Pomeroy of North Dakota will begin. He has played a leading role in both the enactment of the Adam Walsh Child Safety Protection Act, and the creation of the National Sex Offender Register, named in honor of a North Dakota student who was murdered by a repeat sex offender.

He has also worked closely with i-SAFE, prevention-oriented Internet safety awareness program.

I welcome all of my distinguished colleagues and ask Earl Pomeroy to begin when he is ready.

TESTIMONY OF THE HONORABLE EARL POMEROY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH DAKOTA

Mr. POMEROY. Mr. Chairman, thank you very much.

Today is my daughter's 14th birthday, and after hearing that last witness, I agree with you, Mr. Chairman, it was deeply moving testimony. We need to find a way to rationally protect our children.

Mr. Chairman, Ranking Member Smith and Members of the Committee, thank you for inviting me to join you to discuss efforts to strengthen our laws in ways that will help protect children from being exploited by sexual predators on the Internet.

Earlier this session, our departed friend Paul Gillmor and I introduced Keeping the Internet Devoid of Sexual Predators Act, the KIDS Act of 2007. The legislation addresses the threat of dangerous sex predators on the Internet by making it more difficult for convicted sex offenders to use social Internet working sites.

Under the legislation, convicted sex offenders would have to register online identifiers, such as e-mail, domain names, Internet instant messaging addresses, and that will become part of the National Sex Offender Registry.

These online identifiers would not be released to the public. They don't need the mail harassment or the kinds of things that might come if they were publicly released, but they would be made available to social networking sites, and these sites could choose to block the sex offenders from using those services, online social networking sites like MySpace, Facebook, Friendster, that are designed to help people keep in touch with old friends, make new ones.

Unfortunately, these sites and other sites that host chatrooms, like Yahoo, AOL, Google, are also places where sexual predators can exploit young people, find out personal information about potential victims.

Just last year in my home State of North Dakota, a Bismarck man was charged and convicted for luring a minor with a computer. According to the criminal complaint, he engaged in sexual talk in a chatroom with a 16-year-old girl and tried repeatedly to get her to meet him. Fortunately, in that case the father intervened and put a stop to it. Of course as we heard testimony today, that is not always the case.

Now one of these sites, MySpace, has done something pretty extraordinary to protect the young people using that site. They painstakingly created their own database from various State sex offender registries to find high risk sex offenders that were utilizing the MySpace network.

Using this data, MySpace has recently removed the profiles of 29,000 registered sex offenders, 10 profiles from North Dakota. They should be commended for taking this action on MySpace. It has been difficult. It has been expensive. It has not been without controversy. But as a parent of teenager, I and many others applaud their action and we hope others follow this.

But we ought to make it easier. Social networking sites are only able to use the information about a convicted sex offender's physical attributes and locations to remove these individuals because there is no mechanism to gain access to their online identifiers. By requiring sex offenders to register their e-mail addresses, the legislation will help social networking sites prevent convicted sex offenders from registering for their services as well as identify those convicted sex offenders who may currently be using their services.

Basically we are asking the Committee to consider this a balancing of the interest, the strong public interest in protecting the young people using these social networking sites versus the access

right of a high-risk convicted sex offender to use, to access that site. In this balancing, we believe the balance strongly comes down in favor of protecting the juveniles using these sites.

There is a second feature of the KIDS Act. It involves shamefully lying about one's age for purposes of establishing a sexual relationship with a minor. We are seeing sex predators increasingly using the anonymous nature of the Internet to pose as children, gain their trust, and engage in this process called grooming. But we believe that someone engaging in this kind of deception ought to face criminal penalty, and we have one in the bill.

This bill is identical to Senate legislation introduced by Senator Schumer from New York and Senator McCain from Arizona. It has received support from several organizations: MySpace, Boy Club, Girl Club, National Center for exploited children, Enough is Enough, a nonprofit that works for keeping kids safe online, the National Association of School Resource Officers. Eleven States have taken this action.

But I think we all understand this isn't a state-by-state issue. It is a national issue, and it needs this legislation. The Internet is truly transformational technology, 21 million kids on it every day.

So I believe that this bill, the KIDS Act, H.R. 719, is a fair and reasonable response to secure our children's safety. If Paul Gillmor was with us today, he would be right here with me testifying as well.

We urge you to favorably consider this legislation.

Thank you for your time.

[The prepared statement of Mr. Pomeroy follows:]

PREPARED STATEMENT OF THE HONORABLE EARL POMEROY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH DAKOTA

Mr. Chairman, Ranking Member Smith, and members of the Committee, thank you for inviting me to join you to discuss efforts to strengthen our laws in ways that will help protect children from being exploited by sexual predators through the Internet.

Earlier this session, our departed friend Rep. Paul Gillmor (R-OH) and I introduced the "Keeping the Internet Devoid of Sexual Predators Act of 2007" known as the KIDS Act of 2007. This legislation addresses the threat of dangerous sex predators on the Internet by making it more difficult for convicted sex offenders to use social networking sites. Under this legislation, convicted sex offenders would have to register online identifiers, such as e-mail and instant message addresses, which would become part of the National Sex Offender Registry. While these online identifiers would not be released to the general public, this information would be made available to social networking sites which could choose to block sex offenders from using their services.

Online social networking sites like MySpace, Facebook, and Friendster are designed to help people keep in touch with old friends and to meet new ones. Unfortunately, these sites and sites that host chat rooms like Yahoo, AOL and Google are also places where sexual predators can exploit young people and find personal information about potential victims. Just last year in my home state of North Dakota, a Bismarck man was charged and convicted for luring a minor with a computer. According to the criminal complaint, he engaged in sexual talk in a chat room with a 16-year-old-girl and tried repeatedly to get her to meet him. He was finally caught after the girl's father contacted the police. While this father was able to discover that someone was preying on his daughter online, parents are not always able to monitor their child's online communications in time to prevent terrible tragedies from occurring.

One of these sites, MySpace, has taken extraordinary measures to proactively address this threat to the young people using their site. They painstakingly created a database from various state sex offender registries to find high risk convicted sex offenders who were utilizing the MySpace network. Using this data, MySpace has

recently removed the profiles of 29,000 registered sex offenders, including 10 profiles of North Dakota residents. MySpace should be commended for taking this action. It has been difficult, expensive and not without controversy. As the parent of a teenager, however, I and many others applaud their actions and hope other follow.

The reality is, however, that MySpace and other social networking sites and chatrooms need our help. Currently, social networking sites like MySpace are only able to use information about convicted sex offender's physical attributes and locations in order to remove these individuals because there is no mechanism for these sites to gain access to their online identifiers. By requiring convicted sex offenders to register their email addresses and other online identifiers, this legislation will help social networking sites prevent convicted sex offenders from registering for their services as well as identify those convicted sex offenders who may currently be using their services. Additionally, this legislation would provide criminal penalties of up to 10 years for those convicted sex offenders who try to get around these protections by lying about their online identifiers.

A second feature of the KIDS Act addresses the shameful scam of lying about one's age for purposes of establishing an illegal sexual relationship with a minor. Increasingly, child predators are using the anonymous nature of the Internet to pose as children online in order to gain the trust of a child. Alarming, nearly one in eight youth ages 8-18 discovered that someone they were communicating with online was an adult pretending to be much younger. This is shameful and unacceptable. The KIDS Act of 2007 would target this type of a behavior by making it a crime for an adult to lie about their age with the intent to solicit a minor for sexual purposes.

This common-sense bill is identical to bipartisan legislation introduced by Senators Chuck Schumer (D-NY) and John McCain (R-AZ), and I thank them for their important leadership on keeping our kids safe. It has received support from several organizations interested in Internet safety including MySpace; the Boys and Girls Clubs of America; the National Center for Missing and Exploited Children; Enough Is Enough, a non-profit that works on protecting kids online; and the National Association of School Resource Officers.

Since the introduction of the KIDS Act of 2007, eleven states including Arizona, Colorado, Connecticut, Florida, Illinois, Kansas, Kentucky, Louisiana, Mississippi, Oklahoma, and Virginia have passed similar legislation requiring sex offenders to register their online identifiers. Moreover, nearly a dozen other states are currently considering similar legislation to protect our children from sexual predators on the Internet. The reality is, however, this isn't a state issue—it's an issue for all of us. We need to make certain all of the country is making the effort to keep convicted high risk offenders off these social networking sites.

The Internet is truly transformational technology that over 21 million teens—87% of kids across the nation—take advantage of everyday. Unfortunately, law enforcement and law makers have not been able to keep up with those who would abuse this technology. It is critically important that Congress update our laws to keep our children safe. I believe that H.R. 719 is a fair and reasonable response to further secure our children's safety, and I would deeply appreciate your assistance in moving legislation on this issue through the Committee and to the floor of the House of Representatives. I appreciate the Committee's full and fair consideration of this bill and I thank you for your attention to this important matter.

Mr. CONYERS. Thank you for getting us off on this discussion.

The gentleman from Texas, Nick Lampson, was just in his first term in 1997 and a family in his district suffered a horrible crime.

I will let him tell you about it. But Nick Lampson responded by establishing the Congressional Missing and Exploited Children's Caucus, of which many of us are members, just about an equal number of Republicans and Democrats, over 130 members. He has been recognized by John Walsh, host of America's Most Wanted and the National Center for Missing and Exploited Children, for his work to protect kids.

And I invite him to share his thoughts on this subject with us this afternoon.

Welcome, Nick.

TESTIMONY OF THE HONORABLE NICK LAMPSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. LAMPSON. Thank you. It is a pleasure to be here, Chairman Conyers, Ranking Member Forbes, distinguished Members of the Committee.

I thank you for calling this hearing to order, and I thank you for inviting me to testify this afternoon on obviously a critically important issue.

The stories of Internet predators praying on innocents making their way into our children's bedrooms with a simple click of a mouse are seen and heard too often in our media. The age of sweet 16 used to be about parties and learning to drive, but now it marks the threshold of Internet freedom. Popular social Internet working Web sites allow profiles to be public, providing predators with an encyclopedia with pictures and even addresses which they can use to cause harm.

This dangerous trend has become a feeding ground for pedophiles and for convicted sex offenders. Parents, law enforcement and legislation must work together to bring social networking Web sites into the fight to protect America's children.

And I have joined with one of my distinguished colleagues, Congressman Steve Chabot—he is also cochair of the Congressional Caucus on Missing and Exploited Children—in introducing the Securing Adolescents From Exploitation online, the SAFE Act of 2007.

The SAFE Act provides increased resources for law enforcement to capture and to prosecute and to incarcerate these criminals. By expanding the system for service providers to report child pornography found on their systems, we improve child safety and prevent future atrocities.

Currently, Internet providers are mandated to report child pornography to the National Center for Missing and Exploited Children. Under the SAFE Act, all electronic service communications providers and remote computing service providers will have to report child pornography. And for knowingly or willingly not filing a report after being made aware of a child pornography image, these providers will be subjected to fines of $150,000 per image per day for the first offense and up to $300,000 per image per day for any image found thereafter.

Over 10 years ago, Mr. Chairman, as you just stated, I founded the bipartisan Caucus on Missing and Exploited Children after a young girl was abducted and murdered in my district. They found her body in pieces in a drainage ditch. It was a horrendous thing to have happen, and it was an even worse part to play in being there with her family at the time that that discovery was made.

And since then, I have continued to work extensively with organizations such as the National Center for Missing and Exploited Children on educating Members of Congress and others on legislation such as the SAFE Act that strengthens the national center's ability to keep children safer online and on our streets.

The SAFE Act provides limited immunity for electronic providers and social networking Web sites to send images of Internet child pornography to the national center's CyberTipline, and this bill will also increase the efficiency of the tip line, making it a better inves-

tigative tool for law enforcement by mandating that all information submitted by providers is consistent. The process outlined in this bill keeps law enforcement officials in the loop by making information more readily accessible and requires providers to retain key data that law enforcement agencies can use to investigate and prosecute child predators.

Many of us have watched Dateline's popular series, "To Catch a Predator," and organizations such as Perverted Justice that actively look for Internet child predators. We need to become partners in this fight by talking to our kids about the dangers of strangers online and making Internet use a family activity.

While parents should teach their children that the Internet offers many different types of resources, from education to entertainment, it also poses many risks. Parents are the first line of defense against online predators, and the SAFE Act will enforce their efforts.

Internet companies will need to do their part also. When we begin to hold Web sites accountable for the images they host, we have taken the first step towards supporting parents in their efforts to protect children.

Our combined efforts will make the Internet a safe place.

So, Mr. Chairman and the Committee, thank you very much for calling this hearing to order. I appreciate your good work.

[The prepared statement of Mr. Lampson follows:]

PREPARED STATEMENT OF THE HONORABLE NICK LAMPSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Thank you, Mr. Chairman for calling this hearing to order. And thank you for inviting me to testify this afternoon on this critically important topic.

Stories of Internet predators preying on innocence, making their way into our children's bedrooms with the simple click of a mouse are seen and heard too often in the media. The age of sweet sixteen used to be about parties and learning to drive, but now it marks the threshold of Internet freedom. Popular social networking websites allow profiles to be public—providing predators with an encyclopedia of pictures, personal interests, and even addresses, which they can use to cause harm.

This dangerous trend has become a feeding ground for pedophiles and convicted sex offenders. Parents, law enforcement and legislators must work together to bring social networking websites into the fight to protect America's children.

I've joined with one of my co-chairs of the Congressional Missing and Exploited Children's Caucus, Congressman Steve Chabot, in introducing the Securing Adolescents From Exploitation-Online (SAFE) Act of 2007. The SAFE Act provides increased resources for law enforcement to capture and prosecute and incarcerate these criminals. By expanding the system for service providers to report child pornography found on their systems, we improve child safety and prevent future atrocities.

Currently Internet service providers are mandated to report child pornography to the National Center for Missing & Exploited Children. Under the SAFE Act, all electronic service communications providers and remote computing service providers will have to report child pornography. For knowingly and willingly not filing a report after being made aware of a child pornography image, these providers will be subject to increased fines of $150,000 per image per day for the first offense, and up to $300,000 for any image found thereafter.

Over 10 years ago I created the bipartisan Congressional Missing and Exploited Children's Caucus after a young girl was kidnapped and murdered in my district. Since, I have continued to work extensively with organizations such as the National Center for Missing & Exploited Children on educating Members of Congress and others on legislation such as the SAFE Act that strengthen the National Center's ability to keep children safer online and on our streets. The SAFE Act provides limited immunity for electronic service providers and social networking websites to send images of Internet child pornography to the National Center's CyberTipline.

This bill will also increase the efficiency of the CyberTipline, making it a better investigative tool for law enforcement by mandating that all information submitted by providers is consistent. The process outlined in this bill keeps law enforcement officials in the loop by making information more readily accessible, and requires providers to retain key data that law enforcement agencies can use to investigate and prosecute child predators.

Many of us have watched Dateline's popular series "To Catch a Predator," and organizations such as Perverted Justice that actively look for Internet child predators. We need to become partners in this fight by talking to our kids about the dangers of strangers online and making Internet use a family activity. While parents should teach their children that the Internet offers many different types of resources—from entertainment to educational—it also poses many risks. Parents are the first line of defense against online predators and the SAFE Act will reinforce their efforts.

Internet companies will need to do their part too. When we begin to hold websites accountable for the images they host, we've taken the first step toward supporting parents in their efforts to protect children. Our combined efforts will help make the Internet a safer place.

Thank you again, Mr. Chairman, for calling this hearing to order.

Mr. CONYERS. We appreciate your experience and your leadership in this subject matter.

I am now pleased to call Congresswoman Marilyn Musgrave of Colorado.

TESTIMONY OF THE HONORABLE MARILYN MUSGRAVE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. MUSGRAVE. Thank you, Mr. Chairman, and thank you, Ranking Member Forbes, and distinguished Members of the Committee.

You know, in the years that I have been in Congress and in the State legislature in Colorado, I have heard some difficult testimony, testimony that was very hard as we took in the information. And I believe the testimony of this young woman today was—I mean as a mother and a grandmother, it is just amazing to me that—"heinous" does not describe the crimes that are being perpetrated on our children. So I thank you for holding this hearing today.

The Internet has become a virtual playground for sexual predators and pedophiles who satiate their desire for child pornography with relative anonymity. Pedophiles can download images to their personal computers or, even worse, watch the sexual abuse of children in real-time.

Child pornography consists of more than just pictures, visual depictions of children in suggestive poses. Rather, child pornography involves the rape, abuse, and molestation of innocent children, in some cases even involving infants as young as 3 months old.

The National Center for Missing and Exploited Children CyberTipline receives reports of suspected Internet child pornography every day. Since its launch in 1998, the tip line has received nearly half a million child pornography reports, averaging almost over 1,400 tips per week.

Child pornography is a profitable global criminal enterprise, and it is growing rapidly in technical sophistication in response to efforts to detect and disrupt these criminal operations.

Child pornography is not even a crime in more than half of the 84 Interpol countries. Unfortunately, this means that many of the

children victimized by child pornography are foreign and not protected by the laws of their country.

My legislation makes important improvements to Federal law to help eliminate child pornography. Most importantly, the bill prohibits the access of child pornography.

Although current law prohibits the possession, trafficking or transport of child pornography, a person who uses a computer who knowingly accesses child pornography intending to view it and who then views that child pornography can arguably avoid criminal liability as long as he or she does not download or print the images. The law must be amended to ensure that these offenders do not escape liability because of technicalities in the law, and this is something that my bill does.

My legislation would make it a crime to knowingly access child pornography. My legislation also imposes mandatory penalties for possession of child pornography, increases civil penalties for Internet service providers who fail to report child pornography to law enforcement and provides mandatory restitution for child pornography victims.

Currently, the penalty for sexual exploitation and possession of child pornography is a maximum of 10 years in prison. My bill would change this to make it a minimum of 2 years and a maximum of 15 years.

Current law requires Internet service providers who knowingly and willfully fail to report such violations to 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. My bill 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.

In addition, the legislation would add civil fines for negligent failure to report a child pornography offense. The civil penalty is set at $50,000 for the initial violation and $100,000 for each subsequent violation.

The Federal Communications Commission would be provided with the authority to levy the civil fines under this section and to make the necessary regulations in consultations with the Attorney General in order to carry the fines into effect and to provide an appropriate administrative review process.

The restitution requirements in my bill would require offenders to pay the full amount to the victims—of the victim's losses, which could include medical services, therapy, and necessary transportation for treatment or care as a result of the offense, lost income, attorney's fees and any other losses as determined by the court.

Another very important step my legislation takes is amending the definition of "illicit sexual conduct." The definition of "illicit sexual conduct" for purposes of the sex tourism statutes is too narrow. It does not encompass a sex tourist who either travels for the purpose of producing child pornography or who produces child pornography in a foreign place or persons who facilitate that travel for financial gain. My legislation would amend the definition of "illicit sexual conduct" by adding production of child pornography to the definition.

The Internet is an excellent resource for advancing communications, education and business. However, the ready access to explicit content, including child pornography, is dangerous to our children and harmful to society. It is our responsibility to protect children from becoming victims and better policing illegal content on the Internet is one way we can do this.

I applaud the Committee for taking up this important issue, and I thank you again for your time.

[The prepared statement of Ms. Musgrave follows:]

PREPARED STATEMENT OF THE HONORABLE MARILYN MUSGRAVE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CIOLORADO

Good afternoon Chairman Conyers and Ranking Member Smith. Thank you for holding a hearing on this very important topic. I appreciate the opportunity to testify about my bill, H.R. 3148, the Child Pornography Elimination Act of 2007.

The Internet has become a virtual playground for sexual predators and pedophiles who satiate their desire for child pornography with relative anonymity. Pedophiles can download images to their personal computers or, even worse, watch the sexual abuse of children in real-time.

Child pornography consists of more than just visual depictions of children in suggestive poses; rather, child pornography specifically involves the rape, abuse and molestation of innocent children, some cases even involving infants as young as three months old.

The National Center for Missing and Exploited Children CyberTipline receives reports of suspected Internet child pornography every day. Since its launch in 1998, the tipline has received nearly half a million child pornography reports, averaging almost 1,400 tips each week.

Child pornography is a profitable, global criminal enterprise, and is growing rapidly in technical sophistication in response to efforts to detect and disrupt these criminal operations. Child pornography is not even a crime in more than half of the 184 Interpol countries. Unfortunately, this means that many of the children victimized by child pornography are foreign and not protected by the laws of their country.

My legislation makes important improvements to federal law to help eliminate child pornography. Most importantly, the bill prohibits the access of child pornography.

Although current law prohibits the possession, trafficking, or transport of child pornography, a person who uses a computer to knowingly access child pornography intending to view it, and who then views that child pornography, can arguably avoid criminal liability as long as he or she does not download or print the images. The law must be amended to ensure that these offenders do not escape liability because of technicality in the law, and this is something my bill does. It will criminalize the knowing access of child pornography.

My legislation also imposes mandatory penalties for possession of child pornography, increases civil penalties for Internet Service Providers who fail to report child pornography to law enforcement, and provides mandatory restitution for child pornography victims.

Currently, the penalty for sexual exploitation and possession of child pornography is a maximum of 10 years in prison; my bill would change this to make it a minimum of 2 years and a maximum of 15 years.

Current law requires Internet Service Providers who knowingly and willfully fail to report such violations to 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. My bill 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.

In addition, the legislation would add civil fines for negligent failure to report a child pornography offense. The civil penalty is set at $50,000 for the initial violation and $100,000 for each subsequent violation. The Federal Communications Commission would be provided with the authority to levy the civil fines under this section and to make the necessary regulations, in consultation with the Attorney General, in order to carry the fines into effect and to provide an appropriate administrative review process.

The restitution requirements in my bill would require offenders to pay the full amount of the victim's[1] losses which could include: medical services, therapy, and necessary transportation as a result of the offense, lost income, attorney's fees, and any other losses as determined by the court.

Another very important step my legislation takes is amending the definition of "illicit sexual conduct." The definition of "illicit sexual conduct" for purposes of the sex tourism statutes is too narrow because it does not encompass a sex tourist who either travels for the purpose of producing child pornography or who produces child pornography in a foreign place or persons who facilitate that travel for financial gain. My legislation would amend the definition of "illicit sexual conduct" by adding "production of child pornography" to the definition.

The Internet is an excellent resource for advancing communications, education and business. However, the ready access to explicit content, including child pornography, is dangerous to our children and society. It is our responsibility to protect children from becoming victims, and better policing illegal content on the Internet is one way we can do this.

I applaud the Committee for taking up this important issue and I thank you for your time.

Mr. CONYERS. Thank you.

I failed to note that you were serving your second term as policy chair for the Western Caucus and served with great distinction as Ranking Member on the House Subcommittee on Specialty Courts.

Again, your concern is evident by your statement.

We welcome now the gentleman from Pennsylvania, Chris Carney, a political science professor at Penn State University who, ever since he got here, has made the issue of child protection one of his top priorities in the Congress.

We are very pleased to have you this afternoon and invite you to make your testimony.

TESTIMONY OF THE HONORABLE CHRISTOPHER P. CARNEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

Mr. CARNEY. Thank you for holding this important hearing regarding sex crimes and the Internet.

Congressman Chabot and I have introduced bipartisan legislation as the Responsible and Effective Solutions for Children Entering Online Services Act of 2007, or RESCUE Online Services Act of 2007 for short.

This legislation will allow the National Center for Missing and Exploited Children to share information and material related to child pornography with service and technology providers.

This will assist in the development of technology to thwart pornography distribution, especially child pornography distribution. The Rescue Online Services Act of 2007 will allow the National Center for Missing and Exploited Children to forward incidents to foreign law enforcement agencies as well.

It will enhance the quality and detail of information provided to the NCMEC by enabling early preservation of evidence at the point of referral, and this is critical to be able to capture the online signatures so we can capture the perpetrators.

---

[1] The term 'victim' means the individual harmed as a result of a commission of a crime under this chapter, including, in the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, the legal guardian of the victim or representative of the victim's estate, another family member, or any other person appointed as suitable by the court, but in no event shall the defendant be named as such representative or guardian.

As a father of five, I strongly feel we need to do more to protect our children from online predators. My children spend hours a week online, and of course we cannot always be over their shoulder watching what they are doing.

This is why Congressman Chabot and I are working in a bipartisan manner, and with the support of online industries we will accomplish our goal: protecting our children. This is a protection we owe to kids nationwide.

I want to thank you, sir, for this opportunity to contribute to today's hearing.

As a father and a Representative of Pennsylvania's 10th Congressional District, I look forward to working with this Committee in supporting the protection of children from online predators.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Carney follows:]

PREPARED STATEMENT OF THE HONORABLE CHRISTOPHER P. CARNEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

Thank you, Chairman Conyers and Ranking Member Smith for holding this important hearing regarding sex crimes and the internet.

Congressman Chabot and I have introduced bipartisan legislation known as the Responsible and Effective Solutions for Children Entering Online Services Act of 2007 or RESCUE Online Services Act of 2007 for short.

This legislation will allow The National Center for Missing and Exploited Children to share information and material related to child pornography with service and technology providers. This will assist in the development of technologies to thwart child pornography distribution.

The RESCUE Online Services Act of 2007 will allow the National Center for Missing and Exploited Children to forward incidents to foreign law enforcement agencies.

It will enhance the quality and detail of information provided to the National Center for Missing and Exploited Children by enabling early preservation of evidence at the point of referral.

As a father of five, I strongly feel we need to do more to protect our children from online predators. This is why Congressman Chabot and I are working in a bipartisan manner, and with the support of online industries to accomplish our goal of protecting our children. We owe this protection to our children.

Thank you for the opportunity to contribute to today's hearing. As a father of five, I look forward to working with this committee in support of protecting our children from online predators.

Mr. CONYERS. Thank you, Congressman Carney.

Debbie Wasserman Schultz is in the Judiciary Committee hearing room here, 2141, a great deal of the time. We welcome the gentlelady from Florida as a witness for a change, and her sustained commitment to this subject matter is very, very appreciated.

This summer she vigorously questioned the Federal Bureau of Investigation Director Mueller as to the FBI's attention to how they are fighting sex crimes, and I am not at all surprised that she would be with us in this capacity today.

And Ms. Wasserman Schultz, we welcome you to your own Committee.

TESTIMONY OF THE HONORABLE DEBBIE WASSERMAN SCHULTZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Ms. WASSERMAN SCHULTZ. Thank you, Mr. Chairman. Mr. Chairman, I might borrow an extra 45 seconds that Congressman Car-

ney left on the table. So I hope that is okay, and I appreciate the opportunity to testify.

Mr. CONYERS. You probably won't need it.

Ms. WASSERMAN SCHULTZ. I talk pretty fast.

Ranking Member Forbes, Chairman Conyers, my distinguished colleagues of the Judiciary Committee and fellow panelists, you know, sometimes the problems we face as a Congress are extremely complex, and other times the solutions are simple and right in front of our eyes. As you will hear today, there is no mystery about what we need to do now to save thousands of children from sexual abuse and exploitation.

In the last Congress our colleague and friend Joe Barton, then the Chairman of the Energy and Commerce Committee, conducted a series of hearings on this topic. Not only did those hearings expose the dearth of Federal resources devoted to investigating and prosecuting child exploitation crimes, but they also brought together an extraordinary group of parents who formed an organization called the Surviving Parents Coalition. In June of this year, I was visited by this very special group of parents.

When I sat down with Mark Lunsford, Erin Runnion, Ed Smart, Mark Klaas, Mary Kozakiewicz, and other founders of the Surviving Parents Coalition, I was not prepared for what they had to tell me. They shared with me their own horrific stories of how their children were abducted by sexual predators. As you know, some of these children will never come home. As the mother of three young children myself, their stories broke my heart. And as a Member of Congress, I felt compelled to act.

What surprised me most about these brave parents was their message about child pornography and child exploitation. What they said was this: If you want to prevent predators from hurting other children like ours, the way to do that is go back through the Internet and get them. Most children who are victims of sexual abuse are not abducted by strangers. They are violated by adults they know and often trust, including family members.

But as we learned yesterday, with the apprehension of a predator in Las Vegas, Nevada, for the first time we have the technology and the evidence not only to find these predators, we have the technology to find their victims, too.

This week Congressman Barton and I introduced H.R. 3845, a bipartisan bill called the Protect Our Children Act of 2007. This bill addresses an issue that Speaker Pelosi has dedicated her speakership to, and one that should be at the top of our agenda, the protection of children.

Our children deserve a future that is healthy, prosperous, bright, and safe. But our children are vulnerable on the Internet. The Internet has facilitated an exploding multi-billion dollar market for child pornography. The demand in this market can only be supplied by new images, and these images can only be supplied through the sexual assault of more children.

A 2005 Justice Department study found that 80 percent of child pornography possessors had images and videos of children being sexually penetrated. Another 21 percent possessed images of bondage, sadistic abuse, and torture. The children depicted in these photos are very young. Eighty-three percent of child pornography

possessors have images of children younger than 12 years old, and another 19 percent possess images of infants and toddlers, as Congresswoman Musgrave mentioned. There are even Web sites that provide live pay-per-view rape of very young children.

Let me be clear. This is not about obscenity or pornography. These images are crime scene photos created by a thriving industry that uses children as sexual commodities.

Later in this hearing we will hear from Special Agent Flint Waters of the Wyoming State Police, a highly respected child exploitation investigator. His research established that right now there are nearly 500,000 identified individuals in the United States trafficking child pornography on the Internet. Law enforcement knows who they are and they know where they are. What shocked me most and what compelled me to get involved in this issue is that due to a lack of resources, law enforcement is investigating less than 2 percent of these known 500,000 individuals. Even more shocking is that it is estimated that if we were to investigate these cases we could actually rescue child victims nearly 30 percent of the time.

We need a national campaign. That means the full weight of law enforcement, the National Center for Missing and Exploited Children, Congress, the executive branch, parents and victims advocacy groups, and Internet service providers with us in the fight.

Alicia Kozakiewicz is a living reminder of the lives we can save. She is not a victim; she is a survivor.

The Protect Our Children Act will help provide the safety net we so desperately need by creating statutory authority for these highly successful Internet Crimes Against Children task forces which support State and local law enforcement agencies that investigate child exploitation. It will supplement this local effort with hundreds of new Federal agents who will be solely dedicated to crimes against children. It will also provide desperately needed forensic and computer labs so we can lift the digital fingerprints of these perpetrators and bring them to justice, as well as a special council within the Department of Justice to be created to plan and coordinate child exploitation prosecution efforts.

I want to remind you about a conversation I had with FBI Director Mueller at an oversight hearing in this Committee in July. I asked him how many agents were dedicated exclusively to child exploitation. His answer was 242. 242. I asked him how many agents were dedicated exclusively to investigating white collar crime, and the answer was 2,342. Although he said child exploitation was a substantial priority, he also said that there were too many competing priorities. The time has come to reorder priorities at the Department of Justice, and the Protect Our Children Act will do just that. We must prevent predators from hurting our children.

It is a privilege to serve on this Committee, Mr. Chairman. Thank you very much.

[The prepared statement of Ms. Wasserman Schultz follows:]

PREPARED STATEMENT OF THE HONORABLE DEBBIE WASSERMAN SCHULTZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA, AND MEMBER, COMMITTEE ON THE JUDICIARY

Chairman Conyers, Ranking Member Smith, distinguished colleagues of the Judiciary Committee, and fellow panelists:

Thank you for the opportunity to appear before you today. It feels strange to be on this side of the dais, but I am grateful that you extended the invitation to me to testify about an issue I care deeply about—an issue I know is troubling to us all—the explosion of child pornography on the Internet and the horrific abuse that too many of our children suffer, at the hands of child sexual predators.

Sometimes the problems we face as a Congress are extremely complex. Other times, the solutions are simple and right in front of our eyes. As you will hear today, there is no mystery about what we need to do—NOW—to save thousands of children from sexual abuse and exploitation.

In the last Congress, our colleague and friend Joe Barton, then the Chairman of the Energy and Commerce Committee, conducted a series of hearings on this topic. Not only did those hearings expose the dearth of federal resources devoted to investigating and prosecuting child exploitation crimes, but they also brought together an extraordinary group of parents who formed an organization called the Surviving Parents Coalition.

In June of this year I was visited by this very special group of parents. When I sat down with Mark Lunsford, Erin Runnion, Ed Smart, Marc Klaas, Mary Kozakiewicz and other founders of the Surviving Parents Coalition, I was not prepared for what they had to tell me. They shared with me their own horrific stories of how their children were abducted by sexual predators. As you know, some of these children will never come home. As the mother of three young children, their stories broke my heart. But as a Member of Congress, I felt compelled to act. What surprised me most about these brave parents was their message about child pornography and child exploitation. What they said was this: if you want to prevent predators from hurting other children like ours, the way to do that is to go back through the Internet and get them.

Most children who are victims of sexual abuse are not abducted by strangers. They are violated by adults they know and often trust, including family members. Tens of thousands of these children are prisoners in their own homes or keeping a dark secret from those who could protect them. But, as we learned yesterday with the apprehension of a predator in Las Vegas, Nevada, for the first time, we have the technology and the evidence not only to find these predators—we have the technology to find their victims, too.

This week, Congressman Barton and I introduced H.R. 3845, a bipartisan bill called "The PROTECT Our Children Act of 2007." The PROTECT Our Children Act is the kind of legislation that reminds us of why we enter public service and the moral responsibility we often have as we shape our nation's laws. The bill addresses an issue that Speaker Pelosi has dedicated her Speakership to and one that should be at the top of our agenda: the protection of children. Our children deserve a future that's healthy, prosperous, bright and SAFE!

But our children are not safe when they are online. The Internet has facilitated an exploding, multi-billion dollar market for child pornography. The demand in this market can only be supplied by new images, and these images can only be supplied through the sexual assault of more children.

A 2005 Justice Department study found that 80 percent of child pornography possessors have images and videos of children being sexually penetrated. Another 21 percent possess images of bondage, sadistic abuse and torture. The children depicted in these photos are very young: 83 percent of child pornography possessors have images of children between the ages of 6 and 12, and another 19 percent possess images of infants and toddlers. There are even websites that provide live "pay-per-view" rape of very young children.

Let me be clear: This is not about "obscenity" or "pornography." These images are crime scene photos—created by a thriving industry that uses children as sexual commodities. This is a human rights issue.

Later in this hearing we will hear from Special Agent Flint Waters of the Wyoming State Police—one of the most renowned and highly respected investigators on child exploitation today and the driving force behind the Internet Crimes Against Children Data Network. His research established that right now there are nearly 350,000 identified individuals in the United States trafficking child pornography on the Internet. That's 350,000 people, right here, in the United States, buying, swapping, selling, and sharing the kinds of images I just described. Law enforcement knows who they are, and they know WHERE they are.

But what shocked me, and what compelled me to get involved in this issue, is that due to a lack of resources, law enforcement is investigating less than two percent of these known 350,000 individuals. Less than two percent!

Even more shocking is that it is estimated that if we were to investigate these cases, we could actually rescue child victims nearly 30 percent of the time. Research shows that more than half of child pornography possessors have also sexually as-

saulted or attempted to sexually assault children. Because child pornography prosecutions also have extremely high success rates, a national campaign against those who create, possess, and traffic in child pornography is the best way to prevent future sexual abuse. And we need the full weight of law enforcement, the National Center for Missing and Exploited Children, Congress, the Executive branch, parents and victims' advocacy groups, and Internet service providers with us in the fight.

The Protect Our Children Act will help provide the safety net we so desperately need, by creating statutory authority for these highly successful ICAC Task Forces, which support state and local law enforcement agencies that investigate child exploitation. It will supplement this local effort with hundreds of new federal agents from the FBI and Immigration and Customs Enforcement that will be solely dedicated to crimes against children. It will provide desperately needed forensic crime and computer labs so we can lift the digital fingerprints of these perpetrators and bring them to justice. It will create a Special Counsel within the Department of Justice to not only plan and coordinate child exploitation prosecution efforts, but who will also be responsible for achieving results.

I want to leave you with a conversation I had with FBI Director Mueller at an Oversight Hearing in this Committee in July. I asked him how many agents were dedicated exclusively to child exploitation. The answer was 242. I asked him how many agents were dedicated exclusively to investigating white-collar crime. The answer was 2,342. Although he said child exploitation was a "substantial priority," he also said that there were too many "competing priorities." The time has come to reorder priorities at the Department of Justice, and the PROTECT Our Children Act will do just that.

Colleagues, the status quo is unaccepatable. Our mandate here is clear: if we want to prevent predators from hurting our children, we must not only provide federal, state, and local law enforcement the resources they need to go back through the Internet and get them—we must also re-order priorities at the Justice Department.

Again, thank you for the opportunity to testify this afternoon. It is an honor to serve on this committee and to come before you.

Mr. CONYERS. And you are on the right Committee to make sure that the Department reorders its priorities. You have been doing this these last several months. I congratulate you.

Ms. WASSERMAN SCHULTZ. Thank you very much.

Mr. CONYERS. Finally, last, not least, is the congressional co-chair of the Women's Caucus, Cathy McMorris Rodgers of Washington. And we are delighted to have you. With your permission, we are going to excuse any of the Members. We have enough time to take her testimony. There are three votes on the floor. And we will resume as soon as those votes are concluded.

We welcome you, Ms. Rodgers.

TESTIMONY OF THE HONORABLE CATHY McMORRIS RODGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

Mrs. MCMORRIS RODGERS. Absolutely. Thank you, Mr. Chairman, Ranking Members Forbes, Members of the Committee. And I just join in being honored to be with you today. We have heard some compelling testimony, beginning with Alicia, as well as my fellow panelists, and I appreciate the chance to testify.

As many of you know, I became a mom for the first time this year, and it has become more important to me than ever that I do everything possible to protect my son and, like any parent, protect kids from those who would do him and others harm.

This year I was also introduced to social networking sites like MySpace and Facebook, and while intended mainly for high school students and college students, these sites, as we are all becoming aware, are being used by sexual predators as a way to prey on innocent children. As was mentioned earlier by Congressman Pom-

eroy, it has been reported in the press that MySpace.com has identified and taken action now on more than 29,000 registered sex offenders, and we applaud them for their efforts.

Today in America one in five children between the ages of 10 and 17 will receive a sexual solicitation online during their lifetime. The FBI estimates there are as many as 50,000 child predators prowling the Internet. The Internet has unfortunately become an easy avenue for predators to find unsuspecting victims. And that is why I have introduced legislation, the Sex Offender Internet Prohibition Act of 2007, which imposes mandatory penalties for individuals who are required to register as a sex offender and knowingly access a Web site with the intent to communicate with an unsuspecting child. This bill sends a clear message to sex offenders that if they use the Internet sites to contact children they will go to jail.

Just a few days after I introduced this legislation, police in Peachtree, Georgia, arrested a 28-year-old man for exchanging sexually explicit e-mails and online chats with a 14-year-old girl in Liberty Lake, Washington, a city in my district. Nearly 4,200 children in Spokane County were victims of physical abuse and sexual abuse or neglect in 2005. We must not only focus on keeping children safe from strangers they meet on the street, but protecting them from strangers they meet online.

I would like to take a minute to commend Washington State Attorney General, Rob McKenna, for his work on this issue and for putting together a Youth Internet Safety Task Force, focusing on keeping the Internet safe for our kids. The goal of the task force is to address issues of online predation, while at the same time devising ways to combat the proliferation of child pornography, and ultimately sexual exploitation and victimization of children.

Finally, I thank the Committee for the opportunity to testify. I am pleased that the Committee is holding this hearing today on an important component of our efforts to reduce crime and keep our communities safe.

[The prepared statement of Ms. McMorris Rodgers follows:]

PREPARED STATEMENT OF THE HONORABLE CATHY MCMORRIS RODGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

This year, as many of you know, I became a mom and it is important for me to keep my child safe as he grows up and protect him from anyone who would do him harm. Every parent has this wish.

This year I was also introduced to social networking sites like MySpace and Facebook. And while intended mainly for high school and college students, these sites are now being used by sexual predators as a way to prey on innocent children.

In fact, an Associated Press story recently reported that MySpace.com has identified more *than 29,000 registered sex offenders* with profiles—more than four times the number cited by the company two months ago. Today, 1 in 5 children between the ages of 10 and 17 will receive a sexual solicitation online during their lifetime. The FBI estimates that as many as 50,000 child predators are prowling the Internet.

The Internet has unfortunately become an easy avenue for predators to find unsuspecting victims. That is why I have introduced legislation, the *Sex Offender Internet Prohibition Act of 2007,* which imposes mandatory penalties (5-10 yeas in prison) for individuals who are required to register as a sex offender and knowingly access a website with the intent to communicate with an unsuspecting child. This bill sends a clear message to sex offenders that if they use these Internet sites to contact children they will go to jail.

In fact, a few days after I introduced the legislation police in Peachtree, George arrested a 28-year-old man for exchanging sexually explicit emails and online chats with a 14-year-old girl in Liberty Lake, Washington a city in my district. Nearly 4,200 children in Spokane County were victims of physical abuse, sexual abuse or neglect in 2005. We must not only focus on keeping children safe from strangers they meet on the street, but protecting them from strangers they meet online.

I would like to take a minute to commend Washington State Attorney General Rob McKenna for his work on this issue and for putting together a Youth Internet Safety Task Force focused on keeping the Internet safe for our kids. The goal of the Task Force is to address issues of online predation while at the same time devising ways to combat the proliferation of child pornography and ultimately the sexual exploitation and victimization of children.

Finally, I would like to thank the Committee for the opportunity to testify. I am pleased that the Committee is holding this hearing today as an important component of our efforts to reduce crime and keep our communities safe.

Mr. CONYERS. Thank you so much, everyone. We have another panel, and we are called to the floor. And we will resume as soon as those votes are disposed of. And I thank you, Mr. Forbes.

[Recess.]

Mr. SCOTT. [Presiding.] The Committee will come to order. We will now hear from our witnesses.

Our first witness will be Michael Mason, Executive Assistant Director of the Criminal, Cyber Response, and Services Branch of the FBI. Since arriving at the FBI in 1985, he has worked in five FBI field divisions, worked as an undercover agent, and served on a SWAT team. He has served as Special Agent in Charge for the Sacramento field office, and as Assistant Director in Charge of the Washington field office, the FBI's second largest office.

In his current position he oversees the Criminal Investigative Division, Cyber Division, Office of International Operations, Office of Law Enforcement Coordination, and the Critical Incident Response Group.

Our second witness will be Laurence Rothenberg, who is Deputy Assistant Attorney General of the Department of Justice's Office of Legal Policy, where his responsibilities include helping develop the Department's legal policy regarding child exploitation and obscenity, violence against women, and trafficking in persons, among other issues.

Next witness will be Special Agent Flint Waters, team leader for the Wyoming Internet Crimes Against Children Task Force, and lead developer of a task force data network. His work has led to the arrest of hundreds of Internet sex offenders around the world.

Next will be Michelle Collins, Director of Exploited Children at the National Center for Missing and Exploited Children. Among her responsibilities, she directly oversees the Nation's CyberTipline, a congressionally-mandated recipient of reports on child exploitation for the public and all U.S.-based electronic service providers. She has published numerous articles on child sexual exploitation, and has helped coordinate 25 international law enforcement agencies for Operation Web Sweep, a worldwide child pornography sting conducted by the New Jersey Division of Criminal Justice.

Our next witness will be Grier Weeks, the Executive Director of the National Association to Protect Children, a nonpartisan organization with members in 50 States. In 2002, Mr. Weeks was instrumental in bringing together national experts on child protection

with political veterans to form Protect, a pro-child, anti-crime lobby focused exclusively on child protection. Since 2002, Protect has worked in a dozen State legislatures and nationally to win stronger child protection laws.

Next we will hear from John Ryan, Chief Counsel to America Online, Incorporated. He heads the Compliance and Investigations Department, where he is responsible for the development and implementation of policies and processes to combat illegal activities on AOL services. He serves as the liaison with law enforcement to coordinate investigations and prosecutions of criminal activities, including offenses against minors, and serves as a board member at the National Center for Missing and Exploited Children.

Our last witness will be Elizabeth Banker, Vice President and Associate General Counsel for Compliance at Yahoo, Incorporated. She manages the global law enforcement compliance function, and her team advises the company on child protection, information security, and related compliance issues. She is on the board of directors of the U.S. Internet Service Providers Association. She recently served on the Virginia Attorney General's Youth Internet Safety Task Force.

So we will begin with Mr. Mason.

TESTIMONY OF MICHAEL A. MASON, EXECUTIVE ASSISTANT DIRECTOR, FBI, CRIMINAL, CYBER RESPONSE AND SERVICES BRANCH

Mr. MASON. Good afternoon, Mr. Chairman, Ranking Member Forbes and Members of the Committee. I would like to thank you for the opportunity to discuss the FBI's role in combating the sexual exploitation of children through the use of the Internet.

With more than one billion people around the world routinely online, the Internet has become an integral part of our daily lives. It has dramatically enhanced the way we communicate, the way we learn, and the way we work. Today I want to talk about what the FBI is doing to attack child exploitation on the Internet. I want to briefly touch on the scope of our efforts and the role parents and the private sector play in addressing this problem.

One of our most important programs is the Innocent Images National Initiative, which for the past 11 years has targeted sexual predators who use the Internet to exploit children. Between 1996 and 2005, there were over 15,500 investigations opened in this program. During this 10-year period, the efforts of the Innocent Images National Initiative have resulted in the conviction of over 4,800 child predators.

Facing increasing scrutiny, child predators are going further underground, using file sharing networks, encrypted Web sites, concealing their financial transactions through a maze of online payment services, and traveling to foreign countries to exploit minors.

In pursuit of these criminals, we currently have 42 ongoing undercover operations across the country, with more than 240 agents investigating cases with their State and local counterparts. The FBI also works with officers and analysts from Great Britain, Australia, Belarus, Thailand, and the Philippines, among other countries, at the Innocent Images International Task Force located in Calverton, Maryland.

Identifying child predators is only part of the equation. We must also collect the evidence necessary to convict them. Child predation is a global threat that requires a global response. We have trained more than 16,000 law enforcement officers to handle digital forensic evidence, using a variety of tools, and an additional 4,600 on the use of a special tool known as the Image Scan. This program enables investigators to identify, isolate, and store images from a suspect's computer onto a thumb drive. This year we will conduct training with our international partners as well.

The volume of evidence confronting FBI digital evidence forensic examiners is staggering. To address this ever-increasing challenge, the FBI has deployed 25 state-of-the-art forensic networks to major FBI field offices, with 10 additional offices scheduled to receive this equipment in 2008. These networks enable the FBI forensic examiners to more effectively process seized digital evidence for review by investigators on their desktop computers.

Also in 2008, the FBI plans to establish the first computer forensic unit dedicated solely to the processing of Innocent Images evidence.

Part of our job, and an integral part of the Project Safe Childhood, is to educate the public about child exploitation. A parent may see a Web cam as an easy and inexpensive way for a child to communicate with friends or relatives, but a predator sees it as an open window into a child's bedroom. In field offices around the country, agents are teaching parents the variety of tactics used by predators.

We are also working with the media to get our message out. Our Endangered Child Alert Program, conducted in partnership with National Center for Missing and Exploited Children, and DOJ's Child Exploitation and Obscenity Section, uses national and international media exposure to identify unknown predators and victims. Since 2004, publicity on the FBI Web site and two national television shows have resulted in the arrest of approximately 17 predators and the identification of more than 30 child victims.

We have also enlisted the help of our private sector partners. We have asked Internet service providers and search engine operators to monitor their Web sites for child pornography and to alert us when they discover illegal content. We are working with Internet service providers, seeking assistance in the retention of records of online activities long enough so that when we identify predators and their activities, legal process will be effective to gather the necessary records in order to pursue successful prosecution.

In closing, I want to recognize those who investigate and prosecute these cases. They deserve our respect, our admiration, and our gratitude. They have seen the darkest side of humanity, and continue to press on, as this is among the most important work we do.

I would like to thank the Committee for addressing this very important issue and for allowing me to testify. I now look forward to answering your questions.

[The prepared statement of Mr. Mason follows:]

PREPARED STATEMENT OF MICHAEL A. MASON

Good morning Mr. Chairman, Ranking Member Smith and distinguished members of the Committee. I would like to thank you for the opportunity to address the FBI's role in combating the sexual exploitation of children through the use of the Internet.

With more than one billion people around the world routinely online, the Internet has become an integral part of our daily lives. It has dramatically enhanced the way we communicate, the way we learn, and the way we work.

As *New York Times* columnist Thomas L. Friedman wrote in his best-selling book "The World is Flat," the Internet has leveled the playing field, creating a convergence of people, places, knowledge, and information. We have gone global as individuals.

However, globalization has brought about new challenges. Criminals are making ready use of the Internet, engaging in illegal activities ranging from credit card scams, consumer frauds, computer intrusions, money laundering and a host of other illegal activities. Terrorists around the world are recruiting, communicating and planning attacks, aided by laptops and Internet access.

One of the most insidious uses of the Internet is for child sexual exploitation. An increasing amount of this exploitation takes place in the dark shadows of the Internet—on websites and message boards, through file sharing and e-mail, and in real time with web cams and streaming video.

The assault on children is nothing new, however the internet grants a far greater level of immunity to those who would prey on our children. As a result, there can be no tolerance and no retreat in our efforts to combat this scourge. We cannot and will not rest until these predators are shut down and locked up. That is why coordinated efforts like Project Safe Childhood, which brings federal, state, and local law enforcement and prosecutors together in task forces led by the local United States Attorney to combat online child sexual exploitation, are so important.

Today I want to talk about what we in the FBI are doing to attack child exploitation on the Internet. I want to touch on what we do in terms of evidence collection and prosecution. Lastly, I want to talk about the role of both parents and the private sector in addressing this problem.

One of our most important programs is the Innocent Images National Initiative, which for 11 years has targeted sexual predators who use the Internet to exploit children. Unfortunately, there is no shortage of work in this arena. Between fiscal years 1996 and 2005 there were over 15,556 investigations opened in this program. In 2005 alone, there were over 2,500 cases opened as opposed to 113 in 1996. This represents an increase of 2050%. During this ten year period, investigations under the Innocent Images National Initiative have resulted in 4,784 individuals being charged, 6,145 individuals being arrested, located or summoned to appear in a court of law and 4,822 convictions being obtained.

We have ongoing undercover operations across the country, with more than 240 agents who investigate cases with their state and local counterparts.

On any given day, these investigators may pose as children to lure online predators into the open. They may pose as collectors seeking to share images through peer-to-peer networks. They may coordinate with the National Center for Missing & Exploited Children to identify children and adults featured in child pornography. Or they may train police officers to investigate cases in their own jurisdictions.

With heightened scrutiny in the United States, child pornographers are going further underground, using file-sharing networks and encrypted websites. They are concealing their financial mechanisms through a maze of online payment services, including the use of stolen credit cards. They are traveling to foreign countries to exploit minors. They are victimizing more children, in more ways, at younger and younger ages.

In one instance, agents in Chicago searched a predator's residence and found a customized computer with five hard drives and several external drives. They seized more than a terabyte of digital evidence—the equivalent of more than one million paperback books. This man has been sentenced to 20 years in prison not only for distributing pornography, but for producing images of his own resulting in the victimization of a minor child.

In another such case, a cyber agent traced images downloaded from a file-sharing network to a man in the Pittsburgh area. Together, agents and members of the High Tech Crimes Task Force seized more than 2,500 images of highly graphic child pornography, housed everywhere from the subject's computer to DVDs to his Apple iPod.

These cases are significant not just because of the amount of material seized, but because of our collaboration with state and local counterparts.

This coordination is not limited to the national level. Police officers from Britain, Australia, Belarus, Thailand, and the Philippines, among others, work with agents and analysts on the Innocent Images International Task Force in Calverton, Maryland.

Our international partners know the language, the customs, and the cultures of their home countries. Today, information that once took weeks or even months to relay can be exchanged simply by walking across the room. Together, we have convicted a number of child predators around the world.

For example, last October, Ukrainian investigators arrested a man associated with a young girl featured on a pornographic website. The man had received money and gifts in exchange for allowing the girl to be sexually abused on camera. This investigation started in Denmark, and spread to Ukraine and the United States. It was a Ukrainian police officer, a member of the task force, who played a key part in capturing this criminal and shutting down this website.

Child pornography is a global threat that requires a global response. We have no choice but to work together. It is not just a matter of preference, but of necessity.

As these cases illustrate, identifying child predators is only part of the equation. We must also collect the evidence necessary to convict them.

Our Regional Computer Forensics Labs (RCFLs) and our Computer Analysis Response Teams (CART) work with federal, state, and local officials to find and preserve this vital evidence.

Last year, RCFL examiners working with the San Diego Internet Crimes Against Children Task Force targeted an international ring of child molesters, who distributed photos and videos over the Internet. These individuals victimized at least 45 children, including 37 children from the United States, ranging in age from 2 to 14. Twenty-five individuals in Europe and North America were arrested and tried for their involvement. Examiners spent more than 500 hours collecting the evidence necessary to put these men away.

Unfortunately, such cases are all too common. In the past five years, RCFL and CART examiners have conducted more than 31,000 examinations. As the number of computer crimes we investigate has increased, so has the need for computer forensics.

It is always a struggle to square priorities and improve services with limited resources. We must find a way to balance our forensic needs in counterterrorism, counterintelligence, and computer intrusion cases with an ever-increasing need for such analysis in child exploitation cases.

To meet that need, we have trained more than 16,000 law enforcement officers to handle digital forensic evidence.

FBI digital evidence forensic examiners developed a special tool to aid investigators known as Image Scan. This tool and its training course is one of our most sought-after training programs by both domestic and international law enforcement agencies. This program enables investigators to identify, isolate, and store images from a suspect's computer on a thumb drive without altering the original evidence on the computer.

We have provided Image Scan training to more than 4,600 state and local task force officers, enabling them to collect data necessary to obtain search warrants, or to detain subjects pending a more comprehensive analysis. This year, with the Department of Justice's Computer Crime and Intellectual Property Section, we will train our international partners in Brazil, Budapest, Estonia, Portugal and Canada, to name just a few.

At the same time, the FBI is constantly evaluating, expanding and improving the way that it performs computer forensics and delivers the processed results to investigators. Each year the size of personal computing storage capacity increases while the overall cost drops. The result is that the volume of evidence confronting FBI digital evidence forensic examiners today has become staggering. As of the end of FY 2007, FBI CART reports that it has processed in excess of 2.5 petabytes of data (that is in excess of 2.5 million gigabytes). To combat these trends, the FBI has deployed 25 state-of-the-art forensic networks to major FBI Field Offices. These networks enable FBI forensic examiners to more efficiently process seized digital evidence and then present the results to investigators for their review through their desktop computers.

Despite the unprecedented growth of seized data, the FBI has witnessed a ten per cent reduction for the past two years in the backlog of child exploitation digital evidence examinations as a result of these network efficiencies. Based upon the proposed FY 2008 budget, the FBI plans to expand the forensic networks to an additional ten field offices while continuing to examine smaller network solutions for the FBI's smaller field offices and resident agencies. To enhance our investigative efforts, the FBI's Digital Evidence Section and Cyber Division have recently joined

forces to stand up the first digital evidence forensics unit dedicated solely to the processing of Innocent Images evidence. The new unit, expected to be fully operational by the end of FY 2008, will be in Linthicum, Maryland, and will have up to ten full time forensic examiners. It will perform full content forensic examinations on priority investigations.

By giving cyber investigators the tools they need, we are reducing our backlog and leaving more complex matters for the CART teams and the RCFLs.

We know there is a real need for additional training, faster services, and better coordination, and we will continue to expand these efforts in the years to come.

I want to talk for just a moment about the importance of community outreach and private sector partnerships.

Part of our job—and an integral part of Project Safe Childhood—is to educate the public about child exploitation. The Internet has provided child predators with a sense of anonymity and their products a world-wide portability. These are not mere pictures or posed shots, but live acts of molestation. And as predators become desensitized, those who once collected images may start to create images, seeking to harm younger children, in more terrifying ways.

Our cyber agents routinely meet with members of the community to talk about Internet safety. Parents may not understand the dangers lurking in cyber space, or what they are doing to put themselves and their children at risk. A parent may see a web cam as an easy and inexpensive way for a child to communicate with friends or relatives, but a predator sees it as an open window into a child's bedroom.

In field offices around the country, agents are teaching parents how to protect against the tactics used by predators, and the risks of peer-to-peer file-sharing networks, instant messaging, and social networking sites.

We are also working with the media to get the message out. Our Endangered Child Alert Program, conducted in partnership with the National Center for Missing & Exploited Children and Department of Justice's Child Exploitation and Obscenity Section, uses national and international media exposure to identify unknown predators and victims. Through publicity on the FBI website and the television show "America's Most Wanted," we have identified and arrested eight predators. More importantly, we have identified more than 30 child victims.

In another effort, Oprah Winfrey uses her television show to alert viewers to known sexual predators and posts their faces and identifying information on her website. She is offering $100,000 out of her own pocket for each predator brought into custody. Within the first week, two fugitives were arrested. Since then, two more predators have been taken into custody.

We have also enlisted the help of our private sector partners. We have asked Internet service providers and search engine operators to monitor their websites, and to alert us when they discover illegal content.

We in law enforcement face another hurdle in purging predators from the Internet—and that hurdle is tracking both the criminal and the crime. Data linking criminals to their crimes is absolutely essential in the fight against online child exploitation. We are working with Internet service providers on a voluntary basis to retain records of online activities so that we can identify predators and their activities and successfully prosecute them.

Everyone in this room is familiar with violence and injustice. There are few things more difficult to bear than the victimization of a child. These cases are horrific, heartrending, and seemingly endless in number.

The FBI is committed to protecting the most vulnerable among us. We are committed to sweeping sexual predators off the street, off the Internet, and out of our children's lives.

In closing, I want to recognize those who investigate and prosecute these cases. They deserve our respect, our admiration, and our gratitude. They have seen the darkest side of humanity. However, this is some of the most important work we do.

I would like to thank the Committee for addressing this very important issue and for allowing me to testify. I look forward to answering your questions.

Mr. SCOTT. Thank you, Mr. Mason. I forgot to advise people about the little lights before you and to confine your remarks to 5 minutes, but Mr. Mason, apparently you didn't need directions. So I thank you for your testimony.

Mr. MASON. Yes, sir.

Mr. SCOTT. Mr. Rothenberg.

TESTIMONY OF LAURENCE E. ROTHENBERG, DEPUTY ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL POLICY, DEPARTMENT OF JUSTICE

Mr. ROTHENBERG. Thank you, Mr. Chairman, Ranking Member Forbes, and the other Members of the Committee. Thank you for inviting me to represent the Department of Justice at this important hearing, and to describe our current proposals for enhancing our ability to investigate and to prosecute predators who sexually exploit children, especially through the Internet.

The fight against child exploitation is a priority for the Department as exemplified by our work in Project Safe Childhood, a nationally coordinated investigative and prosecutorial initiative linking U.S. Attorneys offices across the country with Federal, State, and local law enforcement, and with organizations like the National Center for Missing and Exploited Children. The Department appreciates Congress' strong support for these efforts, and the work that you have done recently. Most notably, the passage of the Adam Walsh Child Protection and Safety Act of 2006 has already made a difference.

I ask that my full written statement be included in the record, and I will just summarize our principal proposals.

Three of these proposals are contained in the Violent Crime and Antiterrorism Act announced by former Attorney General Gonzales this past May, and we also have several new proposals to facilitate prosecution of fugitive sex offenders. A number of these proposals will be familiar to you from Congressman Musgrave's testimony earlier today, and I will provide the Department's perspective on them.

First, we urge that Congress establish a mandatory minimum sentence for possession of child pornography. This is crucial because too many people believe that child pornography is just pictures and not a big deal. That is wrong, Mr. Chairman. Each child pornography image is a visual record of the sexual exploitation of a child. It is not just a picture. And every time it is viewed the child is violated again. Furthermore, it is the demand for such images that fuels the physical violation of the child in the first place.

Unfortunately, since the Federal Sentencing Guidelines became advisory, the number of downward departures by judges in child pornography possession cases has leapt to 26.3 percent, more than twice the average rate of such departures. Establishing a two-year minimum sentence will be a warning to potential consumers of child pornography, prevent unwarranted downward departures, and forcefully express our society's revulsion at this type of material.

Our second proposal would amend the current law providing that an Internet service provider who knowingly and willfully fails to report the presence of child pornography images on its computer services is subject to a criminal fine. This provision has been virtually impossible to enforce. Our legislation would therefore add a civil penalty that would be easier to enforce for negligent failure to report such images. Those images are out there, they are on somebody's computer server, and law enforcement needs to know about them to investigate and prosecute the crimes.

Our third proposal fills a gap in existing law that has led some courts to overturn convictions of possessors of child pornography. Some courts have narrowly interpreted, incorrectly in our view, the definition of the term "possession" in the Federal Criminal Code so that a person who, for example, viewed images of child pornography on his computer but did not save them onto his disk drive would not have violated the statute. Our proposal would amend the statute explicitly to cover, quote, knowingly accessing child pornography with the intent to view it, close quote.

Our final set of proposals relates to 18 U.S.C. Section 2250, created in the Sex Offender Registration and Notification Act, SORNA, part of the Adam Walsh Act. Section 2250 creates the Federal felony offense of failure to register as a sex offender or to update a registration. By terms of the statute, it applies to a person who travels in interstate or foreign commerce. Since the law has been enacted, one Federal district court has found that the statute's use of the present tense "travels" means that the law only applies when the interstate or foreign travel occurred after the statute enactment. In order to clarify that this jurisdictional requirement is satisfied, regardless of whether the travel occurred before or after the enactment of the Adam Walsh Act, it should be amended to add "has traveled."

Additionally, our proposal will clarify that section 2250 offenses are continuing offenses as long as an offender's failure to register or update a registration exists. This clarification would eliminate the possibility of a claim by an offender that section 2250 was an ex post facto law.

Finally, as an enhancement of the current law, we propose to include section 2250 among the child abduction and felony sex offenses that can be prosecuted at any time without limitation.

Thank you for giving me the opportunity to discuss our proposals, and I am happy to answer your questions.

[The prepared statement of Mr. Rothenberg follows:]

PREPARED STATEMENT OF LAURENCE E. ROTHENBERG

Testimony of
Laurence E. Rothenberg
Deputy Assistant Attorney General
Office of Legal Policy
U.S. Department of Justice

Before the U.S. House of Representatives
Committee on the Judiciary

Hearing on Sex Crimes and the Internet: Danger is Just a Click Away

October 17, 2007

Chairman Conyers, Ranking Member Smith, and other members of the Committee:

Thank you for inviting me to represent the Department of Justice at this important hearing and to describe our current proposals for enhancing our ability to investigate and to prosecute predators who sexually exploit children, especially through the Internet. The Department appreciates Congress's strong support for our efforts. The work that you have done recently, most notably the passage of the Adam Walsh Child Protection and Safety Act, has already made a difference.

The Department has a number of proposals to enhance our current investigative and prosecutorial efforts. Three of these proposals are contained in the Violent Crime and Anti-Terrorism Act that former Attorney General Gonzales transmitted in June. We also have several new proposals to facilitate prosecution of fugitive sex offenders.

Mandatory Minimum for Possession of Child Pornography

First, we urge Congress to establish a mandatory minimum sentence for possession of child pornography. This is crucial because too many people believe that child pornography is "just pictures" and is not "a big deal." That is wrong. Each pornographic image of a child is the visual record of the sexual exploitation of that child. It is not just a picture. Every time that image is viewed, the child is violated once again. Moreover, the demand for such images is what fuels the physical violation of the children in these images in the first place. Possession of child pornography is victimization of a child and should be punished accordingly.

Unfortunately, since the Federal Sentencing Guidelines became advisory under the Supreme Court's decision in *United States v. Booker* the number of downward departures by judges in federal child pornography possession cases has increased. After enactment of the PROTECT Act of 2003, which restricted in various ways the authority of courts to make non-government-sponsored downward departures in sentences, the rate of non-government-sponsored below-range sentences for all offense types was about 5%. *See* United States Sentencing Commission, Final Report on the Impact of *United States v. Booker* on Federal Sentencing (March 2006), at p. 54, *available at* http://www.ussc.gov/booker_report/Booker_Report.pdf. Following *Booker*, that rate jumped up to 12.5%. *Id.* at p. 47. For child pornography possession offenses, however, the rate of non-government-sponsored below-range sentences leapt to 26.3%, more than twice the average rate. *Id.* at p. 122. By way of comparison, for drug trafficking and firearms violations, the rate has increased to 12.8% and 15.2%, respectively, much closer to the average. *Id.* at table on page D-5.

The increase in non-government-sponsored, below-range sentences for possession offenses after *Booker* demonstrates the need for a mandatory minimum sentence for possession offenses. Establishing a two-year minimum sentence will be a warning to potential consumers of child pornography, prevent unwarranted downward departures, and forcefully express our revulsion at this type of material. This change is contained in

section 201 of the Department's Violent Crime and Anti-Terrorism Act of 2007 and is included as section 201 of H.R. 3156, the Violent Crime Control Act of 2007.

Strengthening 42 U.S.C. § 13032 to Ensure That Child Pornography is Effectively Reported.

Our second proposal would amend an existing law that requires certain providers of electronic communications services to report violations of the child pornography laws. Currently the law provides that a provider who knowingly and willfully fails to report the presence of child pornography images on its computer servers 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. These impediments severely hinder the needed crackdown on the presence of child pornography on the Internet.

Our 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.

Even more importantly, the legislation would add civil fines for *negligent* failure to report a child pornography offense. The civil penalty is set at $50,000 for the initial violation and $100,000 for each subsequent violation. The Federal Communications Commission would be provided with the authority to levy the civil fines under this section and to promulgate the necessary regulations, in consultation with the Attorney General, for imposing the fines and for providing an appropriate administrative review process.

These proposals would make it much more likely that service providers will exercise sound practices for weeding out child pornography. The images are out there, too often on commercial computer servers, and law enforcement needs to know about them to investigate and to prosecute the sexual predators who consume them. This amendment is contained in section 202 of the Department's Violent Crime and Anti-Terrorism Act of 2007 and in section 202 of H.R. 3156.

Knowingly Accessing Child Pornography.

Our third proposal fills a gap in existing law that has led some courts to overturn convictions of possessors of child pornography.

18 U.S.C. §§ 2252 and 2252A currently criminalize various activities related to child pornography including transportation, trafficking, and possession. Some courts have narrowly interpreted (incorrectly, in our view) the definition of possession so that a person would not have violated the statute if he, for example, viewed images of child pornography on his computer but did not save them onto his disk drive. Even if, in his computer's "temporary Internet cache," we have a record of his viewing the images, and

thus proof that he accessed them on a website, under this narrow interpretation, he would not be guilty of violating the statute if he did not know that his temporary Internet cache automatically saved the images on his computer.

Two recent cases demonstrate the need for these changes. In *United States v. Teal*, No. 1:04-CR-00042-CCB-1 (D. Md., motion to dismiss granted Aug. 13, 2004), the Maryland U.S. Attorney's Office prosecuted Marvin Teal, a former administrative law judge who had prior convictions for sexually abusing children, for possession and attempted possession of child pornography based on his viewing child pornography at a public library in Baltimore, Maryland. Library police officers saw child pornography on the computer Teal was using, arrested him, and printed out the images that could be seen on the computer screen. Because there was no evidence that the defendant had himself downloaded or saved anything, the District Court dismissed the case. We chose not to appeal, given the state of the law and the facts of the case.

In *United States v. Kuchinski*, 469 F.3d 853 (9th Cir. 2006), the Ninth Circuit vacated and remanded the sentence of an offender found with between 15,120 and 19,000 separate images of child pornography on his computer on the basis that he did not know that they were in his Internet cache. The court stated, "There is no question that the child pornography images were found on the computer's hard drive and that Kuchinski possessed the computer itself. Also, there is no doubt that he had accessed the web page that had those images somewhere upon it, whether he actually saw the images or not. What is in question is whether it makes a difference that, as far as this record shows, Kuchinski had no knowledge of the images that were simply in the cache files. It does." Of course we acknowledge the Ninth Circuit's authority to interpret the law this way. However, we think the court's distinction should not make a difference under the law.

Our proposal would correct these anomalies while protecting unsuspecting persons who unintentionally access child pornography from prosecution. Specifically, the bill would amend 18 U.S.C. § 2252(a)(4) and 18 U.S.C. § 2252A(a)(5) to criminalize not only possession of child pornography, but also "knowingly accessing child pornography with the intent to view it." That is, a person would be liable to prosecution if he purposefully clicked on a link with the intent that when the link opened, he would view child pornography. It would therefore be a two-step test that the prosecution would have to satisfy—first, that he purposefully (that is, not accidentally) clicked the link, and, second, he did so with the intent that by clicking on the link child pornography would appear on his computer screen. This test would not be difficult to satisfy in the case of people who really did want to view child pornography. Extrinsic evidence—such as the name of the link, which would probably have terms indicating that it displayed child pornography, and payment for the images—would be used to prove the violation. But in the case of an "innocent viewer" who accidentally came across child pornography, the two-step proof would be his protection. This change was included in Section 203 of DOJ's proposed bill and is now included in Section 4 of H.R. 3148.

Amendments to 18 U.S.C. § 2250

Our final set of proposals relates to 18 U.S.C. § 2250, which was enacted in the Sex Offender Notification and Registration Act (SORNA), Title I of the Adam Walsh Child Protection and Safety Act of 2006. Section 2250 creates the federal felony offense of failure to register as a sex offender or to update a registration. We understand that similar proposals will be included in legislation currently being developed (or that is expected to be introduced shortly).

First, by the terms of § 2250(a)(2)(B), the law applies to a person who "travels" in interstate or foreign commerce. Since the law was enacted, one federal district court has found that the statute's use of the present tense "travels" means that the law only applies when the interstate or foreign travel occurred after the statute's enactment. In order to clarify that this jurisdictional requirement is satisfied regardless of whether the travel occurred before or after the enactment of § 2250, the statute should be amended to add "or has traveled."

In relation to SORNA's objective of comprehensive registration and tracking of sex offenders on a nationwide basis, and in relation to the federal government's constitutional authority to enforce these registration requirements through federal prosecution in appropriate cases, it makes no difference whether the circumstances supporting federal jurisdiction under § 2250 occurred before or after SORNA's enactment on July 27, 2006. Thus, for example, a sex offender who traveled from one state to another, or entered or left Indian country, prior to the enactment of SORNA, and failed to register as SORNA requires following its enactment, should be subject to liability under § 2250 to the same extent as one whose interstate travel (or entry to or departure from Indian country) occurred after the enactment of SORNA.

As a practical matter, many of the sex offenders who have been apprehended by federal authorities for failing to register engaged in their interstate travel prior to the enactment of SORNA. A typical case might involve a sex offender released in 2002 following incarceration in New York for a rape or child molestation offense, who relocated from New York to Oklahoma in 2004; never registered in Oklahoma; and was apprehended in Oklahoma as a fugitive by federal authorities in 2007. The federal courts that have considered this issue have generally discerned the legislative intent accurately, finding that the occurrence of the travel prior to SORNA's enactment is no bar to liability under § 2250 for the sex offender's continuing failure to register following July 27, 2006. *See, e.g.*, *United States v. Madera*, 474 F. Supp. 2d. 1257 (M.D. Fla. 2007); *United States v. Husted*, No. CR-07-105-T, 2007 U.S. Dist. LEXIS 56662 (W.D. Okla. Jun. 29, 2007); and *United States v. Markel*, No. 06-20004, 2007 U.S. Dist. LEXIS 27102 (W.D. Ark. Apr. 11, 2007).

In one case, however, a federal district court has dismissed a prosecution under 18 U.S.C. § 2250 on the ground that the defendant's travel occurred before SORNA's enactment. *United States v. Bobby Smith*, 481 F. Supp. 2d 846 (E.D. Mich. 2007). While

the dismissal in that case is being appealed, this is not a matter that should be open to litigation, and the fact that one judge has misunderstood the legislative intent in 18 U.S.C. § 2250 raises concerns that others may do so as well.

The amendment will foreclose such errors and problems by changing § 2250(a)(2)(B) to refer explicitly to any sex offender who "travels or has traveled in interstate or foreign commerce," together with conforming changes in the language relating to Indian country. This will help to ensure that sex offenders who have failed to register in conformity with SORNA do not enjoy a windfall immunity to federal criminal liability based on fortuities of timing in their travel among jurisdictions, and will thereby advance SORNA's basic objective of promoting public safety against sex offenders and offenders against children through a comprehensive national system for the registration of those offenders.

This could be accomplished by a simple change in the statute as follows:

Section 2250(a)(2)(B) of title 18, United States Code, is amended –

(1) by inserting "or has traveled" after "travels";

(2) by inserting "or has entered or left, or resided in," before "Indian country"; and

(3) by inserting ", after conviction of the offense by reason of which the person is a sex offender as defined for the purposes of the Sex Offender Registration and Notification Act" after "Indian country".

Additionally, the amendment would clarify that § 2250 offenses are continuing offenses as long as an offender's failure to register or update a registration exists. Certain courts have found that § 2250 offenses are not continuing offenses for *ex post facto* purposes. *See, e.g.*, *United States v. Sallee*, No. CR-07-152-L, 2007 U.S. Dist. LEXIS 68350 (W.D. Okla. Aug. 13, 2007); and *United States v. Stinson*, Crim. Act. No. 3:07-00055, 2007 U.S. Dist. LEXIS 66429 (S.D.W.V. Sep. 7, 2007). Additionally, a district court has found that a § 2250 offense is not a continuing offense for venue purposes, *United States v. Roberts*, No. 6:07-CR-70031, 2007 U.S. Dist. LEXIS 54646 (W.D. Va. Jul. 27, 2007), while another court in the same district has found that it is. *United States v. Hinen*, 487 F. Supp. 2d 747 (W.D. Va. 2007). The amendment will address these various opinions by clarifying that § 2250 offenses are continuing offenses for both purposes.

These two clarifications could be made by the following change to the statute:

Section 2250 of title 18, United States Code, is amended by adding at the end the following subsection:

"(d) Continuing offense. Failure to register or update a registration in violation of subsection (a) is a continuing offense for as long as such failure exists."

Finally, as an enhancement of the current law, we propose amend 18 U.S.C. § 3299, which currently provides that child abduction and felony sex offenses can be prosecuted at any time, without limitation, to cover § 2250 offenses as well. This enhancement could be accomplished with the following legislative language:

> Section 3299 of title 18, United States Code, is amended by inserting "109B," after "chapter 109A,".

Conclusion

Thank you for giving me the opportunity to discuss our proposals, and I am happy to answer your questions about them.

Mr. SCOTT. Thank you. Mr. Waters.

TESTIMONY OF FLINT WATERS, WYOMING INTERNET CRIMES AGAINST CHILDREN TASK FORCE

Mr. WATERS. Thank you, Mr. Chairman, Ranking Member Forbes, and Members of the Committee. I want to thank you for the opportunity to speak on this matter. I am Flint Waters, Special Agent with the Wyoming Division of Criminal Investigation.

I am not here to testify on behalf of the entire Internet Crimes Against Children network. There are others that can do that. I am here to speak from my work on the front lines investigating these cases and building the ICAC data network. Let me share with you some of the material we see every day.

Imagine the movie of the 4-year-old girl being sodomized on a bed, as her attacker tries to force her to comply with his wishes. And from the speakers you can hear her screams of no, no, no. This child is trying to free herself unsuccessfully from this attacker. We have got movies, the movie of the toddler on a changing table. The video zooms in as her diaper is removed, and an unknown adult male penetrates the child. From the video it is obvious that this is frequent activity for this little girl. In many of these videos, the offender films as they sneak into a child's bedroom with the lights from their camera. We can only imagine that the child's mother must be asleep, unaware, somewhere else in the house.

In a recent case, an offender filmed himself drugging the juice boxes of neighborhood children before tricking them into drinking the mix. He then filmed himself as he sexually abused unconscious children. Through the interdiction of his trading in child pornography, investigators found numerous local victims.

When you do this sort of work there is certain pictures you just can't get out of your mind. For me, one is the picture of a young girl about six or seven. She is nude, she is strapped to a chair, and the chair has fallen over, and this child is being sexually assaulted by a dog. The tears are streaming up this little girl's face. And to my knowledge, she has not been identified.

In one case investigated out of Wyoming, an offender was so fixated on manufacturing these child sexual abuse images, they arranged to abduct two girls, one on the East Coast and one in Wyoming. When he came to Wyoming, he was arrested. During his interview after his arrest he talked about plans to make his fortune selling child pornography. When asked about his intentions with the Wyoming girl, he said he was going to use her to make movies, and then sell her or leave in the mountains to, quote, be eaten by a bear or a lion. She wouldn't survive.

Recently, our investigators have been using systems to find individuals trafficking using peer-to-peer file sharing, searching for sadistic images where the victims are especially young, and they are reported online trading these images at that moment. In one day we found 4,500 unique locations throughout the United States. That is October 4th, 2007. During the month of August, 2007, that is where we found individuals trading—these are distributors of child pornography—around the United States. We have been tracking this for 36 months. The magnitude of this problem, our lowest estimate is that there are over 350,000 individuals trading these

images depicting rape and sexual abuse of children in the United States alone. That is 350,000 unique serial numbers. Of that, we can clearly calculate well over half a million people in the United States that we can track.

The good news is we know how to find these predators. They are just a subpoena away from arrest and prosecution. In a recent case in the western United States, through our operations an offender was found to be trading child sexual abuse images on the peer-to-peer networks. When he was identified, law enforcement found that he was a respiratory therapist at a children's hospital. He admitted targeting the weak, the unconscious, children that were there on hospice care. When asked how many children he had victimized, he looked out at the falling snow and asked how many snowflakes are there.

Chairman Conyers, Members of the Committee, the bad news is that while my task force and the ICAC network can tell you how to interdict tens of thousands of sexual predators tomorrow, the vast majority of these leads will never be investigated. In fact, less than 2 percent of these crimes we know about are investigated due to the sheer lack of resources. Most of these victims will not be rescued.

I am here today to testify about what many of my law enforcement colleagues are not free to come here and tell you. We are overwhelmed, we are underfunded, and we are drowning in the tidal wave of tragedy. We don't have the resources we need to save these children. Law enforcement's efforts, to include the ICAC program, the FBI's Innocent Images National Initiative, ICE's Cyber Crimes Center, and U.S. Postal Inspection Service are all desperately underfunded. From where I stand, these are human rights workers who need and deserve our support. The price we pay for coming up short will be measured in children lost.

There are times in our line of work when you find yourself staring into the eyes of the children in these movies and apologizing. We apologize because we can't find them. We can't rescue them. There is just not enough people or resources to help.

On behalf those victims, I thank you for doing everything in your power to help us fight this human rights crisis.

[The prepared statement of Mr. Waters follows:]

PREPARED STATEMENT OF FLINT WATERS

TESTIMONY OF

Special Agent Flint Waters
Lead Agent for the Wyoming Internet Crimes Against Children Task Force

WYOMING DIVISION OF CRIMINAL INVESTIGATION
OFFICE OF THE ATTORNEY GENERAL

for the

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY

"Sex Crimes and the Internet"

October 17, 2007

Chairman Conyers, Ranking Member Smith, members of the Committee, thank you for the opportunity to testify before you today on the subject of Internet child sex crimes. I am Flint Waters, Special Agent with the Wyoming State Division of Criminal Investigation. Our Department operates one of 59 regional Internet Crimes Against Children—or "ICAC"—Task Forces throughout the United States, which are supported by a grant through the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention (OJJDP). The ICAC Task Forces bring together federal, state and local law enforcement agencies to focus on investigation, education and prevention matters related to the exploitation of children by means of the Internet.

I am here today to testify not on behalf of the entire ICAC network; there are others who can do that. I am here today as a result of my work on the front lines investigating these cases and building the ICAC Data Network. The ICAC Data Network is, in many ways, the high-tech nerve center for the work we do nationally to find online predators and locate their victims.

The True Nature of Child Pornography

I'd like to begin by taking a minute to explain to you what child pornography really is. Many people, when they think about child pornography, imagine photographs of naked teens or babies in the bathtub. Nothing could be farther from the truth. The photographs and movies being traded on the Internet today are extremely graphic and brutal crime scene images, depicting the most horrifying moments in the life of a child.

Let me share with you some of the material we see every day:

Imagine the movie of the four year old girl being sodomized on a bed. As her attacker tries to force her to comply with his wishes you can hear her as she pleads for him to stop. Screams of "No, NO, NO!" play over the computer speakers as the movie depicts this child trying to free herself, unsuccessfully from her attacker.

How about the movie of the toddler on the changing table. The video zooms in as her diaper is removed and an unknown adult male penetrates the child. From the video it is obvious that this is frequent activity for this little girl.

In many videos the offender films as they sneak into a child's bedroom and abuse the children under lights from the camera. We can only imagine that the child's mother must be asleep unaware, somewhere else in the house.

In a recent case an offender filmed himself drugging the juice boxes of neighborhood children before tricking them into drinking the mix. The offender would then film himself as he sexually abused the unconscious children. Through the interdiction of his trading in child pornography investigators found numerous local victims.

When you do this work, there are certain pictures that stay with you, that you cannot get out of your mind. For me, one of those pictures is of a young girl, about six or seven. She is nude and has been tied to a chair. The chair has fallen over. This child is being sexually assaulted by a dog. Tears are streaming up her face. To my knowledge, that little girl has not yet been identified.

My goal every day is to find and rescue that little innocent girl, and to stop that predator from hurting other children like her.

A 2005 Study funded by Congress through the National Center for Missing and Exploited Children[1] shows what those of us on the front lines know too well. Of those individuals arrested for possession of child pornography:

- 83% had images of children 6-12 years old
- 39% had images of children 3-5 years old
- 19% had images of infants and toddlers

The study also described what we see in these photos and movies:

- 80% had images showing sexual penetration of a child
- 21% had images of children subjected to bondage, torture or other sadistic acts
- Just 1% of those possessing these images restricted their collections to simple photos of naked children.

This is what we investigate every day. This is not about obscenity or even pornography. These are movies and images capturing and forever memorializing the complete destruction of innocence.

The Full Magnitude of the Crisis

From our vantage point in Wyoming we are just beginning to measure the magnitude of child exploitation. Our cooperative network focuses primarily not on the large international and commercial rings, but on the mass of trafficking right here in the U.S. and the predators that scour the Internet every day looking for more U.S. victims.

To understand the sheer magnitude of the trafficking, it is necessary to know what the Internet has done to facilitate child exploitation. The Internet has linked together hundreds of thousands of pedophiles, possibly millions worldwide. The danger is not that they form an online community. The danger is that they form an online economy that barters in the lives of children. The true product they seek, child sexual abuse imagery, can only be produced one way: through the sexual assault of children. So in the Internet age, demand for child pornography images in California or Europe can now result in the rape of a child in Texas, Florida or Michigan.

In one case investigated in Wyoming an offender was so fixated on manufacturing child sexual abuse images he arranged to abduct two girls. One on the east coast, one in Wyoming. When he came to Cheyenne to pick up the Wyoming girl he was arrested.

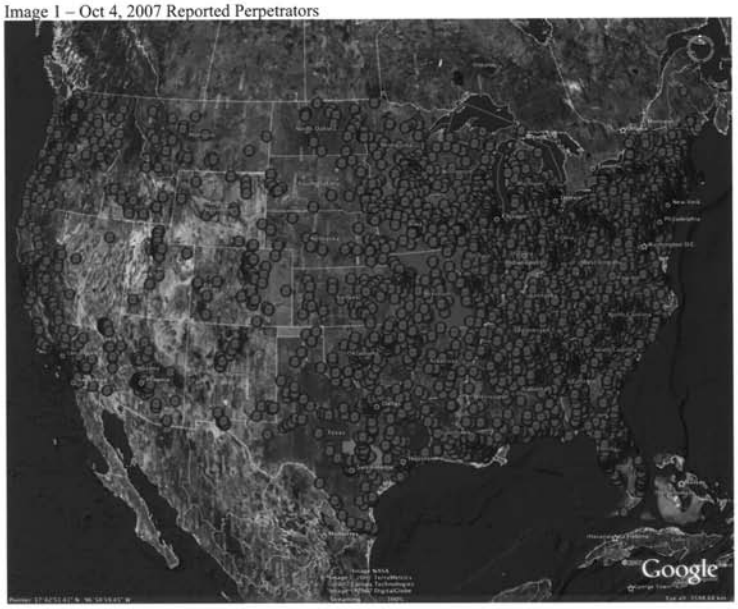
During the interview after his arrest he talked about his plans to make his fortune selling child pornography. His recorded interview includes his boasting about his business plan and how he would profit. When asked about his intentions with the Wyoming girl he said he was going to use her to make the movies and then sell her or leave her in the mountains to "be eaten by a bear or a lion or she wouldn't survive."[2]

Unfortunately the twelve year old Wyoming girl he targeted was actually me. When he traveled to Cheyenne to meet this "little girl" he found things were not as he had hoped.

We are seeing an exploding demand for images of child sexual abuse. Let me give you just a few indicators from the ICAC Data Network:

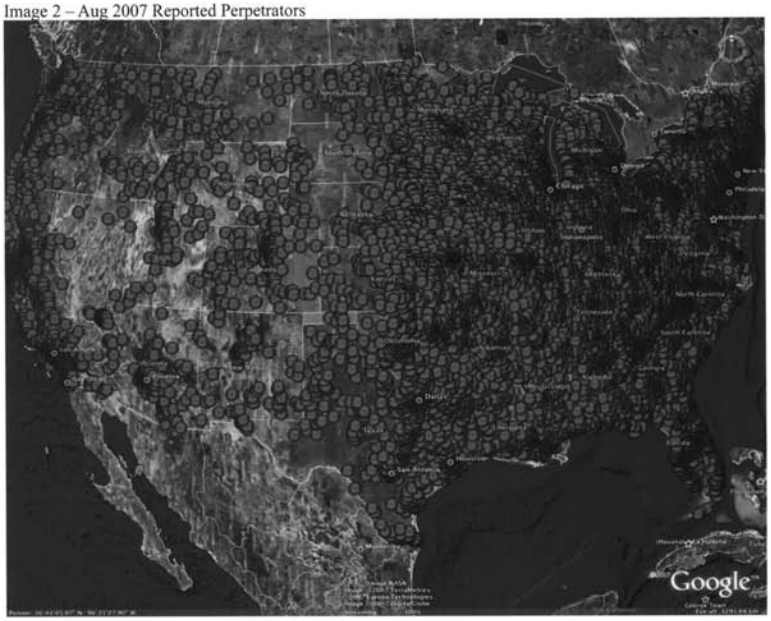
- Recently, investigators using our systems searched for computers actively engaged in the distribution of child pornography via just one method: peer-to-peer file sharing. We searched for sadistic images, where the victims were especially young and where individuals were reported to be online offering the files to others. In just a single day, we found individuals actively engaged in trafficking from over 4,500 unique locations in the United States alone. You can see that this is a very small subset, a minimum indicator of the problem. (Image 1)

Image 1 – Oct 4, 2007 Reported Perpetrators

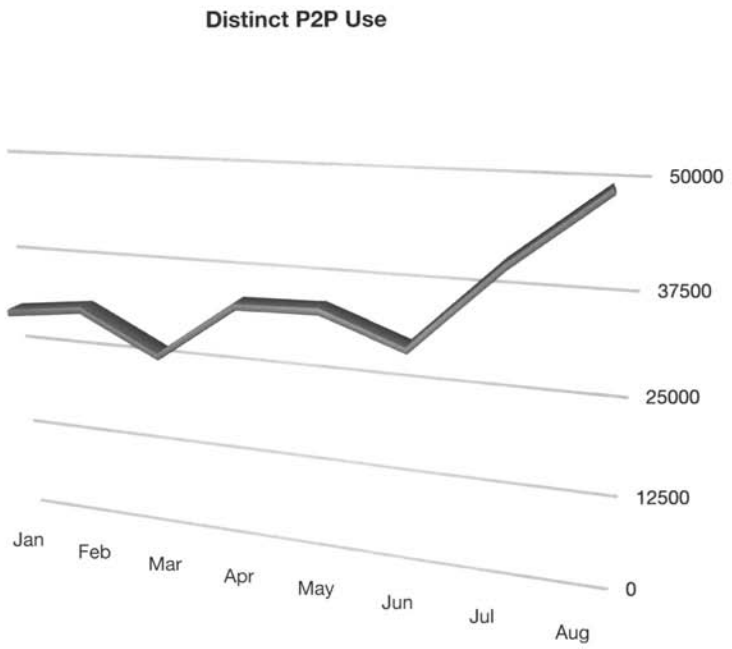


- Using the same narrow search criteria, we logged individuals trafficking in these images through peer-to-peer file sharing from over 49,000 unique locations within the U.S. during August 2007. (Image 2)

Image 2 – Aug 2007 Reported Perpetrators



- How much bigger is the full magnitude of the problem? Our lowest estimate is that there are well over **350,000**[3] individuals trading images depicting the rape and sexual abuse of children within the United States alone.
- Over the last thirty-six months we have seen a steady increase in this activity, even though many agencies are aggressively pursuing these offenders in one manner or another. (Figure 1)



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
Unique US Serial Numbers	30817	32017	26976	34167	34443	30803	41073	49554

Figure 1 - Continued rise in distinct P2P use for trafficking child sexual abuse imagery Jan-Aug 2007

For clarification that is hundreds of thousands of perpetrators in the United States alone and these numbers are climbing.

Lack of Resources

The good news is that we know how to find these predators. Most are just a subpoena away from arrest and prosecution. And finding them will lead us to thousands of child victims. Some are victims of child exploitation. Others are victims of sexual predators who also happen to be committing child pornography crimes. Either way, these investigations have and will continue to lead us to their doorstep… and to rescue children from harm.

Take a recent case from the western United States. Through our operations an offender was found to be trading child sexual abuse images on the P2P networks. When he was confronted law enforcement found the perpetrator to be a respiratory therapist at a children's hospital. He admitted targeting the weak, the unconscious, children there for hospice care. When asked how many children he had victimized he looked out at the falling snow and asked, "How many snowflakes are there."

The 2005 study I cited earlier found that 55% of those arrested for "simple possession" of child pornography had either sexually assaulted a child or attempted to entice a child online. Another federal study found the percentage to be much higher.

That means that following the trail back through the Internet to interdict these criminals is the single best way we have of rescuing otherwise unidentified children and preventing future child sexual assault.

Chairman Conyers, members of the committee, the bad news is that while my task force and the ICAC network can tell you how to interdict tens of thousands of sexual predators tomorrow, the vast majority of these leads will never be investigated. In fact, less than 2% of the crimes we know about are investigated, due to sheer lack of resources. Most of these victims will never be rescued.

I am here today to testify about what many of my law enforcement colleagues are not free to come here and tell you.

We are overwhelmed.

We are under-funded.

We are drowning in a tidal wave of tragedy and we don't have the resources we need to save these children. Law enforcement efforts to pursue these offenders to include the ICAC program, the FBI's Innocent Images National Initiative, ICE's Cyber Crimes Center and the U.S. Postal Inspection Service are all desperately under-funded. From where I stand, these are human rights workers who need and deserve our support.

The price we pay for coming up short will be measured in children lost.

There are times in our line of work when you find yourself staring into the eyes of the children in these movies and apologizing. You apologize to the child because you just can't find them. You can't rescue them. There are not enough people or resources to help.

On behalf of those victims, I thank you for doing everything in your power to help us fight this human rights crisis.

[1] Child-Pornography Possessors Arrested in Internet-Related Crimes:
Findings From the National Juvenile Online Victimization Study 2005
Janis Wolak, David Finkelhor, and Kimberly J. Mitchell

[2] United States vs. Todd Noble
Interview transcription between Todd Noble and Special Agent Waters
November 1, 2003

FW: What other options did you have to get rid of her besides selling her to the bikers?
TN: Dropping her off on the side of the road. That's…
FW: What else?
(Pause)
TN: I…take her in the mountains and leave her. I…the only really options that I…even knew about.
FW: Where did you talk about taking her in the mountains and leaving her at? You did specify.
(Pause)
TN: I don't think so. I don't know.
(Item removed)
FW: What do you think would have happened to her if you took her to the mountains and left her?
TN: She'd probably be eaten by a bear or a lion or she wouldn't survive.
FW: You feel like law enforcement has treated you well today?
TN: Yeah.

[3] Examining a single client application for just one Peer to Peer file sharing network reveals over 350,000 unique serial numbers identified as child pornography traders. This application represents 66% of the clients used on this network to trade child pornography. These serial numbers are provided to all members of the public in this trading community by the client software as a manner to programmatically locate each other during the exchange of material. Law enforcement makes note of the numbers only in situations where the other party has publicly advertised child sexual abuse material for trade.

ATTACHMENT

State of Wyoming Attorney General

Child Sex Crimes on the Internet

Prepared for: House Judiciary Committee
Prepared by: Flint Waters, Special Agent, Wyoming Attorney General Division of Criminal Investigation

October 3rd, 2007

State of Wyoming Attorney General 316 West 22nd Street,Cheyenne, Wyoming 82001 **T** 307.777.7181 **F** 307.777.7545

Summary

Overview

The statistics herein come from documented observations of one particular type of technology being used to facilitate child exploitation globally. Therefore, at most, the staggering numbers reported reflect a small portion of the severity of this problem given the growing form of predation facilitated by several types of technology associated with the Internet. Prior efforts to measure the use of technology in child exploitation have proven difficult due to the complexity of the systems leveraged by Internet predators. However, this report is able to provide some clear insight into the use of Peer to Peer networks in this type of crime.

Approach

Investigators deploying software written by the State of Wyoming have identified a vast network of traffickers who have distorted the original uses of Peer to Peer (P2P) networks to feed their own needs. The tactics being deployed by law enforcement have resulted in the identification of staggering numbers of individuals trading child sexual abuse movies and images.

Introduction

This report is presented by Flint Waters, Lead Special Agent for the Wyoming Internet Crimes Against Children Task Force. (ICAC) Agent Waters is the hands-on supervisor of a team of investigators tasked with interdicting child predators for the State of Wyoming. He carries a daily case load alongside state and federal agents in the Wyoming ICAC Task Force. Agent Waters is the author of the software used in Operation Peer Precision and has trained law enforcement from around the world. He has been recognized as an expert in Internet Child Exploitation in state and federal court and has previously testified before congress.

Estimates

The details you are about to review originate from a single P2P network, one of many used daily on the Internet. These details relate to just one small corner of the Internet. It applies only to one P2P system where child sexual abuse movies and images were presented to undercover law enforcement throughout the world. This data does not include traders using email, chat, social networks, news servers or paid and free web sites. At most it can be seen as a bare minimum of the trafficking of child sexual exploitative materials.

Just One System

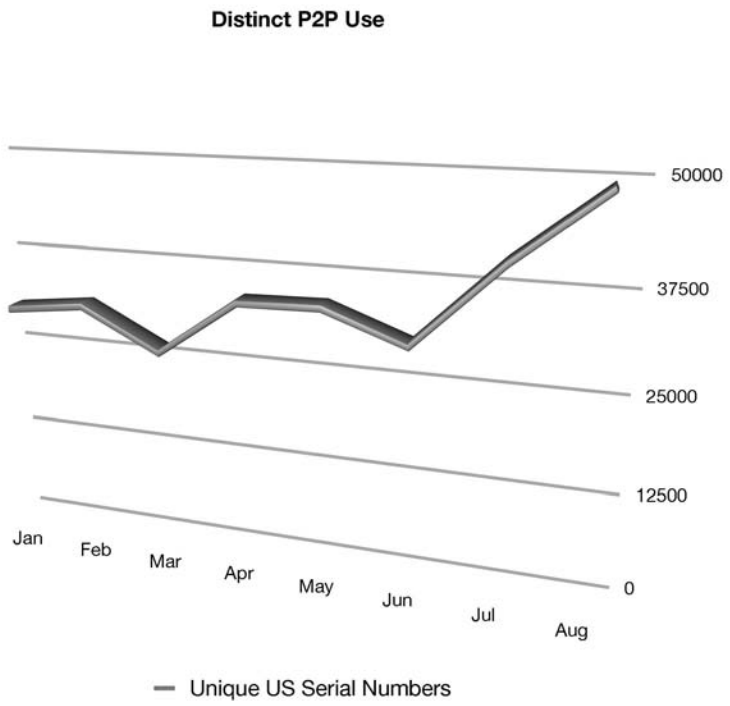
During undercover operations officers are presented with the same search results viewable by the predator using the system in their home. These results contain hundreds if not thousands of images of child sexual abuse and are a virtual menu of movies depicting the brutal rape of children as young as infants. Based on the preference of the user, downloads can focus on children being tied up, abused by adults, forced to have sex with animals or any combination thereof.

Investigators can download thirty minute movies complete with sound where an adult is forcibly penetrating a child. The user can listen to the child cry out for help as the video permanently memorializes each horrifying moment.

Problem Scope

The software used on this particular network maintains a unique serial number for each installed system. During undercover operations, investigators track these serial numbers to get a global perspective of individual users. Previously, investigators could only document the Internet Protocol addresses (IP) of these users, however, since IP addresses are dynamic and subject to frequent change, it is difficult to get a conclusive picture of the volume of individual trafficking.

With that in mind, the following chart represents the number of unique users identified trading child sexual abuse imagery in 2007. The numbers for each month represent one software application on one P2P network. These are only the U.S. offenders found by law enforcement during undercover operations.



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
Unique US Serial Numbers	30817	32017	26976	34167	34443	30803	41073	49554

Unique Traders

In the chart labeled Distinct P2P use we can see that over forty-nine thousand unique systems were found trading child sexual abuse imagery in August, 2007. That number represents the latest statistics available at the time of this report and we can see a continuing trend in the increase of this activity even though law-enforcement has been trying to disrupt this system for three years.

The monthly totals listed only depict unique use during that month. In most cases these users were also reflected in prior months. A review of the complete seven month period reveals 193,626 unique computers in the United States located by law enforcement trafficking child sexual abuse imagery. This ability to track serial numbers was implemented in late 2005. Since that time we have identified 377,044 unique serial numbers related to this activity.

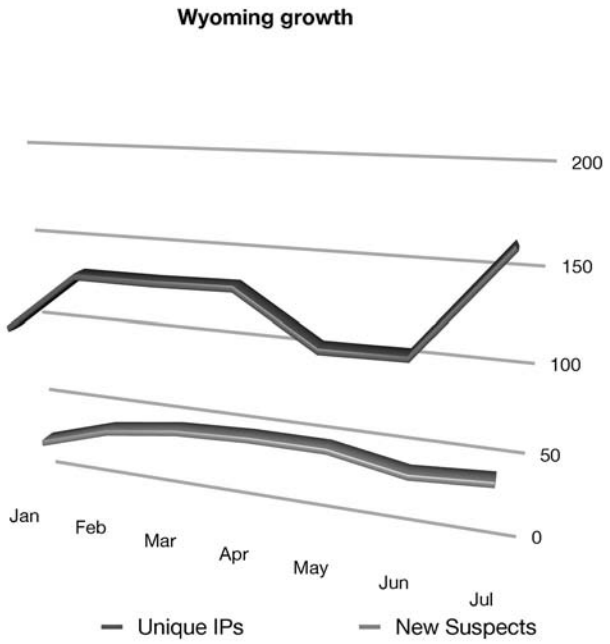
We should note that individuals using two computers or who purchase a new computer will be reflected twice in these numbers. Simply upgrading the software does not change this serial number for the application reported. In Wyoming, we have seen only two cases out of over 100 search warrants served where an individual had two serial numbers associated with their activity.

Impact

The impact of these traders on law enforcement's ability to respond has been catastrophic. This one small segment of the Internet has caused the investigative and forensic infrastructure to be overwhelmed. In Wyoming alone we are behind over eight hundred (800) search warrants. With Wyoming being the smallest state by population, it is not difficult to imagine how these offenses have crippled much larger jurisdictions.

Growth

In Wyoming we send process on each IP address found during these undercover operations. Resulting records allow us to match the number of new IP addresses to the number of new individuals trading child sexual abuse material in Wyoming.



	Jan	Feb	Mar	Apr	May	Jun	Jul	Cumula-tive
Unique IPs	107	139	139	140	113	114	169	921
New Suspects	29	42	48	50	50	42	45	306
% of Unique IPs	27.1%	30.2%	34.5%	35.7%	44.2%	36.8%	26.6%	33.2%

The steady increase in Wyoming has continued to tax an already overwhelmed system. We have specific records that demonstrate how many IP addresses refer to specific individuals. Over the first six months of 2007 we were able to show that the nine hundred twenty one (921) unique addresses related to three hundred and six (306) individuals.

There have been 1,519,791 unique IP addresses identified in the United States. If the breakdown were constant with the results in Wyoming that would indicate 504,947 individuals identified throughout the United States in the last three years. This is a rough estimate but again, it only pertains to one of many P2P systems and does not include other methods of trading child sexual abuse material.

Methodology

Conducting the undercover portion of these P2P operations is fairly simple. Investigators use the search terms known to law enforcement to identify advertised child sexual abuse material. The investigator then initiates downloads and starts to identify IP addresses. Be examining these addresses the investigator can see where an offender is located. This allows each investigator to focus their efforts within their own jurisdiction.

Once an offending computer has been identified in the local jurisdiction the investigator may download child pornography directly from the suspect computer. As this progresses the investigation is documented and memorialized through software applications. Investigators will also check the reported IP address for involvement in previous activities related to child sex crimes. Often records will be found associating the address with other investigations.

Once criminal conduct is confirmed the investigator sends process to the Internet Service Provider (ISP). This request will attempt to identify the physical address associated with the IP address. Most frequently this will match a residence or business with a paid Internet account. If the ISP has records the investigator can continue the investigation.

Investigators will then research the location provided. Investigators will attempt to identify the occupants as well as immediate risks to children. Criminal history information will be obtained if available to help establish the priority of the investigation.

Once all background material has been reviewed a decision to apply for a search warrant will be made. If a warrant is appropriate an application will be submitted to a local or federal prosecutor. If approved, the application then goes before the appropriate judge. If signed the investigators have a limited amount of time to execute the warrant and seize any evidence found.

Interviews may be conducted pursuant to the investigation. All digital evidence will be submitted for forensic examination. Depending on the evidence and the potential for risk to individuals an arrest may be made during the execution of the warrant.

Rescues

These P2P undercover investigations have resulted in the rescue of many children.

Mr. SCOTT. Thank you. Ms. Collins?

TESTIMONY OF MICHELLE COLLINS, DIRECTOR, EXPLOITED CHILD DIVISION, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

Ms. COLLINS. Thank you, Mr. Chairman, and the distinguished Members of Committee. As the Director of the Exploited Child Division at the National Center for Missing and Exploited Children, I welcome this opportunity to appear before you to discuss crimes against children on the Internet.

The National Center 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. The National Center is a not-for-profit corporation mandated by Congress and working in partnership with the Department of Justice as the national resource center and clearinghouse on missing and exploited children.

One of our programs is the CyberTipline. It acts as the 911 of the Internet. It serves as the national clearinghouse for investigative leads and tips regarding crimes against children on the Internet. Congress mandated that the National Center establish and operate the CyberTipline in its Justice Department appropriations legislation for fiscal year 1998.

The CyberTipline operates in partnership with the FBI, with ICE, with the U.S. Postal Inspection Service, with the U.S. Secret Service, the Department of Justice's Child Exploitation and Obscenity Section, the nationwide Internet Crimes Against Children Task Forces, as well as all State and local law enforcement agencies here in the United States.

Since the CyberTipline began operation, the National Center has received and processed more than 525,000 reports regarding child sexual exploitation, resulting in hundreds of arrests and prosecutions. These leads come from both the public as well as electronic service providers, which we call ESPs. They are mandated to report to the CyberTipline any images of apparent child pornography under section 13032 of Title 18 of the U.S. Code. Reports are prioritized, processed, and then submitted to the appropriate law enforcement agency by our analysts.

The FBI, ICE, and the Postal Inspection Service have real-time access to the leads, and all three agencies assign agents and analysts to our building. Rapid dissemination of CyberTipline reports is accomplished using Virtual Private Network connections. ESPs, the electronic service providers that are registered with the CyberTipline, use a secure Web site to upload images of apparent child pornography directly onto our server, which we then encrypt. The VPN is also used to transmit these images and the CyberTipline reports to the National ICAC task forces, which also have secure, encrypted connections into the CyberTipline. The majority of the CyberTipline leads are referred to the 46 federally-funded ICAC task force agencies, one of the most effective initiatives in the fight against online child sexual victimization.

It was Congress in 1997 that conceived the idea of creating specialized units to investigate these types of crimes. In the 10 years since then, the national ICAC program has become a model of suc-

cessful Federal oversight of State and local programs, which though geographically diverse, are united by national standards with investigative policies and procedures. The national ICAC program complements the Federal agencies efforts as they work seamlessly in the fight against online victimization.

The typical analysis of a report that we would receive from an electronic service provider begins with taking in whatever information that company provides to us, and then we try match it to other online activity. Conducting online searches is one method we use to try to connect a real person to their online identity. We use both publicly available search tools, as well as commercial search tools that are often given to the National Center at no cost.

These searches often turn up information valuable to law enforcement, including whether or not the offender has legitimate access to a child, such as a school bus driver. Law enforcement will want to move quickly in cases where a child could be in imminent danger. Using the information we gather from the CyberTipline, law enforcement serves legal process, gathers evidence, and obtains probable cause to arrest of the perpetrator.

In our experience, the child victims would have never told anyone about their abuse. Their perpetrator would have remained anonymous but for the CyberTipline, and despite what should have been the obvious clues to the true nature of the offender.

Who are the children that we see in these images every day? Of the identified offenders in a one-year period 83 percent of them had images of children being sexually abused under the age of 12, 39 percent had images of children under the age of 6, while 19 percent of the offenders had images of children being sexually abused under the age of 3 years old.

Because of our role as a clearinghouse for online crimes against children and the reputation we have earned while assisting law enforcement, our analysts have seen more child pornography than any law enforcement agency in the world. This benefits our Child Victim Identification Program, a joint project with our Federal law enforcement partners and the ICAC task forces to identify children who are being actively abused, as well as assist with prosecution of these cases.

At this point we know of at least 1,200 child victims who have been rescued. And thankfully, I can report to you that the child that you are viewing here has been rescued by law enforcement.

Today we are working with leaders in the Internet industry to explore improvements, new approaches, and better ways to attack the problem. NCMEC urges the Committee to take a serious look at the dangers threatening our children, moving decisively to provide law enforcement with the tools that they need to identify and prosecute those who victimize our children.

Thank you very much.

[The prepared statement of Ms. Collins follows:]

PREPARED STATEMENT OF MICHELLE COLLINS

Mr. Chairman and distinguished members of the Committee, as the Director of the Exploited Child Division of the National Center for Missing & Exploited Children (NCMEC), I welcome this opportunity to appear before you to discuss crimes against children on the Internet. 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. 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 under Section 5773 of Title 42 of the United States Code, which is attached.

These include 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 programs designed to help stop the sexual exploitation of children.

One of our programs is 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. Congress mandated that NCMEC establish and operate the CyberTipline in its Justice Department appropriations legislation for fiscal year 1998, which is attached. The 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, the national Internet Crimes Against Children Task Force (ICAC) program, and 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.

Since the CyberTipline began operation, NCMEC has received and processed more than 525,000 leads, resulting in hundreds of arrests and successful prosecutions. These leads come from both the public and electronic service providers (ESP), which are mandated to report under Section 13032 of Title 18 of the United States Code.

Reports are prioritized, processed and submitted 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 on-site at NCMEC and review the reports. We are not authorized to send CyberTipline reports to foreign law enforcement agencies. This is a real problem, considering the global nature of the Internet.

Rapid dissemination of CyberTipline reports is accomplished through the use of Virtual Private Network (VPN) connections. ESPs that are registered with the CyberTipline use a VPN to upload images of apparent child pornography directly into our server. These images are encrypted for additional security. The VPN is also used to transmit images and CyberTipline reports to the national ICAC program, which also has a secure, encrypted connection to the NCMEC system.

The majority of CyberTipline leads are referred to the 46 federally funded ICAC taskforce agencies, one of the most effective initiatives in the fight against online child victimization. It was Congress that, in 1997, conceived the idea of creating specialized units to investigate these crimes. In the 10 years since then, the national ICAC program has become a model of successful federal oversight of state and local programs which, though geographically diverse, are united by national standards of investigative policies and procedures. The national ICAC program complements the federal agencies' efforts, as they work seamlessly in the fight against online child victimization.

A typical analysis of an ESP report begins by taking whatever information is in the report and trying to match it to other online activity. Conducting online searches is one method we use to try to connect a real person to the online criminal conduct. We use both publicly-available search tools as well as commercial search tools that are given to us at no cost by our corporate partners.

Because Congress intended the CyberTipline to augment rather than replace established law enforcement procedures, the information we provide is only the first step in the process. Our searches turn up information that is valuable to law enforcement, including whether the perpetrator has legitimate access to children—such as a school bus driver. Law enforcement will want to move quickly in cases

where children could be in imminent danger. Using the information we gather, law enforcement serves legal process, gathers evidence, and obtains probable cause to arrest the perpetrator.

An obstacle to this process is that not all ESPs are reporting and those that do report are not sending uniform types of information, rendering some reports useless. Some ESPs take the position that the statute is not a clear mandate and that it exposes them to possible criminal prosecution for distributing child pornography themselves. In addition, because there are no guidelines for the contents of these reports, some ESPs do not send customer information that would allow NCMEC to identify a law enforcement jurisdiction. As a result, potentially valuable investigative leads are left to sit in the CyberTipline database with no action taken.

There is also another necessary yet missing link in the chain from detection of child pornography to conviction of the distributor. Once the CyberTipline analysts give law enforcement all the information they need about specific images traded on the Internet, there can be no prosecution until the date and time of that online activity is connected to an actual person. There is currently no requirement for ESPs to retain connectivity logs for their customers on an ongoing basis. Some have policies on retention but these vary, are not implemented consistently, and are for too short a time to have meaningful prosecutorial value. One example: law enforcement discovered a movie depicting the rape of a toddler that was traded online. In hopes that they could find the child by finding the producer of the movie, they moved quickly to identify the ESP and subpoenaed the name and address of the customer who had used that particular IP address at the specific date and time. The ESP was not able to provide the connectivity information. To this day, we have no idea who or where that child is—but we suspect she is still living with her abuser.

In the cases we have seen, the child victims would have never told anyone about their abuse, and their perpetrators would have remained anonymous but for the CyberTipline and vigorous law enforcement investigation.

Who are the children in the images we see every day? Of the identified offenders in a one-year period, 83% had images of children younger than 12 years old, 39% had images of children younger than 6 years old, and 19% had images of children younger than 3 years old.

Because of our role as a clearinghouse for online crimes against children, and the reputation we've earned for assistance to law enforcement, our analysts see more child pornography than any law enforcement agency in the world. This benefits our Child Victim Identification Program, a joint project with our federal law enforcement partners and the national ICAC task force program, whose mission is two-fold: (1) to help prosecutors get convictions by proving that a real child is depicted in child pornography images; and (2) to rescue the children. To date we have records relating to almost 1200 identified child victims.

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. The CyberTipline is a tool used by law enforcement to apprehend those who use the Internet to victimize children.

Today, NCMEC is working with leaders in the Internet industry in order to explore improvements, new approaches and better ways to attack the problems. We are also bringing 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.

NCMEC urges the Committee to take a serious look at the dangers threatening our children today, and to move decisively to provide law enforcement with the tools they need to identify and prosecute those who target our children.

Now is the time to act.

Thank you.

Mr. SCOTT. Thank you. Mr. Weeks?

TESTIMONY OF GRIER WEEKS, PROTECT, INC.

Mr. WEEKS. Chairman Scott, Ranking Member Forbes, and distinguished Members, thank you for having us. I am Grier Weeks, Executive Director of the National Association to Protect Children. We are a grassroots organization that is active in the States and now in Washington on this Federal issue.

I am going to depart from my remarks. Just to be brief here, I am going to focus on the one thing that this Congress is consist-

ently not hearing year after year at these hearings, and that is a frank assessment of the state of readiness of law enforcement at the Federal, State, and local level. Let me begin by reviewing what we know about the magnitude of this crisis.

First, we know that there are hundreds of thousands of individuals within the U.S. Right now actively engaged in these crimes, hundreds of thousands. The Department of Justice has testified before Congress to this. And as you have heard from Agent Waters, this is a matter of fact.

Second, we know that these individuals are responsible for hundreds of thousands of child victims in the United States. Everything we know about the rate of victimization, the number of victims tells us that if there are a half a million people out there trafficking in child pornography, that you are talking about hundreds of thousands of child victims.

Third, we know that these hundreds of thousands of perpetrators are committing millions of crimes. That is important, because the volume of crimes is the best indicator we have of what is essentially a market demand, a crushing market demand for more and more product, which can only be provided by the rape and torture of more children.

The most important thing, perhaps, that we know is we can prevent this. This is entirely unnecessary. Because of the innovative law enforcement techniques that Agent Waters has talked about, the FBI is engaged in, we know where these guys are. And there is no reason in the world why these children should continue to suffer because we won't get up and go get them.

Only a token of these cases, as you have heard today, are ever investigated. According to the FBI, in the 6½-year period between fiscal year 2001 and mid-2007, the number of suspects identified and arrested by the FBI for online child exploitation crimes was 5,048. The ICAC program, comprised of 46 task forces nationwide, reports just over 2,000 arrests in fiscal year 2006. We don't have reliable numbers on ICE and Postal, but they would be considerably smaller.

All of this, though, is no fault of these heroes that are out there on the front lines doing this work. And I want to emphasize that clearly. As of July 11th, the FBI's Innocent Images National Initiative, based in Calverton, had just 32 staff, including 13 agents. Now, in previous congressional testimony, the FBI and Department of Justice have emphasized essentially the full-time equivalents, but I think it is important that this Committee understands the very inadequate, grossly inadequate size of this unit itself.

The Innocent Images congressional appropriation last year was $10 million. That is less than half of what HUD gave to Jersey City, New Jersey, for housing and community development. In fiscal year 2006, the budget for the entire ICAC task force program, which is a tremendous success, was 14½ million. After years of administration neglect and mounting congressional scrutiny, the Department of Justice has finally increased that by $11 million, but we are talking about a quarter of one bridge in Alaska, the Bridge to Nowhere.

Law enforcement also suffers from a critical lack of forensic resources at every level. In your States and at the Federal level we

hear again and again people waiting 8 months to get a hard drive analyzed. How is this possible? How in a country where you can't go a single night without hearing about sex offenders, you have got TV shows about sex offenders, how is it possible that we can have a flourishing criminal marketplace in children that goes on with impunity?

Let me take a stab at that, and I will conclude with our insight into why this has been allowed to happen. In 1996, the World Wide Web really took off. That was the year that the public became aware of it and started to use the World Wide Web. That was also the year that Megan's Law was passed, which is a good piece of legislation. But I want to point out that Megan's Law, which imposed a form of citizen supervision on released sex offenders, became essentially the whole paradigm for how this country thinks about child sexual abuse. It became the way we talked about it, the way we legislated about it, and it was popular because it was cheap, it was irresistible to the media, and it was popular.

As that decade wore on and we talked consistently about registered sex offenders, child pornography exploded. Children became a commodity in an underground economy, and law enforcement continued to fall farther and farther behind. Law enforcement was not given the personnel, the equipment, the training, the forensic labs, or any of the other support they needed to go find these kids and rescue them. Year after year we heard unbelievable rhetoric. The Administration talked tough, but refused to support law enforcement. Year after year they refused to even shoot straight with Congress about what the resources really were and what they needed.

It got so bad that finally last year Congressman Joe Barton from Texas practically begged the Department of Justice to tell them what they needed from Congress. It was apparently useless. By the end of the Megan's law decade, America ended up with an enormous surplus of rhetoric about sex offenders and a severe deficit of resources to do anything about them. We were spending millions hunting for sex offenders who failed to register their addresses, while ignoring legions of new sexual predators whose locations we do know. We were doing the things that cost the least and sound the toughest, while neglecting the things that cost real money and could save the most lives.

Now the 110th Congress has the opportunity to do what the 109th Congress and this Administration did not: Fight back, pay what it costs, disrupt this market, and go get these children. You have the opportunity to show America and 50 State legislatures a little less talk and a lot more action. You can launch the toughest offensive against child sexual predators this Nation has ever seen.

It will also be the largest child abuse prevention campaign in history, and I will just add that millions of American taxpayers from all walks of life will be behind you 100 percent.

Thank you.

[The prepared statement of Mr. Weeks follows:]

PREPARED STATEMENT OF GRIER WEEKS

Chairman Conyers, Ranking member Smith, distinguished members, thank you for the opportunity to testify today. I am Grier Weeks, executive director of the National Association to Protect Children, or PROTECT. PROTECT was established in

2002 as a grassroots membership association that works to promote legislation with one exclusive aim: child protection. We work primarily in state legislatures to win stronger laws for child protection, and last year helped secure greater funding for law enforcement to combat child exploitation in California, Tennessee and North Carolina. For the past two years, we have done extensive research into the magnitude of the problem nationally and what law enforcement at all levels of government needs to combat this crisis.

You are hearing today from some of the foremost experts on child exploitation in the United States. When it comes to data on the nature, scale and magnitude of child pornography trafficking, there is not even a close second to ICAC Agent Flint Waters. In the FBI's Arnold Bell, you have a seasoned veteran who has spent years at the very center of national and international anti-child exploitation law enforcement efforts.

I will confine my testimony, therefore, to the one set of facts that Congress urgently needs but has not been given during previous legislative hearings on this subject: a frank assessment of the state of readiness of our federal, state and local law enforcement agencies to combat this epidemic.

HUNDREDS OF THOUSANDS OF PREDATORS ARE AT LARGE

Let me begin by reviewing what we know about the magnitude of this crisis. First, we know that there are hundreds of thousands of individuals within the United States who are actively engaged in child pornography crimes. Assistant Attorney General Alice S. Fisher gave this testimony to the House Energy and Commerce Committee in 2006.[1] Agent Flint Waters, the primary architect of the Internet Crimes Against Children (ICAC) information-sharing network and the one person who has compiled the most data on trafficking, estimates there are at least 350,000 such criminal offenders within the U.S.[2]

HUNDREDS OF THOUSANDS OF CHILD VICTIMS

Second, we also know these individuals are responsible for hundreds of thousands of child victims, whether of child pornography production or other forms of direct sexual assault. FBI Cyber Crimes Division Chief Raul Roldan gave this testimony to Congress in 2006.[3] Both research and anecdotal evidence tell us that a majority of those arrested for so-called "simple possession" of child pornography are known to have sexually assaulted children or attempted to.[4] Most of these children are preyed upon not by strangers, but by adults in their own daily circle of trust. Child pornography in the U.S. is largely a home-grown, cottage industry.

MILLIONS OF CRIMES, A MULTI-BILLION DOLLAR MARKET

The third important fact we know is that these hundreds of thousands of individuals commit *millions of crimes* each year.[5] This distinction between offenders and crimes is not an academic one, because the volume of crimes being committed is our best indicator of the crushing market demand for new "product." This is a market estimated to range in the billions of dollars annually,[6] although it also thrives on barter. This demand drives the rape and torture of more American children every day.

WE CAN PREVENT THIS

Finally, perhaps the most important thing we know is that we can prevent this. Thanks to the innovative high tech investigations of the ICACs and federal agencies, law enforcement can now locate tens of thousands of the predators referred to by Ms. Fisher, Mr. Roldan and Agent Waters. In one recent 30-day period, the ICAC Data Network gathered evidence on individuals trafficking in child pornography

[1] Testimony of Alice S. Fisher, U.S. House Energy and Commerce Committee, May 3, 2006
[2] Correspondence between Flint Waters, Wyoming Division of Criminal Investigation and PROTECT
[3] Testimony of Raul Roldan, U.S. House Energy and Commerce Committee, May 3, 2006
[4] "Child Pornography Possessor Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Survey, University of New Hampshire Crimes Against Children Research Center / National Center for Missing and Exploited Children, 2005; Testimony of Andres Hernandez, U.S. House Energy and Commerce Committee, September 26, 2006
[5] Testimony of Flint Waters, U.S. House Energy and Commerce Committee, April 6, 2006
[6] National Center for Missing and Exploited Children estimate

from nearly 50,000 unique locations.[7] These criminals are now caught in a web of their own making.

ONLY A TOKEN PERCENTAGE INTERDICTED

If there were hundreds of thousands of active bank robbers at large in the United States, we might declare a national state of emergency. But these are just children. Only token number of these crimes will ever be investigated. Law enforcement agencies at the federal, state and local level are overwhelmed and are triaging.[8]

According to the Federal Bureau of Investigation, in the six and a half year period between FY 2001 and mid-2007, "the number of suspects identified and arrested by the FBI for online child exploitation" crimes was 5,048.[9] The ICAC program, comprised of 46 task forces nationwide, reports just over 2,000 arrests nationwide in FY '06.[10] We do not know of reliable numbers from Immigration and Customs Enforcement or the U.S. Postal Inspection Service, but they would be smaller than either the FBI's or the ICAC networks.

LAW ENFORCEMENT AGENCIES STARVED FOR FUNDING

All of this is no fault of the heroes who work at the FBI, ICE, U.S. Postal Inspection Service and the ICAC Network.

As of July 11th, the FBI's Innocent Images National Initiative, based in Calverton, Maryland, had just 32 staff, including 13 agents. Previous Congressional testimony by the Bureau has emphasized the total number of full-time equivalents assigned to child exploitation cases agency-wide, which is around 260.[11] But it is important that Congress understands the grossly inadequate size of this unit itself.

The Innocent Images Congressional appropriation in FY '06 was $10 million. That's less than the U.S. Department of Housing and Urban Development gave to Jersey City, New Jersey last year for housing and community development.[12] The FBI supplemented this with approximately $23 million in discretionary funds.

In FY '06, the budget for the entire Internet Crimes Against Children task force program, which has been tremendously successful, was $14.5 million.[13] After years of administration neglect and mounting Congressional scrutiny, the Department of Justice finally doubled funding for this program in 2007. However, funding for this bridge to safety for children is still less than one-fourth the federal investment in Alaska's infamous "Bridge to Nowhere" (Gravina Island project).[14]

Law enforcement also suffers from a critical lack of computer forensic resources. No FBI lab is dedicated to crimes against children, and agents at all levels of government report typical wait times for forensic work of around 8 months. This bottleneck not only limits prosecution, but it often leaves victims in danger while authorities wait for evidence.

TIME FOR A CHANGE OF POLICY IN WASHINGTON

How is any of this possible? How—in a nation where not a single night goes by without a television show or newscast on the topic of "sex offenders"—can a flourishing criminal marketplace prey on American children with such impunity? I will conclude by offering our insight into this question.

It was just 1996, eleven years ago, that the world wide web took off, facilitating what would become a vast new online marketplace for child exploitation. Nineteen ninety-six was also the same year that Megan's Law was enacted, facilitating a decade of public awareness about child sexual abuse.

Megan's Law—which imposed a form of citizen supervision on released sex offenders—was enormously popular, far cheaper than intensive surveillance and control by parole or probation officers, and irresistible to the news media. It quickly became a virtual paradigm for how America would think about, talk about and legislate about child sexual abuse. And although "registration" was a surprisingly weak response to the problem, it was the wellspring for a decade-long flood of often-partisan "get tough" rhetoric.

---

[7] Information provided to Sen. Joseph Biden by ICAC Data Network, October, 2007

[8] A law enforcement panel testifying before the U.S. House Energy and Commerce committee on April 6, 2006 discussed the triaging of child exploitation cases.

[9] FBI letter to Sen. Joseph Biden, July 11, 2007

[10] Office of Juvenile Justice and Delinquency Prevention, U.S. Department of Justice

[11] FBI letter to Sen. Joseph Biden, July 11, 2007

[12] "HUD Announces $12.7 Million for Affordable Housing and Community Development in Jersey City, U.S. Department of Housing and Urban Development news release April 20, 2006

[13] "2007 Budget Highlights," U.S. Department of Justice

[14] Despite much controversy over this project in Washington, progress continues using federal funding. See the Gravina Access Project website at http://dot.alaska.gov/gravina/

Meanwhile, as the decade wore on, child pornography trafficking exploded exponentially. Children became a commodity in a new underground economy, and law enforcement began to fall farther behind. Those on the front lines were not given the basic personnel, equipment, training, forensic labs or other support they needed to protect American children.

Year after year, the administration talked tough, but refused to support law enforcement, even in the face of an unfolding domestic human rights catastrophe. Year after year, the administration failed to even shoot straight with Congress about the magnitude of the problem law enforcement was seeing and to ask for meaningful budget increases. Finally, in 2006, Rep. Joe Barton practically begged the Department of Justice in a public hearing to ask Congress for more help combating child exploitation, to no avail.[15]

By the end of the Megan's Law decade, America ended up with an enormous surplus of rhetoric about sex offenders and a severe deficit of resources to do anything about them. We were spending millions hunting for ex-offenders who failed to register their addresses, while ignoring legions of new sexual predators whose locations we *know*. We were doing the things that cost the least and sound the toughest, while neglecting the things that cost real money and could save the most lives.

Now, the 110th Congress has the opportunity to do what the 109th, and this administration, did not: Fight back. Pay what it costs. Disrupt this market. Go get these children.

You have the opportunity to show how America, and 50 state legislatures, a little less talk and a lot more action. You can launch the toughest offensive against child sexual predators this nation has ever seen, as well as the largest child abuse prevention campaign in history. Millions of American taxpayers from all walks of life will be behind you 100 percent.

Mr. SCOTT. Thank you, Mr. Weeks. Mr. Ryan?

TESTIMONY OF JOHN RYAN, GENERAL COUNSEL, AOL

Mr. RYAN. AOL thanks Chairman Scott, Ranking Member Forbes, and the distinguished Members of this Committee for the opportunity to appear before you today to discuss the issue of online child protection. AOL strongly supports the efforts of this Committee, and shares the goal of protecting children's experience online and safeguarding online users from predators.

My name is John Ryan, Chief Counsel at AOL, where I oversee our efforts to assist law enforcement and keep criminal activity off our networks. Prior to joining AOL, I was a prosecutor in New York, where I investigated and prosecuted numerous high-tech crimes, including crimes against children. I am a founding member of the Electronic Crimes Task Force in New York, which has been used as a model for cooperation between law enforcement and industry in the prosecution of electronic crimes.

The story that I believe needs to be told today is the extraordinary work that we and other online companies have done to protect children online. Those include technology solutions that provide children with safe areas and provide parents with tools to guard and monitor their children's activities, provide law enforcement with tools and assistance needed to investigate and prosecute Internet-related crimes, our educational efforts to empower parents and children, and our ongoing work with others in the Internet community to develop best practices and solutions. For AOL these efforts make good business sense but, more importantly, are the right thing to do.

A decade ago, AOL pioneered the concept of parental controls, to give parents powerful tools to enable them to set and enforce safety rules for their children's online activities. With AOL's still indus-

[15] U.S. Energy and Commerce Committee hearing, May 3, 2006

try-leading products, parents can now set time limits for online activity, decide whether their children can e-mail and IM, and if so, with whom, choose the Web sites and products they can access, and even get a report on their child's online activities, essentially report card on where they have been and what they have done.

These amazing capabilities have been recognized in a recent landmark decision in the COPA matter. The Federal District Court in Philadelphia recognized that AOL's parental controls blocked over 98 percent of sexually explicit Web sites, and that 87 percent of parents found them easy to use.

Now AOL has made their parental controls free of charge, even to non-AOL users. AOL also offers other tools, such as a visible and convenient "notify AOL" button, for members to report unacceptable or illegal behavior to teams of trained professionals who work closely with law enforcement.

Finally, AOL produces and provides alternative Web programming for children and teens so that they can have a positive Internet experience. Collectively, these are extraordinary tools provided by our industry to parents to protect their children.

In 1999, Congress passed important legislation that required service providers to report apparent images of child pornography to the National Center. This legislation actually reflected a practice that AOL had undertaken several years prior, enabling AOL to begin immediate compliance. To improve reporting further, theindustry developed a broader sound practices document that encourages referral of offending images and other valuable information to NCMEC in order to ensure that law enforcement has sufficient basis for a quick follow-up.

In 2006, AOL and other leading service providers submitted nearly 30,000 reports related to child pornography and endangerment. Those are 30,000 child pornography cases that likely would have gone unnoticed.

We also respond effectively to law enforcement inquiries. This past August, Pennsylvania law enforcement told us they urgently needed to find the location of a child molester who was abusing two children and broadcasting video of the abuse in real-time. Working with law enforcement, AOL was able to provide the police with the location, and the police caught the molester in the act and rescued the children.

AOL's efforts do not simply stop at reporting evidence of crimes. AOL has a team of highly trained and dedicated professionals, including former prosecutors, who assist on tens of thousands of cases per year. We have a 24-hour dedicated law enforcement hotline to respond to law enforcement requests in a timely basis.

Since 1995, we also offer pretrial litigation support, as well as fact and expert witness testimony in criminal cases involving records obtained from AOL.

The important message is while there are ways to enhance these processes even further, the underlying framework for reporting crimes, preserving evidence, and cooperating with law enforcement are strong and effective. The processes that Congress and industry put in place really do work.

We also continue to innovate. AOL implemented extremely effective technologies to identify, detect, and remove child pornography

images from any transmission within our network. In addition to the detection, we collect them and forward them onto the National Center, and then work with law enforcement for ultimate prosecution.

We were the first provider to work online with the AMBER Alert program, and we now use that same technology to alert campuses on safety issues after the tragedy at Virginia Tech. We also recently instituted with the National Center a dedicated area where they can set up a space, since they have been designated as the Emergency Child Locator Center, in light of the tragedy at Katrina.

So our work is ongoing, and we look forward to working with this Committee to develop further strategies.

[The prepared statement of Mr. Ryan follows:]

PREPARED STATEMENT OF JOHN RYAN

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

HEARING ON

"SEX CRIMES AND THE INTERNET"

WRITTEN TESTIMONY OF
JOHN D. RYAN
CHIEF COUNSEL
PUBLIC SAFETY AND CRIMINAL INVESTIGATIONS
AOL LLC
DULLES, VIRGINIA

October 17, 2007

AOL thanks Chairman Conyers, Ranking Member Smith, and the distinguished members of this Committee for the opportunity to appear before you today to discuss the issue of online child protection. AOL strongly supports the interest and efforts of the Committee to address this issue, and shares the goals of protecting children's experience online, and safeguarding online users from predators.

My name is John D. Ryan, Chief Counsel at AOL, where I oversee our efforts to assist law enforcement and keep criminal activity off our networks. Prior to joining AOL, I was a prosecutor in New York, where I investigated and prosecuted numerous high-tech crimes, including crimes against children. I am a founding member of the Electronic Crimes Task Force in New York, which has been used as the model for cooperation between law enforcement and industry in the prosecution of electronic crimes.

AOL has worked diligently to address the issues of child pornography and predation both on our network and on the Internet for more than a decade. My testimony today will focus on several key areas in AOL's effort to promote Internet safety: (1) the technological solutions that provide safe areas for children and parental tools to monitor their activities; (2) our strong partnership with law enforcement; (3) our educational efforts to empower parents and children; and (4) and our ongoing work with others in the Internet community to develop best practices and solutions. For AOL, these efforts make good business sense, but more importantly, are the right thing to do.

I. AOL's Technology Solutions Provide a Safer Online World for Kids

The Internet and the AOL service provide unprecedented communication, education, and entertainment tools for children. Unfortunately, there have been situations where individuals have taken advantage of children online. AOL is committed to protecting children from victimization by online predators or exposure to inappropriate content. The protection of children online is a critical goal and can only be accomplished

through cooperation of industry, law enforcement, educators and parents. What AOL brings is experience and expertise in technical innovation that provides the tools that the other partners can use to help protect children.

A. Parental Controls

A decade ago, AOL introduced the most powerful technology to help parents manage and oversee their children's activities online: state-of-the-art Parental Controls. AOL Parental Controls are available to any parent, regardless of whether they are an AOL member, and without a fee. The technology allows parents to make the decisions about what type of online experiences their children should have and with whom, and to oversee—through regular updates on child online activity—how their children are being protected and parental decisions enforced.

Let me explain how the technology works. Parental Controls are broken down into three age categories: Kids Only for ages 12 and under; Young Teen (13-15); and Mature Teen (16 and 17). Once parents assign their children to one of these categories, certain default protections apply. In addition, the technology is flexible so that parents can decide who their children can email or Instant Message ("IM"), what Web sites they can visit, and whether they are permitted to enter chat rooms, which are fully monitored by internal AOL enforcement teams. AOL Parental Controls also have practical features such as a timer that enables parents to monitor the amount of time spent online, with the ability to customize daily limits, as well as access controls that prevent a child from bypassing Parental Controls settings by using other Web access software. These protections are also integrated across AOL products and services.

As an additional protection, AOL has a feature called Web Guardian that allows parents to receive regular reports on their children's online activities. Parents who subscribe to this service receive a list for every session on AOL detailing all of the Web sites their children visit, which sites they attempted to visit, but were blocked from accessing; and how many e-mails and IMs they sent. AOL provides more than 1 million AOL Guardian reports to parents every week. All of these tools have been highly effective in educating and involving parents regarding their children's Internet experiences and technology more generally, which are key to empowering them to be able to guide their children toward safe and rewarding online experiences.

AOL Parental Controls do not merely restrict a child's access to potentially harmful encounters on the Internet. They also provide positive alternatives with a complete range of age-appropriate programming for parentally controlled accounts. AOL also has state-of-the-art Web filters that allow our Mature Teen visitors to access a much broader range of content while still blocking offensive content. AOL filters are able to rate the content of pages in real time and deliver only those pages that are appropriate, while blocking offensive sites. This gives teens the flexibility to use the Web while affording the maximum protection.

In a recent case, ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. PA 2007), the Court evaluated the parental controls of various Internet service providers ("ISPs") and concluded that, "the testimony of the witnesses as well as the evidence excerpted and referenced in these Findings of Fact are true, reliable, and credible and I accept those facts and that testimony as the foundation of the following Findings of Fact and Conclusions of Law." Id. at 781. Among those findings the Court noted that, "85 percent of parents are highly satisfied with their AOL Parental Controls products, and that 87 percent of parents find them easy to use." Id. at 794. The Court further observed, "that some products, such as AOL's filter, blocked close to 100 percent of all pornography or erotica when the most restrictive setting (for children under the age of 12) was chosen." Id. at 795. Finally, the Court found that, "web pages that were returned in response to the most popular search terms, the AOL filter performed the best and blocked 98.7 percent of sexually explicit Web pages." Id. at 796. The facts that the Court found with respect to AOL were not an accident. They reflect the dedicated effort of AOL over more than a decade to provide a parental control product that offers real protections for children.

B. Removal of Child Pornography

Four years ago AOL implemented extremely effective technologies to identify and remove images of child pornography and to eliminate the sending of known child pornography through email. AOL developed a process that creates unique digital signatures from apparent pornographic images of children and uses these signatures to eliminate further dissemination of such images. AOL has assembled a library of these signatures and, if AOL identifies that someone is attempting to send a file through its network with a signature from that library, AOL prohibits the sending of that file and refers that image to the National Center for Missing and Exploited Children (NCMEC) to be investigated and prosecuted. Once the signature of the image is identified and referred to NCMEC, AOL deletes all record of the image and retains only the signature for future identification of such images. This procedure provides law enforcement with all of the information they require to initiate an investigation while insuring that a child is not re-victimized. As I will discuss in more detail in a moment, this approach has now become part of a broader, cooperative industry effort to remove these images.

Technological solutions such as these have been a highly effective way of protecting children on the Internet, and AOL continues to explore ways to enhance its protections.

II. Partnering With Law Enforcement

A key part of AOL's efforts to protect children online has been its partnership with federal, state and local law enforcement, including the Internet Crimes Against Children Task Forces, which are part of a federally funded program that includes state and local governments in an effort to combat Internet crimes against children. For more than a decade, AOL's support for law enforcement has been broad, ranging from

providing critical information for investigations and prosecutions, to offering training and educational support for officers in areas such as online and computer forensics and statutory requirements. Let me describe a few significant efforts.

AOL has long been a leader in its efforts to ensure that law enforcement is notified about attempts to use our services to lure children. From its inception, AOL has included a visible and convenient "Notify AOL" button for members to report unacceptable behavior, including images of child pornography that they encounter on our network, to teams of trained professionals in the AOL Member Services department, which work closely with law enforcement. This practice soon became the sought-after standard and in 1999, this practice was codified into Federal law in 42 U.S.C. § 13032, which was subsequently amended to designate NCMEC as the sole recipient for referrals of child pornography. Today, our industry sends nearly 30,000 referrals to NCMEC per year. In addition, AOL voluntarily expanded its program to refer not only incidents of child pornography, but also referrals of child solicitation, which in the 2½ years of the program's existence, has led to 153 arrests. That is 153 or more children who were protected from abuse at the hands of a predator.

For example, in August of this year AOL's Public Safety and Criminal Investigations Unit received an urgent inquiry from law enforcement in Pennsylvania. The police had a lead indicating that a child molester was abusing two children and broadcasting video of the abuse in real-time to other Internet users through a web cam. However, the police did not know his exact location. Based on the information furnished by Pennsylvania law enforcement, AOL was able to provide the police with the location of the molester. The police caught the molester in the act and rescued the two children.

AOL has also been a leader in providing law enforcement with training and support to tackle the challenging aspects of computer and Internet-related crimes. Because police and prosecutors frequently need special assistance in dealing with these cases, AOL has a team of highly trained and dedicated professionals, including former prosecutors, who assist law enforcement on tens of thousands of cases per year. Through support services, such as our 24-hour dedicated law enforcement hotline, our team responds to law enforcement requests, answers officers' questions about what types of information would help their cases, and provides guidance on obtaining the right information.

We not only assist law enforcement with their initial investigations, but we offer support throughout the prosecution of cases. Since 1995, AOL has offered pre-trial litigation support, as well as fact and expert witness testimony on criminal cases involving records obtained from AOL. Each day, AOL receives dozens of inquiries and requests from law enforcement officials who request assistance with the many aspects of their cases, and many prosecutors have reported that their success in convicting perpetrators would not have been possible without the assistance and testimony from AOL records, fact, and/or expert witnesses.

AOL also extended its technology capabilities to allow community involvement and cooperation with law enforcement to protect children. When Congress passed the nationwide AMBER Alert law, AOL reached out to NCMEC and became the first ISP to initiate an AMBER Alert program by which AOL members can receive e-mail alerts targeted to their area. To date, more than 365,000 AOL members have signed up to receive AMBER Alerts. This program is unique and innovative, and again demonstrates AOL's unflagging commitment to utilize the power of its network to provide protection to its users and others.

Also, in response to the recent tragedy at Virginia Tech, AOL has embarked on a project to make alerts available to colleges and universities, based on the Amber Alert program. Through this program, colleges and universities will be able to send out emergency notifications to all of their students, faculty, employees, and other interested persons. The alerts can include potential violent incidents on campus, but can also be used to deal with more routine emergencies such as school closings due to inclement weather. The advantage of the alert system provided by AOL will be the ability to simultaneously reach emails, instant messaging, and cell phones.

As these examples of our efforts underscore, we are committed to our close partnership with law enforcement and recognize that these efforts are critical to harnessing our technology to protect children and others online.

AOL is not just engaged in the Internet community. When the federal authorities saw the enormity of the loss and dislocation caused by Hurricane Katrina, they turned to NCMEC to assist in locating children and reuniting them with the parents from whom they had been separated during the storm and its aftermath. One of the lessons learned from Katrina was that NCMEC's unique skill in locating children is a critical national asset. As a part of AOL's commitment to assist NCMEC in locating victims in the event of a future disaster, AOL has agreed to be one of the remote locations for the National Emergency Child Locator Program. AOL will house and support teams attempting to locate and reunite families in the wake of future emergencies.

III. Education

A critical component of online child protection and AOL's safety mission is education. AOL has been a leader for many years in educating parents, children, and teachers about safety online. We recognize that the most important force in protecting children is actively involved and well-informed parents and teachers. That is why in addition to online tools, we have armed parents and teachers with tips, training, and information to monitor and guide children's online experiences.

Among our efforts, AOL was a leading corporate host of the *America Links Up* national public education campaign, designed to give parents information to help their children have a safe, educational, and rewarding experience online.

In addition, AOL created and distributed a special video for kids—called *Safe Surfin'*—that features online safety tips presented by some of the younger generation's favorite celebrities. This video was developed in partnership with the National School Boards Association, and has been introduced into schools across the country.

Working with the American Library Association, AOL also launched the *Internet Driver's Ed* program. This program is a traveling Internet education and safety class for children and parents, hosted in children's museums and other prominent venues in major cities nationwide.

AOL also was a key partner in forming the GetNetWise.org Web site—a resource designed to provide consumers with comprehensive online safety information that includes guidance from some of the major industry leaders.

AOL was also involved in the Virginia Attorney General's Youth Internet Safety Task Force and chaired two of its committees. One of the recommendations that came out of that task force was the involvement of schools and parents in the education of young people on the proper use of the Internet.

These are just a handful of examples of our many important educational outreach efforts.

IV. Working with the Internet Community and Fortifying Our Efforts

Finally, AOL has worked closely with other Internet companies to improve online safety. For example, last year, AOL joined with other companies, such as Yahoo!, Microsoft and Earthlink to develop effective technologies to investigate and prevent child pornography online. These companies have committed to providing financial and personnel resources to pursue these efforts and have met regularly to develop these plans. We anticipate that such measures will improve methods of removing and preventing distribution of online child pornography, as well as ensure that law enforcement has the data, resources and tools necessary for successful investigations and prosecutions. Also, AOL and other industry members have responded to the problem of child pornography on commercial Web sites. This illegal content is not on sites owned or operated by responsible industry members and, because it is not directly under the control of the companies, they can not remove it. However, AOL and other industry members have agreed to take steps to limit the availability of child pornography on the web accessed through their services.

In addition, AOL has also cooperated closely with Yahoo!, Microsoft and Google to identify policies that can effectively combat online child pornography and ensure Internet safety. Many members of Congress, especially on this committee, have also been tirelessly committed to implementing strong and effective solutions, and our company looks forward to working closely with them improve protections. Some suggestions are as follows:

(1) Enhance industry reporting and data preservation, as well as law enforcement tools. Internet companies have played a significant role in referring and preserving information to help law enforcement investigate and prosecute crimes. This program has been a success to date, but more can be done. For example, Reps. Carney and Chabot's RESCUE Online Services Act takes significant steps toward clarifying and enhancing the Title 42 requirements to ensure more effective reporting and preservation. In addition, Rep. Lampson's Intercept Child Predator Act clarifies state law enforcement authority to obtain wiretaps in case of child exploitation or pornography.

(2) Improve online education in schools and parents. Parents are the first line of defense, and they need information and training to protect their tech savvy children. Also, schools are often integrating computers and online training into their curricula, creating the opportunity for teachers to take an active role in guiding young online users. Proposals that move toward this important goal are Rep. Sanchez's bill to provide Internet safety education grants, and Rep. Bean's SAFER NET, which creates an Office of Internet Safety and Public Awareness to improve online safety education.

(3) Increase funds and training for law enforcement and parole officers. Investigating and prosecuting online crimes is resource intensive, and as you have heard, Internet companies provide nearly 30,000 referrals of specific incidents of child pornography and predation a year, many of which are not investigated and prosecuted today. Also, parole officers need sufficient resources and training to monitor and ensure that once released, convicted predators do not strike again. Important steps forward include Rep. Wasserman Schultz's "PROTECT our Children Act", which would increase support for the ICACs and improve forensic capabilities, and Rep. Scott's legislation to authorize additional grants to fight online crimes against children. Also notable is Section 12 of Ranking Member Smith's SAFETY Act, which would authorize funds for the FBI's Innocent Images National Initiative.

V. Conclusion

AOL is proud of the great strides that we and others in the Internet community have made in addressing these issues, and is committed to continuing efforts to maintain a safe and secure medium for our most vulnerable users: children. We look forward to continuing to work with the law enforcement community, educators, our technology colleagues, this Committee, and other stakeholders to protect the safety of children online.

Mr. SCOTT. Thank you, Mr. Ryan. Ms. Banker.

TESTIMONY OF ELIZABETH BANKER, ASSISTANT GENERAL COUNSEL, YAHOO

Ms. BANKER. Chairman Scott, Ranking Member Forbes, and Members of the Committee, thank you for the opportunity to be here today to talk about how we can all work together on the very important issue of child online safety.

I am pleased to tell you in my 8 years at Yahoo I have seen significant improvement in the user control tools, educational resources, and enforcement systems to protect children. Unfortunately, as you have heard today, despite these efforts, criminals persist.

It is essential that both industry and government fulfill their unique roles in promoting online safety. Yahoo's commitment to fostering a safe environment begins with our own products and services. Our approach focuses on four key areas.

First, building safer online spaces. We offer a safe site for kids, and tools such as safe search, parental controls, and privacy preferences that allow users to decide what information to share and with whom to communicate.

Tools alone are not enough. We also educate users. This year we launched Yahoo Safely, an educational site on the do's and don'ts of online safety. More recently, Yahoo Mash joined with i-SAFE on a safety video for teens.

Second, reporting and appropriate content. Yahoo encourages users to report violations through prominent report abuse links, and works with partners such as the Internet Watch Foundation, who report child abuse URLs. To promptly report child pornography to NCMEC, we invested in systems to forward the information needed for successful law enforcement referrals.

Third, detecting and deterring child pornography. We have a multi-faceted approach, combining technology, user and third-party reports, and human review. We also partner to develop new tools, including supporting a technology coalition to build better solutions.

Partnerships are the fourth aspect of our strategy. Yahoo works with groups like i-SAFE and NCMEC to promote online safety. On Friday, Yahoo and the California Technology Assistance Project will host a summit on Internet ethics and safety. Yahoo's partnership with law enforcement is a key element in our efforts. Our compliance team is available to law enforcement 24-7 for emergencies. We have created a guide for law enforcement outlining our procedures, and we regularly participate in training, including ICAC conferences. Recently we partnered with State attorneys general to conduct training in Nebraska, New York, Texas, New Jersey, and Colorado.

Yahoo is committed to protecting children, yet there is more to be done. Critical functions, such as prosecuting and sentencing offenders can only be performed by government. There are four areas where the public-private partnership can be enhanced by congressional action: safety education, law enforcement tools, government supervision of sex offenders, and resources. These are discussed at length in my written testimony. I would like to highlight a few.

The child pornography reporting statute should be revised to clarify the data NCMEC needs to refer reports to law enforcement. Providers should also be given immunity for transferring illegal images to NCMEC. After these improvements, this should become the single national standard to ensure coordination among Federal, State, and local authorities.

We also encourage the Committee to ensure preservation requests are part of the referral process. Preservation authority is a powerful tool that helps ensure future availability of data. This targeted approach avoids many of the pitfalls associated with broader proposals. Thus, we support provisions in the Rescue Online Services Act just introduced by Representatives Christopher Carney and Steve Chabot. Also, a bill introduced by Representative Nick Lampson would allow States to use critical investigative techniques in child exploitation cases.

To address concerns about sex offenders, we recommend the Committee give additional resources, training, and legal authority to those best equipped to determine how to minimize the risk, the judges who sentence offenders and the parole and probation officers who oversee them. This could be done by expanding guidance for judges on restricting Internet use by offenders and by providing monitoring tools and training to parole and probation officers. We are concerned that approaches that do not leverage law enforcement to set and enforce restrictions could have unintended consequences, including ensnaring innocent Internet users.

There are two final areas that support the legislative changes I have outlined, training and funding. There are several bills notable for making the necessary investments to protect children. Bills introduced by Representative Debbie Wasserman Schultz and Representative Bobby Scott both include funds for law enforcement training. A bill introduced by Ranking Member Lamar Smith has resources for Innocent Images, and a bill introduced by Representatives Chabot and Lampson has funds for ICACs. We are hopeful to see this strategic funding, as well as appropriations for the Adam Walsh Act.

Yahoo is pleased to be among the witnesses at this hearing to take decisive action to fight child exploitation. We look forward to working with the Committee on legislation Yahoo can eagerly support to advance this goal.

Thank you.

[The prepared statement of Ms. Banker follows:]

Testimony of

Elizabeth Banker

Vice President, Associate General Counsel

Yahoo! Inc.

October 17, 2007

Before the House Committee on the Judiciary

Hearing on

"Sex Crimes and the Internet"

Introduction

Good morning, Chairman Conyers, Ranking Member Smith and members of the Committee. Yahoo! is grateful for the opportunity to appear before the Committee to discuss the critically important issue of how parents, educators, law enforcement, and service providers can work together to enhance safety for children online. In my eight years working for Yahoo!, I have seen significant growth in the user empowerment tools, educational resources, and enforcement systems that industry-leading providers have put in place to protect all consumers while they are online. Unfortunately, I have also seen how, despite these efforts, some criminals can persist in seeking to circumvent these measures.

Today, I would like to start by providing you with an overview of the steps Yahoo! has taken on its own network and in partnership with our industry peers, the National Center for Missing and Exploited Children ("NCMEC"), and law enforcement to contribute to a safer online environment. In addition to discussing Yahoo!'s role in contributing to online safety, I would like to highlight areas where we think that the government can be particularly effective in addressing these issues. Finally, I would like to express our support for targeted legislative proposals that, if enacted, would help further combat online predatory behavior while making the most efficient use of the resources of law enforcement, industry members, and the judiciary.

I. About Yahoo!

Yahoo! is a leading global Internet brand and one of the most visited Internet destinations worldwide. Yahoo! has nearly 500 million unique users each month. We

offer a broad range and deep array of innovative products and services that are designed to provide our users with the power to connect, communicate, create, access, and share information online. Yahoo! is primarily an advertising-supported company, which enables us to offer many of our services for free. As an online destination, Yahoo! does not provide users with Internet access. Users may access Yahoo! using any mode of Internet access available to them, whether through our partners Verizon and AT&T, through a dial-up connection, or via a wireless connection in a coffee shop.

II. Yahoo!'s Commitment to Safety

Yahoo!'s commitment to fostering a safe online environment for users of all ages begins with our own products and services. Yahoo! actively works to prevent people from misusing our service to harm children. We have demonstrated our commitment to child safety by focusing our efforts on four key areas:

1) Building safer online spaces by educating users and providing user empowerment tools;
2) Developing tools and policies for reporting;
3) Developing processes for detecting and deterring child pornography; and
4) Partnering with law enforcement, child advocacy groups and our industry peers.

I would like to tell you about our prior successes and our current efforts in each of these four areas to enhance online safety for children.

A. Educating Users and Building Safer Online Spaces

Yahoo!'s commitment to educating our users and building safer online spaces dates back to the early days of the company, when we launched our child-safe service, Yahooligans. Now known as Yahoo! Kids, this service offers our younger users news, music, games, jokes, safety links, and other educational content. For older users, we have focused on developing user empowerment tools that help consumers customize their online experiences. These tools include our SafeSearch filter, which allows users to filter adult content from multimedia and text search results; language filters in message boards, IM, chat, and elsewhere; parental control tools offered in conjunction with our broadband partners to help parents customize and monitor their children's online experiences; and privacy preferences that allow users to decide what information about themselves to publish, what content they would like to share and with whom they want to communicate. These tools allow users to exercise their own judgment about the types of content and activities they want to experience on our network.

Yahoo! also has made it a top priority to educate our users about how to use these tools and how to stay safe online more generally. We provide instructions on tool use in Yahoo! Help, and we promote safety information in key services such as Yahoo! Personals and our new beta service Mash, as well as through our centralized security and safety resource centers. As part of our educational efforts, we recently re-launched our Family Resource Center as Yahoo! Safely. (safely.yahoo.com) Yahoo! Safely is an innovative educational site for parents and kids about the do's and don'ts of online safety. The site features content customized to each of these audiences, bringing together articles by leading experts on online safety such as Parry Aftab, i-SAFE and Internet Keepsafe Coalition side by side with interactive games, polls, and quizzes for kids. We continue to

look for additional ways to educate our users and Internet users generally within our network and our industry and governmental partnerships.

B. Tools and Policies to Encourage Reporting

Another critical part of creating a safer online environment is the ability to respond to inappropriate activity on our network by implementing reporting tools and policies. Yahoo! has strict Terms of Service that prohibit behavior that is harmful to minors. To best enforce our Terms of Service, we rely heavily on the eyes and ears of our users, who supplement our efforts to detect inappropriate content.

Because of the key role that user reporting plays in helping us detect inappropriate content, we have taken steps to encourage user reporting and to provide tools to make such reports more effective. We include "report abuse" links throughout many of our services, including prominent placements in chat and webcam windows, alongside video links in Yahoo! video, and on every profile on Yahoo! 360° and our Mash beta. To make the most of user reports, we have developed a chat transcript tool, which allows customer care representatives to see a snapshot of the chat discussion that was reported.

We also work with partners such as the Internet Watch Foundation who report inappropriate behavior to us. In 2006, Yahoo! Inc. expanded on the longstanding relationship Yahoo! UK had with the Internet Watch Foundation, the "IWF". The IWF compiles a list of child abuse URLs that service providers can use to remove or block child pornography content. We regularly receive updated lists from the IWF and remove the URLs listed from our search indices in the UK, the US, and many other countries. By working with the Financial Coalition on Child Pornography ("Financial Coalition") – a

group convened by NCMEC that connects financial institutions, credit card companies, payment systems, and Internet service providers to bring an end to commercial child pornography – we have gathered important information that helps us identify inappropriate sites on our service.

After reviewing user reports, Yahoo! takes action on its network and for many of these, we take the further step of reporting to NCMEC. Yahoo! has invested significant efforts in developing systems and policies for reporting child pornography to NCMEC largely because of Congress's efforts in passing the Protection of Children from Sexual Predators Act (Pub. L. 105-314, Oct. 30, 1998) in 1998. Although the reporting statute only requires providers to report "facts and circumstances" of instances of child pornography, we have worked closely with NCMEC and law enforcement to include the most helpful pieces of information in our NCMEC reports to facilitate successful referrals, investigations and prosecutions.

We also have designed new features to assist in the identification of users engaged in unlawful activity. For example, we now gather Internet protocol address information associated with photo uploads in Flickr, 360, and Profiles so that source information can be reported to NCMEC. In addition, we worked with our peers in the U.S. Internet Providers Association and NCMEC to develop Sound Practices for Child Pornography Reporting. The Sound Practices, finalized in 2005, have filled an important void in the current reporting statute by educating providers on the key elements that child pornography reports should contain for successful referrals to law enforcement. The success of the Sound Practices comes from their flexible approach, which allows

providers with diverse portfolios of services to each develop reporting practices that make sense in the context of the information available through their businesses.

For instance, we know that a geographic locater is a key information element NCMEC needs to assign a report to the appropriate law enforcement jurisdiction. Yahoo! has both self-reported zip-code information and IP addresses in this category. We worked with NCMEC over time to develop systems to report IP addresses as the more reliable information to include in our reports, but law enforcement can still get the zip code information through legal process if they choose to pursue the report.

C. Deterring and Detecting Child Pornography

Yahoo!'s third area of focus is to improve online safety through the development of tools and procedures for deterring and detecting child pornography. Yahoo! is committed to being proactive on our network and to sending a clear message to child predators that they are not welcome on our services. In order to do this, we have had to develop systems that allow us to quickly find and remove offending content. This requires a multi-faceted approach that employs filters and algorithms, user and third-party reports, and human review.

Last year, Yahoo!, together with AOL, Microsoft, Google, Earthlink and United Online pledged support for a technology coalition ("Technology Coalition") dedicated to developing better mechanisms to allow providers to detect and remove child pornography from their networks. Since then, coalition members have contributed nearly $1 million of funding, executed a partnership agreement and worked with NCMEC to create the top level structure for a hash database. Such a database would allow providers to work with

NCMEC to automate identification and removal of known child pornography images on specific areas of coalition members networks. We are currently in discussions with NCMEC to implement this project.

In addition to developing technology for detecting child pornography, we also gather intelligence on trends and emerging methods through ongoing dialogue. One way we do this is through our work with the Financial Coalition, which has helped Yahoo! better understand emerging trends in this area and formulate improved procedures and tools for eliminating commercial child pornography websites. Yahoo! also gathers important intelligence about trends and patterns in child pornography crimes through regular dialogue and meetings with experts in this area, including NCMEC, Internet Crimes Against Children Task Forces ("ICACs"), and state Attorneys General offices.

D. Partnerships

The fourth aspect of Yahoo!'s strategy for improving online child safety is developing and maintaining partnerships with law enforcement, child advocacy groups, and industry peers.

1. Law Enforcement

Yahoo! supports law enforcement investigations within the framework of our Terms of Service, our Privacy Policy, and the trust of our users worldwide. Yahoo!'s compliance team is available 24 hours a day, 7 days a week to handle emergencies and responds to law enforcement requests. Child exploitation requests are given priority handling.

Yahoo! also provides information and training to law enforcement agencies. Yahoo! has created a Law Enforcement Compliance Manual to ensure that law enforcement personnel are familiar with Yahoo!'s policies, procedures, and systems, and understand how to obtain information when investigating child exploitation cases. We also participate in ongoing training programs for law enforcement personnel who focus on protecting children in order to educate them on the function and operation of Yahoo! systems. We regularly participate in and/or sponsor a number of law enforcement training events, including the National ICAC Conference in 2005, 2006, and 2007; the San Jose ICAC Conference in 2004, 2005 and 2006; the Dallas Children Advocacy Center's Crimes Against Children Conference in 2007; and events for the American Prosecutor Research Institute.

In addition, Yahoo! has worked closely with the offices of a number of state attorneys general on child safety issues. In 2006, we partnered with the Attorneys General of Nebraska and New York to provide in-depth law enforcement training in those states. In 2007, we organized similar training sessions with the offices of the Texas, New Jersey, and Colorado Attorneys General. Yahoo! participated in Virginia Attorney General Bob McDonnell's Youth Internet Safety Task Force, and is currently a member of Washington Attorney General Rob McKenna's Task Force on Youth Internet Safety along with other representatives from industry, law enforcement, public interest groups and educators. Like Virginia, the Washington Task Force is working to make use of the Internet and related technologies safer for children by increasing Internet safety awareness and reviewing current laws related to child pornography and unlawful communications with minors.

2. Child Advocacy Groups

One example of our working relationship with child advocacy groups is the vital partnership Yahoo! has with i-SAFE, a non-profit organization dedicated to educating children about online safety. Our work with i-SAFE includes our sponsorship of the i-SAFE curriculum and training for students in Sunnyvale, where Yahoo! is headquartered, and the planned inclusion of an i-SAFE safety education video in our newest community product, Mash. In addition, Yahoo! has contributed cash and in-kind donations totaling more than $1 million so far this year to sponsor the online child safety initiatives of organizations like NCMEC and other Internet safety organizations, such as iKeepSafe and Wired Safety. Our partnership with NCMEC involves providing advertising placement in sponsored search and network banners for NCMEC Public Service Announcements, hosting NCMEC's NetSmartz online safety content in Yahoo! Safely, and sponsoring NCMEC's annual Hope Awards and Congressional Breakfast. Yahoo! also sponsors ikeepsafe.org's partnership with D.A.R.E. to develop and distribute online safety training materials for D.A.R.E. officers internationally, and hosts iKeepsafe.org and i-SAFE.org content on microsites within Yahoo!. Further, on October 19th, Yahoo!, in partnership with the California Technology Assistance Project & Sunnyvale Police Department, will host "CyberCitizenship – a Summit on Internet Ethics and Safety" for education leaders across Northern California. The event, to be held at Yahoo!'s headquarters, will convene a dialogue among many of the country's leading Internet Safety experts, educators, local law enforcement and representatives from NCMEC and

the DOJ/Project Safe Childhood about safe and effective technology management within schools.

3. Industry Peers

Yahoo! works closely with its peers in the industry to combat child pornography and to protect children online. For example, in 2005, Yahoo! worked with other members of the USISPA and with NCMEC to develop the Sound Practices for Child Pornography Reporting. As I mentioned previously, Yahoo! partnered with AOL, Microsoft, Google, Earthlink and United Online to create the Technology Coalition to work on measures to better enable service providers to detect, report, and remove child pornography from their networks. We also work with the Financial Coalition to gain information that helps us improve our existing tools and procedures for ridding our network of child pornography.

III. Legislative Efforts

Yahoo! has made a concerted effort to protect children online. We are prepared to play our part in the effort to protect children online by creating tools our users can employ to protect themselves and by supporting efforts to educate children, parents, and communities about ways to use the Internet while staying safe. And we will continue to work with others in the industry to develop tools and educational resources aimed at protecting children online. However, while service providers can contribute by providing tools and educational resources, there are critical functions that government can perform more effectively than private industry. For example, monitoring sex offender behavior is a task that is most effectively performed by the government. Similarly, only judges can

evaluate the appropriateness of placing special conditions on offenders after release. One of my goals today is to share our perspective on where legislation could help enhance law enforcement agencies' and the courts' ability to perform essential government functions such as enforcement, sentencing, and monitoring functions to further promote child online safety.

In our view, there are four primary areas where government involvement could fill gaps in the existing public-private partnership to help fight child exploitation online. These areas are: (1) efforts to educate children, parents, and the public; (2) law enforcement tools; (3) governmental supervision of sex offenders; and (4) resources.

A. Education

Education is a critical component of our nation's online safety efforts, just as technology is a core part of our nation's education policy. Children, parents, and teachers need adequate guidance in order to safely and effectively interact online. While child safety is also an issue in offline environments, interactive media is becoming more mainstream, creating a timely opportunity to improve and expand online safety education. Teaching children how to use technology is now recognized as a vital component of their education. Teaching children to use technology *responsibly* helps them to become productive members of an increasingly "online" culture while keeping them safe.

Research shows that education is essential to combating online child predation. A recent study from the University of New Hampshire shows that a smaller percentage of youth are being solicited online than just a few years earlier, and a smaller proportion

seem to be communicating online with people they do not know in person.[1] According to the study, in 2000, approximately 1 in 5 (19%) of Internet users under 18 received unwanted sexual solicitations, and that number declined to 1 in 7 (13%) by 2005.[2] The percentage of persons under 18 who used the Internet to communicate with people they do not know decreased from 40% in 2000 to 34% in 2005. However, as the report notes, it is important to continue and expand efforts to send prevention messages, particularly those messages aimed at teens and preteens, to encourage safer online behavior.[3]

We believe that industry programs such as Yahoo! Safely and GetNetWise should be supplemented by government efforts to: 1) provide reliable information as a trusted source for parents and the public; 2) encourage online safety education in schools; and 3) provide education and training in online investigations and digital forensics for law enforcement.

Proposed legislation that would specifically further these education goals include H.R. 1008, introduced by Representative Melissa Bean, which would establish an Office of Internet Safety and Public Awareness within the Federal Trade Commission. Portions of S. 1965, introduced by Senator Ted Stevens, would also give the Federal Trade Commission a broader education role. The Federal Trade Commission has a long history of education on consumer protection issues, and extensive experience in focusing consumer attention to important issues that could be drawn upon to effectively educate the public about online safety. For example, the FTC could use some of its successful consumer campaigns, like the "Onguard Online" educational effort (designed to educate

---

[1] Online Victimization of Youth: Five Years Later, at 7. See http://www.missingkids.com/en_US/publications/NC167.pdf
[2] *Id.*
[3] *Id.* at 59.

consumers about preventing Internet fraud and identity theft), as a model for creating campaigns to inform parents, children, and the general public about ways to stay safe online.

Finally, Representative Linda Sanchez has introduced H.R. 3577, which would direct the Attorney General to create and administer a grant program for organizations to provide Internet safety education programs to teach parents, children, teachers, and communities about how to recognize and prevent Internet dangers.

B. Procedural Tools

To enhance law enforcement's arsenal of tools to discover, investigate and prosecute child predators, Yahoo! supports changes to several current statutes to improve the ability of law enforcement to obtain successful prosecutions.

1. Changes to the Reporting Statute

First, we recommend the child pornography reporting statute, 42 U.S.C. § 13032, be revised to more explicitly define the obligations of electronic communications service providers to report child pornography and to ensure that providers have clear immunity for making those reports. Congress acted with great foresight in passing the reporting statute as part of the Protection of Children From Sexual Predators Act of 1998. Many major providers, including Yahoo!, have worked to implement systems to fulfill their obligations under the statute. However, the reporting obligations are not well defined. We suggest revising the statute to incorporate the U.S. Internet Service Providers' Association Sound Practices for Child Pornography Reporting. Adopting the Sound Practices will provide clarity and help smaller providers to better understand the types of

information NCMEC needs to successfully refer a report to law enforcement for investigation. The statute should also be amended to include a preemption clause to ensure a consistent national standard for reporting images to NCMEC, without potential state-by-state variations.

Second, the immunity provision in the current statute does not give providers clear immunity for transferring the actual illegal images to NCMEC to help law enforcement. The immunity provision should be revised to ensure that providers may transmit images to NCMEC without fearing potential liability for making their required reports. These two changes are part of the RESCUE Online Services Act, recently introduced by Representatives Christopher Carney and Steve Chabot and we recommend they be the centerpiece of legislation to improve the substantive and procedural laws relating to the investigation and prosecution of child pornography offenses.

2. Improving Investigative Techniques in Federal Statute

In addition to the changes to the reporting statutes, the federal statute relating to the crimes for which state authorities can obtain wiretaps, 18 U.S.C. § 2516(2), should be amended to permit state authorities to use this investigative tool in online sexual exploitation investigations. Declaring these offenses to be eligible for wiretap applications will remove a gap in the current statute and give state authorities an important investigative tool to combat crimes against minors. This change to investigative authority will parallel authority that exists for federal law enforcement. H.R. 3811, introduced by Representative Nick Lampson, would further this goal.

3. Increasing NCMEC's Authority

Yahoo! supports proposals to give NCMEC more authority to make international referrals, issue preservation requests, and share information with service providers and technology companies regarding child pornography. The exploitation of children is a worldwide problem, as evidenced by the number of large, well-organized international child pornography distribution rings that have been discovered.[4] By giving NCMEC the authority to make referrals to international law enforcement agencies, NCMEC can work with law enforcement around the world to combat the exploitation of children wherever it occurs. Cooperation with law enforcement in other countries will not only enable NCMEC to share information about crimes against children outside the United States, but will also encourage those agencies to share key information for investigating and prosecuting crimes involving the exploitation of children with domestic law enforcement agencies.

Giving law enforcement agents detailed to NCMEC the responsibility to quickly issue preservation requests to service providers after a case is referred for investigation to an Internet Crimes Against Children taskforce is another targeted and effective way to ensure that specific information critical to child pornography investigations is preserved early in the investigative process. Because NCMEC is mandated to receive child pornography reports from service providers, agents detailed to NCMEC are in a unique position to quickly identify those situations in which preservation of information is necessary and issue requests to providers. In addition, because of the analysis that NCMEC performs on such reports, any additional providers, beyond the reporting provider, who may hold information could also be sent a preservation request. NCMEC

[4] "Austrian Police Uncover Global Porn Ring,: MSNBC.com, February 7, 2007 at http://www.msnbc.com/id/17022345 (last visited October 14, 2007); Gretchen Ruethling, "27 Charged in International Online Child Pornography Ring," The New York Times, March 16, 2006, page A18.

will then be able to report to the law enforcement agencies who receive referrals that the key information has been preserved, thus eliminating any delays during which evidence could be deleted.

Yahoo! also supports authorizing NCMEC to share information related to child pornography with service providers and technology companies to assist in the development of technologies and tools to thwart the distribution of child pornography and to keep children safe online. Many service providers, such as Yahoo!, have already devoted resources to developing tools and procedures to stop the dissemination of child pornography. Enabling NCMEC to share information would help service providers and technology companies to design and implement tools and procedures to effectively identify and combat the ever-evolving methods used by criminals to exploit children online and disseminate child pornography. This would also further the goals of the industry technology coalitions working to end distribution of child pornography.

We encourage the committee to support a provision of the recently introduced RESCUE Online Services Act to provide more immediate preservation through law enforcement agents assigned to NCMEC, and to consider proposals in the additional areas we've outlined.

C. Enhanced Governance of Offenders

Yahoo! would also like to address the sentencing and post-release monitoring of sex offenders. As I stated previously, there are some capabilities, such as creating tools consumers can use to protect themselves and providing education about safe online behavior, that service providers can effectively provide. However, other critical functions, such as sentencing and monitoring can be most effectively performed by the government.

Additional resources, training and legal authority for sex offender monitoring may help strengthen the capabilities of those who are best equipped to evaluate the overall risk presented to the community by a specific offender, giving them tools to both create and enforce restrictions designed to minimize that risk. Even in the Internet context, the experts are the judges who sentence the offenders and the parole and probation officers who oversee the offenders during their supervised release, not the ISPs who may provide their Internet services.

1. Sentencing

If Congress would like to enhance the government's oversight of sex offenders, we recommend that Congress consider expanding current federal sentencing guidelines to provide more guidance for judges on the imposition of special release conditions for sex offenders to include varying levels of monitoring of and restrictions on Internet use. Sentencing judges and probation officers are best situated to determine whether certain special conditions of supervised release, such as restrictions on Internet use, should be applied, and how severe those restrictions should be. Adding a variety of suggested conditions to the sentencing guidelines will encourage judges to consider imposing restrictions on the sex offender's use of technologies when appropriate, while obtaining valid data to inform future public policy decisions. For example, the Adam Walsh Act calls for the Attorney General to conduct a study to evaluate the effectiveness of monitoring and restricting activities of sex offenders, including the effectiveness of restrictions limiting access to the Internet.[5] Until the Attorney General's study is complete,

[5] Title VI, Subtitle C, §(C)(2), Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat. 587 (2006).

these potential conditions are merely recommended. However, upon completion of the study and depending on its findings, Congress may consider making one or more of these conditions mandatory in subsequent legislation.

2. Monitoring

Monitoring sex offenders so that they are not a danger to society is an important component of keeping children safe online and in the real world, especially given the risk of recidivism. These concerns prompted the passage of the Adam Walsh Act in 2006 and have also inspired subsequent legislative efforts. This is an area where there are no easy answers. While full implementation of the Adam Walsh Act is an important first step towards improving the sex offender oversight system, there are other measures that could make the system even more effective.

Yahoo! recommends that Congress consider focusing legislative efforts on empowering parole and probation officers to monitor any Internet restrictions placed on sex offenders after their release. In order to perform this function, parole and probation officers would need to have the proper tools and training to allow them to either electronically monitor an offender's online activity remotely or to conduct forensic examination of a sex offender's computer for signs of inappropriate activity. The technology to perform this monitoring exists today. However, Congress could help make a difference in this area by giving additional guidance that: (1) Internet restrictions should be imposed on offenders who commit crimes against children online; (2) parole and probation officers are the first line of defense against violation of those restrictions as well as other violations of

conditions of parole; and (3) the necessary training, tools, and resources should be allocated for this work to be performed effectively.

Yahoo! also recommends the Committee consider amending existing law, 42 U.S.C. § 16919, to require that all sex offenders convicted of crimes involving a minor check in with their parole officers every 90 days. Such mandatory reporting may allow parole officers to identify any potential irregularities or warning signs from those sex offenders most likely to put a child at risk.

Yahoo! encourages the committee to examine this targeted approach to monitoring the post-release activities of sex offenders and enforcing any special conditions imposed on sex offenders as part of their sentence. We believe that, out of all the proposals being discussed today, working closely with law enforcement and giving them greater tools will, in the end, be the most effective strategy. Importantly, this proposal will not result in ensnaring innocent bystanders from the broader Internet population who may be falsely identified as sex offenders.

D. Resources

Finally, providing sufficient funding to carry out the initiatives passed by Congress is the key to making any policy work. Yahoo! believes that: 1) funding Project Safe Childhood under the Adam Walsh Act[6] at the authorized level of $47 million is enormously important; 2) DoJ, NCMEC and other Internet Safety programs should receive appropriate funding in addition to authorizations passed by Congress last year; 3) ICAC funding should be increased to $25 million per year to meet the goals of expansion

[6] Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat. 587 (2006).

envisioned under the Adam Walsh Act; and 4) appropriate funding for the adequate management of sex offenders should be allocated.

Obviously, Congress must make choices between and among many worthy programs each year. Based on my experience in working with law enforcement, providing additional resources to the ICACs in particular will yield vast improvements in the ability to bring additional prosecutions of child predators building on their excellent work to date. While the ICAC task forces are able to investigate many of the child pornography incidents reported to NCMEC, the cases represent a heavy load for the federal, state and local law enforcement personnel that make up these squads. Providing additional funding for the ICACs would enable them to investigate and prosecute even more cases.

As Chris Swecker, the Acting Assistant Executive Director of the FBI testified before a House subcommittee in April 2006:

> SWECKER: I'd also, again, just beat the drum for the forensic laboratories, because, again, that is a choke point when it comes to the forensic analysis. We have the laws, but we need the training. We need to export the training to state and local level at a much faster pace.[7]

Additional funding would enable more investigators to attend training, while expanding the training to address a broader range of technical issues critical to law enforcement efforts to prevent and investigate offenses against children. We urge the committee to support H.R. 2797, introduced by Rep. Bobby Scott, which would provide additional law enforcement grants for law enforcement training, research support, public education programs, and the establishment of regional training centers with the aim of improving

[7] Sexual Exploitation of Children Through The Internet: Hearings before the Subcommittee on Oversight and Investigations, of the House Energy and Commerce Committee, 109th Cong.,April 6, 2006.

the identification, investigation, and prosecution of certain crimes, including cybercrimes against children. We also urge your support of the PROTECT Act, recently introduced by Representative Debbie Wasserman-Schultz, which would authorize funding for an ICAC grant program, increased federal agents and increased forensic capacity. In addition, we support provisions of H.R. 837, introduced by Representative Lamar Smith, encouraging funding for the Innocent Images program, and H.R. 876, introduced by Representatives Steve Chabot and Nick Lampson to authorize $25 million for ICACs. Yahoo! also believes funds to train parole and probation officers to monitor offender online activity may be needed.

It is heartening to see the commitment to authorizing these funds. We are hopeful that, as the appropriations process continues, we will see strategic funding for programs in this area.

Conclusion

Yahoo! is pleased to be among the witnesses at this hearing who are taking decisive action to fight child exploitation online. Though we are proud of the contributions we have made towards keeping children safe online, we know there is much more to be done. We recognize our shared responsibility to address this important issue and pledge to continue our commitment to protecting children online. In addition, we look forward to working with the Committee on legislation Yahoo! can eagerly support to advance the fight against child predation. Thank you.

Mr. SCOTT. Thank you very much. I would like to thank all of our witnesses. We will now have rounds of questions, and I will recognize myself first for questions for 5 minutes.

First, just very briefly, Mr. Ryan and Ms. Banker, do you have any difficulty complying with the laws that require you to report images? Is there any logistical problem in doing that?

Mr. RYAN. With respect to AOL, no, Chairman Scott. That has been our practice for over 7 years. Even prior to the legislation, we were doing that on a voluntary basis. So we were very comfortable with that practice. We do call upon this Committee for the opportunity, though, to clarify and grant immunity in the transmission of those images so it minimizes any open issues that may be raised. Clearly, the Department of Justice understands and endorses the practice. But it would give, I think, greater assurance to those ISPs who still may be on the sidelines to get them to pony up and get engaged in the process as well.

Mr. SCOTT. And what do you need immunity for? Is that to protect you against any liability that could occur because of the transmission, violation of privacy or something like that?

Mr. RYAN. That is correct, because we as private citizens do not have any nonlegislative immunity to possess those images during the time which they are conveyed to NCMEC or to law enforcement.

Ms. BANKER. I would just like to add that the current reporting statute does not specify that the image should be part of the report, and we think that both clarity as to what should go into a report to NCMEC, saying that it should include the image, as well as then making sure that the appropriate immunities are in place for the transfer of the image would greatly improve the quality of the reports that NCMEC receives.

Mr. SCOTT. Okay. You don't need—I thought you were looking for immunity for violation of people's privacy, if you take somebody's property if it wasn't in fact illegal activity and you would expose their privacy or something like that. That is not—you would want immunity from that, but you are talking about immunity because you, during that period of time, actually have possession of the material. Okay.

Mr. Waters indicated that we don't have the resources. Mr. Weeks has indicated that the number of prosecutions compared to the number of cases we know about is somewhat modest. Now Mr. Mason, you indicated hundreds of thousands of leads and only 42 open cases. Did I hear you right?

Mr. MASON. No, sir.

Mr. SCOTT. Okay. How many cases—how many possible investigations? I thought you said hundreds of thousands of possible investigations.

Mr. MASON. No, sir, I didn't say that. We have approximately 2,600 current cases open.

Mr. SCOTT. Okay. How much more money would you need to pursue the cases that Mr. Weeks and Mr. Waters have indicated are cases where you have live leads, and but for resources, because of lack of resources you can't pursue them?

Mr. MASON. That would be an answer I would have to come back to the Committee with. It would be hard to answer now. It is tanta-

mount, in some respects, to trying to catch everybody going 58 miles an hour in a 55-mile an hour speed zone. The number of people out there engaged in this activity is absolutely staggering. So at this moment in time I wouldn't be able to give you a figure that would allow us to cover all of the people out there engaged in this kind of activity.

Mr. SCOTT. I suspect that you might have—I mean the difference between going 58, if the going 58 caused the kinds of damage that is being caused here, I think you might get the resources to catch everybody going 58.

Mr. MASON. I agree, and I certainly didn't mean to compare the consequences of those two acts.

Mr. SCOTT. So if you could give us some resource numbers.

Mr. Waters, what kind of numbers should we be hearing in terms of resources?

Mr. WATERS. Mr. Chairman, from the perspective where Wyoming is concerned right now, we are bringing in roughly 35 to 40 new offenders that we identify in our State each month. And I can handle with my seven agents, counting myself, we can handle right at seven to 10 cases a month. If we tripled our funding we may be able to get a start on trying to keep up with just what is coming in, not the growth. We are seeing it escalate each month. So at the current state, I think tripling our efforts would be——

Mr. SCOTT. I would ask you and Mr. Weeks, do you need any new laws or just need resources?

Mr. WATERS. From our perspective, Project Safe Childhood and the push with the U.S. Attorney's office to prosecute these cases has given us amazing coverage in getting the offenders that we do catch brought before the judge and put in jail. So right now our laws are working fairly well. Other folks have spoken about other issues that we are not yet facing in Wyoming.

Mr. SCOTT. Mr. Weeks?

Mr. WEEKS. Mr. Chairman, there are laws that would be very helpful. I know that they do need some help with some of these data retention issues. But honestly, I don't think the answer is more laws at this point. I think the answer is more resources. Because as long as they can't even begin to pursue what they—the predators that they see now on their screens, it is almost a moot point.

Mr. SCOTT. Thank you. I recognize my colleague from Virginia, the Ranking Member, Mr. Forbes.

Mr. FORBES. Thank you, Mr. Chairman, and thank all of you for taking time to be with us today.

Ms. Banker, we heard the testimony from Alicia a little bit earlier, and she had to leave before we could ask her any questions. And just before I ask you one, Mr. Chairman, I would like to ask unanimous consent to put in an article from the *New Jersey Star-Ledger* dated Sunday, August 14th, 2005, outlining Alicia's testimony and her situation.

Mr. SCOTT. Without objection, so ordered.

[The information referred to follows:]

New Jersey Star Ledger

AT FREEDOM'S EDGE: LIBERTY , SECURITY AND THE PATRIOT ACT

To catch a monster, using anti-terror law

Part four of an occasional series

Sunday, August 14, 2005

BY MARK MUELLER

Star-Ledger Staff

PITTSBURGH — Ten minutes.

The time between dinner and dessert in the home of Charles and Mary Ann Kozakiewicz. The time it took the couple's 13-year-old daughter, Alicia, to vanish on New Year's Day in 2002.

Mary Ann Kozakiewicz had been clearing dishes from the table when she saw her daughter leave the dining room. Alicia told her she was going to her room. By the time an apple-walnut pie had been laid out, she was gone.

Her family found no note, no sign of a break-in. On one of the coldest nights of the winter, Alicia's jacket remained in the closet. A pile of cash — $200 in Christmas gifts — lay on her dresser.

The parents called Alicia's friends, searched the neighborhood and alerted Pittsburgh police. An officer asked if Alicia had ever run away. Did she use drugs? Was she having trouble at school? No, no and no, the parents said.

The officer recorded their responses, then told the couple Alicia would probably show up in a few hours.

"But we knew she wouldn't," Charles Kozakiewicz said. "We knew she was gone."

* * *

The search for Alicia Kozakiewicz would involve Pittsburgh police, the Allegheny County Sheriff's Office and dozens of federal agents. It would also mark the first use of the USA Patriot Act in the Western District of Pennsylvania.

Signed into law six weeks after the Sept. 11 attacks, the Patriot Act was portrayed by the Bush administration as an integral tool to help law enforcement and intelligence services recognize, track and arrest terrorists.

Since then, U.S. officials say, the government's expanded powers under the Patriot Act have been used to identify foreign "sleeper cells" in the United States, disrupt terrorist financing networks and arrest home-grown militants, among them a Ku Klux Klansman convicted of stockpiling explosives.

But the law also has been regularly applied to traditional crimes with no connection to terrorism.

While the Justice Department says it does not uniformly track the Patriot Act's use in such cases, a reading of government reports and congressional testimony shows it has been used hundreds of times against the likes of drug dealers, computer hackers, child pornographers, armed robbers and kidnappers.

In Washington state, investigators invoked the law to surreptitiously bug a tunnel that had been bored beneath the U.S.-Canadian border by drug runners. In Las Vegas, prosecutors used it to seize the financial records of a strip-club owner suspected of bribing local government officials.

One controversial Patriot Act provision, referred to by critics as the "sneak-and-peek" statute because it allows authorities to conduct searches without notifying the targets for a period of time, has been used overwhelmingly in non-terrorist cases, according to a Justice Department letter sent last month to Rep. Robert C. Scott (D-Va.).

The letter, issued in response to questions by Scott and other members of the House Judiciary Committee, said that of the 153 times the provision had been used through Jan. 31 of this year, just 18 cases, or 12 percent, were related to terrorism. The majority involved drug investigations.

That broad application angers civil libertarians and some members of Congress, who contend the Patriot Act's expanded powers were never meant to be used against common criminals.

Critics note that long before 9/11, the Justice Department sought some of the powers contained in the Patriot Act — among them, broader wiretapping authority and greater access to the customer records of Internet Service Providers — and that Congress, fearing an erosion of constitutional rights, denied the requests.

"When I voted for the Patriot Act, I was voting to give law enforcement the tools they said they needed to keep this nation safe from terrorists," said Rep. Shelley Berkley (D-Nev.). "I never for a minute thought it would be used in garden-variety crimes or to bring a strip-club owner to justice. Quite frankly, I think it makes a mockery of the Patriot Act to use it for these kinds of crimes."

Mary Beth Buchanan calls such criticism misguided and wrong.

The U.S. attorney for the Western District of Pennsylvania and one of the Patriot Act's more tireless defenders, Buchanan argues the legislation was necessary to upgrade laws that had grown obsolete in the age of the Internet and to eliminate legal peculiarities that deprived terrorism investigators of tools long available to counterparts fighting traditional crime.

She contends the measure was never intended solely for terrorism, that it is applied with restraint and that not a single case of abuse has surfaced in nearly four years.

"The Patriot Act represents a reasonable balance between protecting Americans from terrorism and protecting liberties," she said.
Buchanan has another reason to support the law. As a veteran sex-crimes prosecutor, she has seen firsthand the kinds of miseries people routinely inflict on children.
In the early days of January 2002, Buchanan didn't know what had become of Alicia Kozakiewicz, but she was determined to use every legal tool at her disposal to find out.
* * *
Mary Ann Kozakiewicz (pronounced Koz-uh-KEV-itch) couldn't sleep, couldn't eat, couldn't stop herself from picturing her daughter out there, somewhere, in the cold and the dark. Probably afraid. Probably in danger.
Alicia still slept with a night light. When the sun went down, she flipped every switch in the house, lighting it up like a Christmas tree. Mary Ann Kozakiewicz couldn't imagine her daughter venturing into the night willingly without turning on the outdoor floods.
Now, hours after police had come and gone, the mother sat on a couch in the living room, her eyes locked on the front door, willing it to open.
"Every noise I heard, every car door, I just shot toward the door," she would recall later.
Charles Kozakiewicz wanted to run around the streets, shouting Alicia's name. But he had done that already. Flashlight in hand, he had walked his property repeatedly, searching the snow for footprints.
He checked the house so many times he lost count, hunting for Alicia even in cabinets and under couches — places she couldn't possibly fit — because he needed to know for sure she wasn't there.
"You get into a fog," he said. "You don't know what to do. You don't know what time it is. Time changes for you. There is no time. There's just, 'She's gone.'"
The parents went over the day's events in their heads, searching for clues. It had been a typical holiday gathering. The couple's adult son, now living on his own, had visited. So had Mary Ann Kozakiewicz's parents.
They had watched Cirque du Soleil on TV and talked, the women preparing a traditional New Year's Day meal of pork and sauerkraut, meant to ensure good luck in the year ahead. As Mary Ann Kozakiewicz put out the good china, Alicia asked if they could use paper plates instead. She didn't want to wash all those dishes.
A willowy 5-foot-5, with shoulder-length, chestnut hair and blue-green eyes, Alicia looked older than her 13 years. As long as Mary Ann Kozakiewicz could remember, people told her daughter she should be a model, and Alicia had begun to take an interest in it.
At age 12, she had enrolled in a three-month class at a Barbizon Modeling and Acting Center in the suburbs. The course had helped her overcome some of her shyness.
But modeling didn't define her. She spoke of one day becoming a psychologist. She wrote poetry. She spent hours chatting with friends online. Most of the time, the eighth-grader made the honor roll.
Her home had always been in Crafton Heights, a middle-class neighborhood in the Pittsburgh hills, just west of downtown. Charles Kozakiewicz, a car salesman, believed his children were safe there.
* * *
The arrival of Tom Clinton and Denise Holtz at the home of a missing child can be viewed as a hopeful sign or a bad omen. Hopeful because the two are widely considered dedicated investigators with an impressive record of success.
It's what they investigate that gives rise to a parent's greatest fear.
Clinton, a U.S. postal inspector, and Holtz, an FBI agent, primarily chase child pornographers, child rapists, kidnappers and "travelers," men who troll the Internet for kids, befriend them and travel across state lines to molest them.
It is not work for the faint of heart.
Clinton, a 56-year-old Pittsburgh native with three grown sons, draws out confessions with empathy he doesn't feel and with a gentle manner that took years to master. He has viewed thousands of photos and videos he would just as soon forget.
But the assignment is his by choice. He volunteered for the job in 1987, when child porn was still largely transmitted by mail or smuggled in suitcases.
"I know it sounds like Chevrolet and apple pie, but these are people who need to be prosecuted," Clinton said. "The victims in these cases are really victims."
Holtz, a 39-year-old Kentuckian, sought such cases for the same reason after joining the FBI eight years ago. She has been partners with Clinton ever since.
Both are founding members of the Western Pennsylvania Crimes Against Children Task Force, formed with Mary Beth Buchanan to promote cooperation among law enforcement agencies and to provide social and psychological services to abused kids.
Alicia Kozakiewicz came into their lives the morning of Jan. 2, 2002, when a supervisor popped his head into their windowless fourth-floor office at FBI headquarters on Pittsburgh's South Side. He told them to look into a report of a missing girl.

Holtz and Clinton called Pittsburgh police for a briefing, asking specifically if Alicia spent a lot of time on the Internet. So many of their cases involved the Internet.
She had, the officer told them.
When the pair arrived at the Kozakiewicz home, an FBI computer forensic examiner, Tony Pallone, was with them. They questioned Alicia's parents, asking them to revisit every moment of the previous days. They also confirmed Alicia's heavy Internet use.
It was too early in the probe to draw conclusions, but Holtz and Clinton were developing a hunch.
They talked to neighbors and poked through Alicia's belongings. Next to the teen's second-floor bedroom, in a combination family room and office, they turned on the computer.
"She had the scanner, the Webcam, all the things that are a recipe for disaster," Holtz said. "We knew a clue could be on that computer."
Pallone, the forensic examiner, began copying files and logs, preserving them for a detailed examination at headquarters later.
Downstairs, Charles and Mary Ann Kozakiewicz gave photos of Alicia to the Pittsburgh media, appealing for help.
Neighbors stopped by, offering comfort and bringing food that would go uneaten. Friends and Allegheny County sheriff's officers searched the nearby woods and gullies. Mary Ann Kozakiewicz, a stay-at-home mother, felt like a character in a bad TV movie, and she didn't know how it would end.
"In the back of your mind, you know how quickly children are killed," she said. "You know the statistics. It's a one-in-a-million shot to see your child again. But you have to remain strong. You pray for a happy outcome. You pray for a miracle."
* * *
Holtz and Clinton knew that children will share with friends information they never would tell a parent. On Jan. 3, 2002, a Thursday, the investigators went looking for Alicia's secrets at Carlynton Middle School, now back in session after the holiday break.
It immediately paid off.
One friend said Alicia confided she had recently met someone, a man, in an online chat room. The girl didn't know a name, but she said Alicia had been communicating with him through instant messaging deep into the night.
"She had been coming into school tired," Holtz said. "One of her friends said she had been on the computer until 3 or 4 in the morning.
"That's when alarm bells started going off."
Charles and Mary Ann Kozakiewicz were stunned.
"It was the first I heard of it," the mother said. "It made it even more serious. If this indeed was the scenario, if someone had taken my daughter, you know you have an evil person involved. It's a confirmation of your worst fears."
The investigation had gained focus, but Holtz and Clinton didn't have a name.
At FBI headquarters, Pallone searched the hidden recesses of Alicia's computer, but it wasn't giving up any secrets. It was almost as if Alicia had covered her tracks. The investigators needed a break.
They got one later that night. ▯
* * *
Holtz's cell phone rang at 8 p.m. She had just left a retirement party at a downtown restaurant for a popular agent. Now she was headed home through the Fort Pitt Tunnel, one of many passages that slice through the city's mountains.
Her reception cutting in and out, Holtz had trouble understanding what her office was telling her. Something about a caller in Tampa., Fla., who had information about a missing girl in Pittsburgh. He hadn't left a name, but he'd agreed to call back.
Holtz wheeled around to collect Clinton at the restaurant.
At FBI headquarters, they learned more from a supervisor. The call had been made to the Tampa office from a pay phone, and the man on the line was afraid.
He'd been instant messaging with an online friend, someone named Scott from Virginia, with whom the caller had become acquainted through bondage and discipline clubs on Yahoo.com. Scott had been talking for some time about finding a teenage girl to make his slave.
Early on New Year's Day, Scott had told him, "I think I got one," mentioning a planned trip to Pittsburgh.
Later, at about midnight on New Year's Day, as Mary Ann Kozakiewicz was staring at her front door, Scott wrote again.
"I got one," the message said. To prove it, Scott posted a Webcam image of a young girl.
The caller still had doubts. Had Scott somehow staged it?
"A lot of the Internet world is fantasy, and the informant in Florida didn't necessarily believe it was true," Holtz said.
Before calling the FBI, the tipster had checked the Pittsburgh Post-Gazette Web site. There he found a story about Alicia Kozakiewicz. A photo ran alongside it.

The caller couldn't remember with certainty Scott's Yahoo screen name. He believed it contained the words "master," "slave" and "girl," but he didn't know in what order. Before hanging up, the tipster said he would get back to them with more information when he could.

At FBI headquarters, Clinton, Holtz and other agents began running the words through a Yahoo tool that allows people to search for screen names. If investigators could learn Scott's, they might then find clues in a personal profile.

They remained there through the night.

* * *

At 7 a.m. on Friday, Jan. 4, 2002, the tipster called back. Immediately routed to Pittsburgh from the Tampa office, he explained to Special Agent Tom Carter, a supervisor, that he was still nervous. He wanted to come forward, but he was afraid he would be viewed as an accomplice.

Carter worked to soothe him. A former Marine, Carter learned the caller had served in the military, and he used that information to forge a bond.

Bit by bit, over the course of an hour, the man surrendered clues.

Scott lived somewhere in northern Virginia and had talked for at least a year about taking a girl. On Yahoo, he went by the screen name "masterforteenslavegirls."

With the exact screen name in hand, investigators found Scott's Yahoo profile. It contained no last name, but it did have photos. One revealed a rotund, mustachioed man, a slight smile on his face as he looked into the camera. Another showed the same man posing before a wall of implements associated with sexual torture.

The caller told Carter the items were in Scott's basement, his "dungeon."

There was more, the Florida man said. Scott had sent another image. This time, the girl's arms were bound, suspended above her head from the ceiling. She had been beaten. And she was crying.

Clinton and Holtz remained calm, but they were deeply worried.

"The caller gave us enough information to know we had a real problem," Clinton said. "This kid was in trouble. We had to find her."

Holtz began dialing the phone. She needed to find someone at Yahoo who could provide the Internet Protocol address of the computer Scott had been using.

Like a fingerprint, an IP address is a marker that can identify, with a simple Web search, someone's Internet Service Provider. From there, Holtz and Clinton could put a name to the smiling, round-faced man in the photos.

In another office nearby, an FBI supervisor signed a form letter prepared for moments just like this. For the first time in western Pennsylvania and little more than two months after the law had been passed, the investigators would use the Patriot Act.

* * *

Justice Department officials hold up Section 212 of the USA Patriot Act as one of the law's great success stories, saying it has helped save lives.

Unlike most of the act's provisions, Section 212 expands the government's power only indirectly, shielding ISPs and related companies from civil liability if they voluntarily share customer information with law enforcement in emergencies.

Before the law went into effect, Internet Service Providers generally refused such requests for help unless a search warrant or grand jury subpoena compelled their cooperation. That's because disclosing a customer's name or the contents of e-mail — even if a life was at stake — theoretically exposed ISPs to lawsuits.

Similarly, if an administrator at Yahoo or Google, both of which provide popular Web-based forums, stumbled across a murder plot in an e-mail or a chat room, he or she might be loath to pass it along to police.

Section 212, one of 16 Patriot Act provisions that will expire at the end of the year if Congress does not renew them, was designed to address that problem.

It allows ISPs and companies that provide services on the Web to disclose information without fear of legal action if they have a "reasonable belief" someone is at risk of "immediate death or physical injury." Such disclosures may be made to any federal, state or local law enforcement agency.

Congress granted even greater protection to ISPs with the Homeland Security Act of 2002, which amended Section 212. The revised measure changed the legal standard for disclosure from a "reasonable belief" of danger to a "good-faith belief."

"A lot of people think that's a big difference," said Beryl Howell, former general counsel for the Senate Judiciary Committee's Democrats and one of the party's chief negotiators on the Patriot Act. "A reasonable belief requires a little more due diligence."

The Homeland Security Act changed Section 212 in another important way, broadening it so that emergency disclosures may be made to "any government entity." That could mean the Centers for Disease Control and Prevention, the Environmental Protection Agency, even a local mayor's office.

The Justice Department has not publicly said how many times it has used Section 212. A report on the provision remains classified, a spokeswoman said.

In unclassified reports and in appearances before Congress, government officials have said only that it is used "often," and they cite examples of the provision's successes. Most of the examples have nothing to do with terrorism.

Among them is the nationally publicized murder of Bobbie Jo Stinnett, a Missouri woman whose unborn child was cut from her womb and stolen in December of 2004. Examining Stinnett's computer, federal investigators discovered a suspicious e-mail and, using Section 212, traced it to a Kansas woman who authorities say tried to pass the baby off as her own.

It's hard to argue with such results, and most critics of the Patriot Act don't try, but they still call the emergency disclosure provision a deeply flawed measure that puts unchecked power in the hands of law enforcement and guts the Constitution's Fourth Amendment, which guards against unreasonable searches and seizures.

When an ISP turns over e-mail or customer names under the provision, it does so without the benefit of a grand jury subpoena or a search warrant, both of which require some evidence that a crime has been or will be committed.

Customers whose information has been disclosed are notified only if it becomes evidence in court. And the government need not report to Congress or the public how often it asks for disclosures.

"There are no checks and balances," said James Dempsey, executive director of the Center for Democracy and Technology in Washington, D.C. "I call it off-the-books surveillance because no one will know about it. Not a judge. Not a grand jury. Not the person whose privacy has been violated. It's as if it never happened."

In the absence of oversight, he argues, too many questions go unanswered. What's to stop an FBI agent, a city detective or a small-town cop from calling something an emergency when it's really a fishing expedition?

Critics also would like to know more about when the provision is applied. If authorities are going directly to ISPs for help during business hours, when judges are readily available and grand juries are in session, that could suggest an attempt to avoid standards of evidence.

Despite concerns about the measure, Section 212 has not generated the kind of raucous debate swirling about higher-profile Patriot Act provisions, and it appears it will stand permanently.

Last month, within three weeks of the terrorist bombings in London, both the House and Senate passed separate bills reauthorizing most of the act's provisions, including Section 212. Congress must reconcile minor differences between the two after returning from its August recess. The Bush administration has asked Congress for a bill the president can sign on Sept. 11.

* * *

Denise Holtz stabbed at the numbers on her phone with mounting frustration.

It was 8 a.m. in Pittsburgh — 5 a.m. at the Sunnyvale, Calif., headquarters of Yahoo — and she couldn't get a human being on the phone. The investigators had finally caught a break in learning Scott's screen name, and now Holtz was wasting time bouncing around in voice mail.

With Holtz at a dead end, the Pittsburgh bureau's special agent in charge, Jack Shea, woke up his counterpart in Sacramento, laid out the case and asked if he had a contact at the Internet firm.

He did.

"Make it happen," Shea said. "We need this."

A Yahoo vice president called back at about 9:30 a.m., Pittsburgh time, and told Holtz he had dispatched an employee to the office. There the employee was met by a faxed letter, signed by the FBI supervisor in Pittsburgh, advising him of Patriot Act Section 212.

By 11 a.m., Yahoo faxed back a 10-digit number, the IP address of Scott's computer. An agent immediately ran a Web query to find his Internet Service Provider.

It was Verizon.

As Holtz called the company, an assistant U.S. attorney obtained a subpoena from a sitting grand jury in Pittsburgh. Because it was now during business hours, the Patriot Act was no longer a necessity, Buchanan said.

At 11:30 a.m., a Verizon representative in Texas gave Holtz the words she had been waiting three days to hear.

Scott William Tyree.

* * *

Criminal profilers say men who lure children bring a specific psychology to the hunt for victims.

They flatter. They search for weak spots — family problems, troubles with classmates — and exploit them. They become confidants, presenting themselves as an alternative to the drudgery and constraints of school and home.

Investigators call it "grooming," and for more than four weeks as 2001 came to a close, Scott Tyree used it to full effect on Alicia Kozakiewicz.

The two had come across each other in a chat room in late November or early December. Before long, they were communicating frequently, often for long stretches.

Twice married and divorced, Tyree was a 38-year-old California native who had spent much of his life working with computers. As a young man, he took them apart and put them back together. As an adult, he

programmed them. As a pedophile, he used them to spread the gospel of sadism and to seek out young girls, authorities say.
He moved east in the mid-1990s, paying $1,000 a month in rent for a townhouse in Herndon, Va., a pleasant suburb of Washington. He worked as a programmer at the Herndon office of Computer Associates International, a firm based in New York.
He had a 12-year-old daughter, who lived with Tyree's first wife in California.
Alicia saw him as a friend.
"She confided in him," said Buchanan, the U.S. attorney.
If Alicia had a bad day, she told him about it. After she argued with her brother during one of his visits, Tyree stoked her indignation.
"He would say, 'I understand. It's terrible that he treats you that way,'" Clinton said.
At the same time, Tyree maintained caution, teaching Alicia to "wipe" her computer, eradicating traces of their online talks.
On New Year's Day, as Tyree's daughter was finishing a visit, he arranged to pick up Alicia a block from her home. At noon, he dropped off his daughter at the airport. Between 2 and 3 p.m., he left for Pittsburgh in his black Mitsubishi Eclipse, collecting toll receipts along the way.
Between 7 and 8 p.m., as her mother rinsed the dishes, Alicia quietly slipped out her front door.
* * *
As the sun rose on Friday, Jan. 4, 2002, Charles Kozakiewicz felt his strength slipping away. He hadn't slept since New Year's Eve.
"When you get tired, the hope starts to go away," he said. "Things were not looking good."
He was terrified the phone would ring, that someone on the other end would give him bad news. And yet he wanted it to ring with word of something different.
In the early afternoon, the phone did ring. It was the FBI, summoning the couple to headquarters. There was a possible development.
They didn't ask for details, afraid of the answer.
The 20-minute ride passed in silence. Mary Ann Kozakiewicz believed Holtz and Clinton would tell her Alicia was dead, that her body had been found in some shallow grave. For her husband's sake, she didn't speak the words aloud.
"It would have hurt him more," she said, "and I couldn't go there."
At FBI headquarters, a bland white rectangle on the edge of the Monongahela River, the parents were led to a conference room.
They waited.
* * *
Denise Holtz didn't know if Alicia was alive or dead.
Some 240 miles to the south, in Herndon, Va., a team of police officers and FBI agents from the Washington field office was due to hit Tyree's townhouse.
Holtz had asked her D.C. colleagues to call immediately afterward. Now, more than 30 minutes past the scheduled entry, the wait was excruciating, and Clinton, on an assignment in court, wasn't there to calm her.
Doubts kept flitting through her mind. Did they have the right address? Were they in time?
FBI agents crowded into the office and spilled out the door. Each time the phone rang, they jumped.
The Pittsburgh bureau's assistant special agent in charge pushed his way in at 3:30 p.m.
"They found her," he said. "She's alive."
The room erupted in cheers.
In Virginia, the agents had smashed through Tyree's front door, guns drawn. They found Alicia cowering in a corner of an upstairs bedroom. A chain extended from a collar around her neck to an eyebolt in the floor.
Tyree had left the house that morning, telling Alicia he would hurt her if she tried to escape. When the FBI agents burst through the door, she thought it might be him, coming back to kill her.
* * *
She's alive.
Charles and Mary Ann Kozakiewicz savored the words.
"It was such a dumbfounding statement," the mother said. "It's as if she had come back from the dead."
Charles Kozakiewicz felt the terror drain from his body.
"The missing, as bad as that was, this was the total opposite," he said. "It was the happiest feeling in the world."
Holtz raised Clinton on the phone, delivering the news.
"Yeah," he said. "Now let's get this son of a bitch."
At 4 p.m., a second team of FBI agents arrested Tyree at work. In an hours-long interview with agents from the Washington field office, he confessed.
Alicia was taken to a local hospital for an examination. She was not seriously injured. At Manassas Regional Airport, she was reunited with her parents in a private room.

"We just hugged each other, and that's a hug you never repeat," Charles Kozakiewicz said. "If that feeling of joy were out there all over the place, there would be no wars. That hug made life worth living."

* * *

It is impossible to know with certainty whether the Patriot Act saved Alicia's life.

Her mother thinks so.

"There's at least one American citizen who's going to grow up and go to the prom and have a life because of the Patriot Act," she said.

Some critics of the law are respectfully skeptical, saying that what the Patriot Act achieved might have been carried out in the same time frame — or close to it — using standard legal procedures.

"Warrants are issued every day in this country very quickly," said Lisa Graves, senior counsel for legislative strategy at the American Civil Liberties Union. "Every court has an emergency judge you can call in the middle of the night. These can be approved over the phone. When time is of the essence, this is not an elaborate process."

Buchanan said she can't speculate on what Tyree might have done given more time. She's glad she didn't find out.

"In cases like this, hours matter. Minutes matter," she said.

Tyree, now 41, pleaded guilty to two federal counts — sexual exploitation of a minor and travel with intent to engage in sexual activity with a minor — in March 2003. A judge sentenced him to 19 years and seven months in prison.

Authorities say there is no indication he abused his daughter.

Alicia is now 17. Last year she began speaking to student groups about her experience to warn them about the dangers of the Internet, and she has become a member of Teenangels, a national online safety group based in New Jersey.

On May 25, she addressed a gathering of youth groups in a U.S. Senate caucus room and presented an award to the law enforcement team that rescued her. During the event, she met Attorney General Alberto Gonzales, giving him a teddy bear to pass along to President Bush.

She named it "Patriot."

Mr. FORBES. Also I would just like to mention for the record that the Ranking Member Smith has been on the Floor dealing with FISA today, and that is why he hasn't been here because he would have loved to have heard all of his testimony

Mr. SCOTT. I think that is where the Chairman is, too.

Mr. FORBES. Ms. Banker, first of all, you deserve some questions. You all deserve some questions because, in Alicia's situation, it was your company that actually happened to locate the individual that had kidnapped her and taken her in; is that correct?

Ms. BANKER. That is correct.

Mr. FORBES. Were you General Counsel at that time?

Ms. BANKER. I did oversee our law enforcement combined function at that time.

Mr. FORBES. One of the things that we heard in there when we talked about immunity was when, prior to the PATRIOT Act, which gave you immunity in that particular situation, that many of the providers were reluctant to give that kind of information for fear of lawsuits that would come down on them even if a life was at stake.

Is that accurate?

Ms. BANKER. I think that most providers in the face of a situation where a child is in danger would make the decision to provide the information. But it greatly eased our ability to do so when that was included as a specific legal exception.

Mr. FORBES. Did you ever have to make that determination as General Counsel prior to that time?

Ms. BANKER. I did.

Mr. FORBES. Did you authorize it to be released always, or was it a concern to you that they might have lawsuits that come up?

Ms. BANKER. I don't think our primary concern was lawsuits. I think the company has always tried to do the right thing in terms of protecting our users' privacy interests.

Mr. FORBES. So you are suggesting that the fact that you may be sued later on was not a part of the—one of the components that you would take into advising what actions that the company would take?

Ms. BANKER. It certainly is something that goes into the formula. But having been the person on the other end of the phone, when law enforcement calls and says that a child is missing, I can tell you that you feel a very strong responsibility to act in the best interest of public safety. And while we certainly always adhere to our terms of service and our privacy policy and Federal laws on these issues, we do our best to balance those.

Mr. FORBES. I just can't imagine that general counsel wouldn't at least take that into account, and certainly in the article that I just had admitted to the record, it seems like a lot of other providers said that that was a major concern to them and that they were glad that they had that act.

That allowed them to be able to do that.

Mr. Rothenberg, let me go to you and ask you, what challenges do prosecutors face in receiving adequate sentences against child pornographers? We heard about the need for money. We know that. You know, every single group that comes before us needs more

money. It is not that you don't. We don't disagree with you about that. But we always know that we need more money.

What challenges do you face other than financial in receiving adequate sentences against child pornographers?

Mr. ROTHENBERG. We do in fact have a problem with that, as I pointed out, and I go into it in a little more detail in my written statement.

We have faced slightly higher than 26 percent non-government sponsored downward departure rate by judges in child pornography possession cases. That is twice the rate for other crimes in the last few years since the sentencing guidelines became advisory under the Supreme Court opinion in *U.S. v. Booker*.

Mr. FORBES. That was 29 percent.

Mr. ROTHENBERG. 26 percent. So a little more than one-fourth of these cases we believe reflect the erroneous view that the possession of child pornography isn't such a bad crime, and as I said, possession drives demand. And it is a victimization of the child and needs to be punished sufficiently.

Mr. FORBES. You are saying, even when you have the resources and get it to a conviction, that you are having some problems with some judges giving sentences.

Mr. Mason, what additional tools do you need to stop the flow of money to offenders that are involved in child pornography and the exploitation industry? And I know that you had difficulties because of the use of virtual money on that.

Can you tell us if there are any additional tools that you need in that?

Mr. MASON. They use a lot of different methodologies to move around, and I am not sure right now, I am not prepared to give an answer regarding that specific problem as to what we would need to further curb this problem.

The devices they use, citizens use to buy goods and other things off of the Internet, and I certainly wouldn't want to preclude that activity.

So I would—I am not prepared at this moment to speak to what we would need specifically in terms of legislation to tamp down that particular problem.

Ms. SÁNCHEZ. [presiding.] Do you yield back?

Mr. FORBES. One of the reasons that we hate this format is we have seven witnesses in here. We can't ever adequately ask a question. We would like to pick your brain on more of these issues. Hopefully, we will get to a time where we can talk and get your testimony in a more advantageous situation.

Ms. SÁNCHEZ. The point of the gentleman is well taken, and we also have written questions.

I will now recognize myself for 5 minutes of questions.

I want to commend Ms. Banker and Mr. Ryan, Yahoo and AOL for the wonderful steps that they have taken to—taken to try to help keep children safe online.

You mentioned your work with the National Center for Missing and Exploited Children to create a database for automatic identification and removal of known child pornography images.

Is there anything that Congress can do to help make that a reality?

Ms. BANKER. We think there is something that could be done, and one of those things is that there is information that the National Center has about the attributes of images, and as we work, as companies, to develop new technologies with the goal of doing a better job of detecting and removing these types of illegal images from our networks, we think there may be a need to find out more information about the nature of those images in order to make our screening technology more intelligent about those issues. And that is a provision that we would like to see additional authority given to the National Center to allow them to share that information with us.

Ms. SÁNCHEZ. Can you also talk a little bit about some of the emerging issues in the area of child safety?

Ms. BANKER. One of the big issues that we see coming up for teens in terms of online safety is cyber bullying. And we have been working online and off line to address that issue, including the summit, I mentioned, on Friday on cyber safety is going to address cyber bullying as part of that; and it is focused to educate or to help them understand what types of issues their students will be facing.

We are also sponsoring the i-SAFE curriculum in middle schools in Sunnyvale, California, where we are headquartered, so that teens will learn about cyber bullying and how to address it in their day-to-day lives.

We also noted that you have addressed cyber bullying in your education bill, and we are very glad to see resources being allocated for that important issue.

Ms. SÁNCHEZ. It strikes me, and we have heard very compelling testimony from all of the panels today, but it strikes me that there are the three tools of law enforcement, which are prevention, enforcement and punishment.

What has been discussed today has been the enforcement and punishment, and it was said in the earlier panels, the first line of defense is their parents. But I really believe the first line of defense for children is themselves, and being knowledgeable about what to do if they are online and they are getting improper contact or messages that make them uncomfortable. And I know there are a number of programs that are aimed towards trying to teach children about online safety, and perhaps that aspect of it doesn't get a lot of attention, although really it should because children need to be educated about what to look for when they are online.

Mr. Weeks, I am painfully aware of the fact there is a lack of resources that have been dedicated towards prosecuting these online predators. And that seems to be an overriding theme among all of the panelists that, really, if Congress were serious about this, we would stop spewing rhetoric and do things where we take into account their real costs and are really going to be effective; and I really have to commend you for being tough and speaking the truth.

I mean, speaking truth to power is often the first thing that needs to happen in order to chang attitudes, and unfortunately, up here, oftentimes the easy or least costly solutions are what people grasp for so that they can say, well, we have done something about this.

You did mention, though, in addition to needing more resources and funding for enforcement, that there are perhaps other things that Congress can do as well to help prosecute these predators.

Could you just mention, in as much time as is left, some of those things that Congress can do to help?

Mr. WEEKS. Well, I think there has been a number of bills suggested today that are very good and will help law enforcement and help us do this.

I would add one thing that I think would have a tremendous impact, and that is simply accountability. I think that in communities small and large across the country, nobody in terms of prosecutors, really, is held accountable. We understand the concept of holding judges accountable. We know what we are seeing when we see a judge that sits at the bench and looks at child pornography and then gives probation. But it is not the judges 99 percent of the time who makes those decisions. It is the prosecutors. Most of these cases never get—they are plea bargained before they ever get to a judge.

So accountability in terms of—call it sunshine. If this country—if our citizens knew who took this seriously and who didn't, I think people would change their behavior overnight.

Ms. SÁNCHEZ. Thank you.

My time has expired.

I will recognize the gentleman from Florida for 5 minutes of questions.

Mr. KELLER. For me, the bottom line is online predators must be captured, prosecuted and locked away. No question. Since we are limited to 5 minutes, I am going to limit my questions to the narrow issue of grooming. And that is a behavior that occurs when Internet child predators lie about their age to entice their victims.

For example, earlier today, Alicia testified, "I chatted for months with Christeen, a beautiful red-haired 14-year old girl who just understood me all too well. Christeen was really a middle-aged pervert named John. Somehow in this process, this grooming of me had changed me, had destroyed my ability to reason."

A few months ago, the Florida legislature passed the Cyber Crimes Against Children Act and became the only State in the Nation with a law specifically targeting grooming; 49 out of 50 States have no such law on the books, and the Federal Government has no such law on the books.

Let me begin with Mr. Waters.

What is your experience in dealing with this behavior that we are hearing about called grooming?

Mr. WATERS. Thank you, sir.

We do get a lot of reactive calls where we have children in our State that have been contacted by individuals.

Frequently, we have trouble coming up with chargeable actions if the individuals have not yet started specifically addressing the sexual activity they are looking for with the child or they haven't arranged the meeting.

Mr. KELLER. Is there—is it a common phenomenon for these online predators for them to misrepresent their age to give young teenagers a false sense of security?

Mr. WATERS. It is.

Mr. KELLER. Let me ask you, Ms. Collins, and I know your national center collects a wide variety of data. Do you see this as a problem?

Ms. COLLINS. Absolutely—the problem of online grooming. And we also accept reports of enticement. In fact, we have had a 300 percent, approximately 300 percent increase in just the last year with reports coming in from the public regarding enticement.

It is a big problem. The children, boys and girls in their teen years, are especially vulnerable, particularly girls between the ages of 13 and 15.

The offenders who are targeting them know exactly what they need to do in order to work their way into the child's life, much like they did with—like they did with Alicia.

We see them being deceptive about their age, certainly about their motives. But also they are not only lying about their age, and they are simply playing upon the emotional vulnerability on the child and trying to work in that way.

Mr. KELLER. Mr. Mason, over at the FBI, do you see this issue of this grooming taking place with the child predators lying about their age to make the victims feel more comfortable and give them more information.

Mr. MASON. Yes, sir. We do.

Mr. KELLER. What is it about this behavior that makes child predators think they have to lie about their age? Why does it benefit them, from your investigative point of view?

Mr. ATWOOD. They want to make themselves like the victim, and age is a common factor that they can have with the victim. So they certainly use that as a ploy to get children to speak to them.

And, unfortunately, as Mr. Weeks said, there is—that sometimes at the beginning stage, if you intervene at that stage, there is not much legally that you can do with somebody who is molding them out to be a 16-year old who happens to be a 37-year old.

Mr. KELLER. Would you agree, if there was a law on the books making that a crime to misrepresent their age, that would make it easier then to prosecute them and gather information from the perpetrators?

Mr. MASON. I would agree with that.

Mr. KELLER. And over at Department of Justice, Mr. Rothenberg, do you have any opinion on whether that would make it easier to do the investigation and prosecution if there was a law on the books making it a crime to engage in the misrepresenting of age through grooming?

Mr. ROTHENBERG. I think it is—certainly we would be happy to look at it.

Right now, without language in front of me, it would be difficult for me to express an opinion, but we are happy to work with you on that and take a look at your—any proposals you would have.

Mr. KELLER. Thank you.

Ms. Collins, I had an experience earlier this week. I opened an office to help catch child predators in Orlando, and he cited some specifics from your organization, National Center for Exploited Children.

He said there are 77 million kids that use the Internet daily, and one out of seven kids between the ages of 10 and 17 are sexually solicited online.

Does that sound correct based on your data?

Ms. COLLINS. That is the newest data that——

Mr. KELLER. Where is that trending?

Ms. COLLINS. The original research was conducted in 2001, and at that time, it was one in five children had admitted that they had been sexually solicited online. The good news is it is not saying one in seven. We are hoping that that may have something to do with the prevention work that has been done by countless agencies.

The unfortunate reality, though, is even though the number appears to have been going down in terms of the solicitation, the aggressive solicitations have not changed at all. That would be those solicitors that were trying to reach a child by mail, by phone or in person, and those have held steady since 5 years earlier, as well as the unfortunate fact that many of these children, more than half of them, never tell an adult, a trusted adult, when those things happen to them.

So those are the areas we need to continue working on.

Mr. KELLER. Thank you. My time has expired.

I yield back.

Ms. SÁNCHEZ. I would now like to recognize the gentlewoman from Florida, Ms. Wasserman Schultz.

Ms. WASSERMAN SCHULTZ. My questions will primarily be for Mr. Mason.

Mr. Mason, Arnold Bell is the chief of your Images Unit. Can you tell me why he isn't here to testify?

Mr. MASON. He is here. He is sitting behind me, but I was asked to testify.

Ms. WASSERMAN SCHULTZ. I believe Mr. Bell was actually invited to do the testifying. Was there a substitution made in the Justice Department?

Mr. MASON. Not in the Justice Department. But in the FBI. I only received notification that I was going to be testifying here today.

Ms. WASSERMAN SCHULTZ. Mr. Bell is the person with the most in-depth knowledge about the FBI Innocent Images Unit; isn't he?

Mr. MASON. That is correct.

Ms. WASSERMAN SCHULTZ. I was personally disappointed that he was not sitting here at the table because we would want the person with the in-depth knowledge to be the one who answers the questions.

Can you get back to me why the switch was made? Because I know it didn't come from the Committee on the Judiciary.

Mr. MASON. I can do that.

Ms. WASSERMAN SCHULTZ. Who is James Finch?

Mr. MASON. He is the director of our Cyber Division.

Ms. WASSERMAN SCHULTZ. You are aware, aren't you, that Senator Biden, Joe Biden, wrote a letter to FBI Director Robert Mueller asking him specific and detailed questions about the FBI Innocent Images Unit; aren't you?

Mr. MASON. Yes, I am.

Ms. WASSERMAN SCHULTZ. And Mr. Finch has responded to Mr. Biden. Have you seen the letter?

Mr. MASON. I didn't see the letter, but I know he did respond to the letter.

Ms. WASSERMAN SCHULTZ. I prepared a copy of the letter to submit it for the record.

[The information referred to follows:]

JOSEPH R. BIDEN, JR.
DELAWARE

www.biden.senate.gov

United States Senate

June 5, 2007

JUDICIARY SUBCOMMITTEE
ON CRIME AND DRUGS
CHAIRMAN

FOREIGN RELATIONS COMMITTEE
CHAIRMAN

CAUCUS ON INTERNATIONAL
NARCOTICS CONTROL
CHAIRMAN

CONGRESSIONAL INTERNATIONAL
ANTI-PIRACY CAUCUS
CO-CHAIRMAN

AFFIRMATIVE CAUCUS
CO-CHAIRMAN

By Electronic and Regular Mail

Director Robert F. Mueller
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

Dear Director Mueller:

I am increasingly concerned about the profusion of child pornography trafficked over the Internet. The latest research shows that this threat to our children continues to grow, with offenders trading images of younger victims subjected to more graphic brutal sexual abuse.

Like you, I believe that we must do all that we can to prevent child exploitation and bring child predators to justice. I understand that the FBI has many effective and dedicated agents working tirelessly on this problem. I am not convinced, however, that we have dedicated enough resources toward programs that effectively combat the problem, such as Innocent Images.

I believe that we should enhance the capacity of state and local law enforcement through programs like the Internet Crimes Against Children ("ICAC") Task Force program so that local law enforcement can effectively investigate and prosecute the vast majority of online child exploitation cases and the FBI can focus on complex cases and those that have an international component.

In order to get a better perspective on the extent of the problem and the FBI's efforts to address it, I would appreciate it if you would answer the attached questions in writing within 14 days.

You may contact Nelson Peacock on my Judiciary staff at (202)-514-0558 or Nelson_Peacock@judiciary-dem.senate.gov with any questions and the written responses.

Sincerely,

Joseph R. Biden, Jr.

844 NORTH KING STREET
WILMINGTON, DELAWARE 19801-3519
(302) 573-6345

1105 NORTH MARKET STREET
SUITE 1004
WILMINGTON, DELAWARE 19801-1220
(302) 573-6345

Questions from Senator Joseph R. Biden, Jr.
Chairman, Crime and Drugs Subcommittee
Senate Judiciary Committee

Innocent Images National Initiative Headquarters

Q: In testimony before Congress on May 3, 2006, Cyber Division Section Chief Raul Roldan stated, "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."

1. What is the total number of personnel within the Innocent Images National Initiative program under the direct or indirect supervision of the unit director? (this should not include agents, analysts or other personnel at FBI field offices or labs, even though they may assist with Innocent Images cases.)

2. What were the total 2005 and/or 2006 expenditures for the Innocent Images Unit? What amount, if any, was "passed through" to other FBI programs, outside agencies, or other entities?

Dedicated Investigators, Analysts, Administrative and Support Staff
How many agents are dedicated specifically to working Section "305 matters" (305 classification referring to online exploitation)? If this number is different from the 127 positions referred to by Roldan, please explain. If the category "305 matters" does not sufficiently cover all work done on child pornography and enticement crimes, please explain and provide a breakdown including information on other classifications.

Assuming personnel outside the Innocent Images program must also occasionally work non-305 cases (e.g., terrorism or other urgent cases), "exclusively dedicated" should be defined as spending 90% or more of time on 305 matters? Please break down these dedicated staff positions by number of agents, analysts, support staff or other function.

Other Full-Time Equivalents
Please provide an estimated number of FTEs in addition to personnel identified above that are working section 305 or equivalent cases.

Overlap

If any of the assets mentioned above overlap with other important areas related to child protection, such as child prostitution or trafficking (e.g., the Innocence Lost program), please clearly break these down.

The Scope of the Problem

In order to determine the extent of the problem as it exists today please answer the following:

1. For the last five-year period for which data is available, please provide an estimate of the total number of child pornography or online child enticement transactions over peer-to-peer networks that the FBI is aware of, broken down by type or source if data is available.

2. For the last five-year period for which data is available, please provide an estimate of the total number of suspects identified by the FBI engaged in commercial child pornography production, distribution or purchase within the U.S. and worldwide. Indicators should include, but not be limited to, the number of unique credit cards used in commercial child pornography transactions and the number of "members" or subscribers identified participating in child pornography commerce websites or rings.

3. If data is not available specifically for cases involving commercial production, distribution or downloading, please provide data on the number of suspects identified during this period, both commercial and non-commercial, by type of crime.

4. Are there any other statistical indicators of the magnitude of sexual exploitation crimes—especially child pornography production, distribution and possession—that you can provide to assist the U.S. Senate in understanding the size and nature of this problem?

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 11, 2007

Honorable Joseph R. Biden, Jr.
Chairman, Judiciary Subcommittee
On Crime and Drugs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am writing in response to your letter to Director Robert S. Mueller, III, concerning the FBI's Innocent Images Unit, and the previous testimony provided by Section Chief (SC) Raul Roldan from the Cyber Division.

Innocent Images National Initiative Headquarters

(1) What is the total number of personnel within the Innocent Images National Initiative program under the direct or indirect supervision of the unit director? (this should not include agents, analysts or other personnel at FBI field offices or labs, even though they may assist with Innocent Images cases.)

Response: The current number of personnel assigned to the Innocent Images National Initiative (IINI), located in Calverton, MD, is 32 members, including the Unit Chief (UC). The UC supervises three Supervisory Special Agents(SSA), ten Special Agents (SAs) who conduct investigations, six Intelligence Analysts (IAs), six Investigative Support Specialist (ISS), and four Management Program Analysts (MPA). The IINI has stationed one SSA, one MPA and three ISSs for permanent assignment at the National Center for Missing and Exploited Children. Further, the IINI typically hosts between four to six international officers who are co-located with the IINI staff.

(2) What were the total 2005 and/or 2006 expenditures for the Innocent Images Unit? What amount, if any, was "passed through" to other FBI programs, outside agencies, or other entities?

Response: In fiscal year (FY) 2005, the IINI received $6,829,965 in Congressional funding. The IINI expended $3,871,491, and transferred $2,310,000 to the Internet Crimes Complaint Center (IC3); $258,594 for a Congressional recission; $73,617 to the

Honorable Joseph R. Biden, Jr.

Finance Division (FD) for a compensations and benefits shortfall; and $200,000 to the Sentinel information technology program.

In FY 2006, the IINI received $6,397,771 in Congressional funding. The IINI expended $4,392,650, and transferred $1,535,000 to IC3; $202,500 to a 1% recission, $75,621 for a negotiated savings; and $192,000 to FD for a holdback.

(3) How many agents are dedicated to specifically working Section "305 matters" (305 classification referring to online exploitation)? If this number is different from the 127 positions referred to by Roldan, please explain. If the category "305 matters" does not sufficiently cover all work done on child pornography and enticement crimes, please explain and provide a breakdown including information on other classifications.

Response: All 32 members of the IINI program are exclusively dedicated to working "305 matters." The number of funded staffing level (FSL) positions cited in the quote from the testimony of SC Roldan reflects the Congressionally allocated and funded positions in the field offices allocated to the IINI. The 127 figure is the summation of the 60 positions funded in 1998, an additional 45 positions in 1999, and an additional 22 positions in 2006. The actual Time Utilization Record Keeping (TURK) attributed to the IINI program has fluctuated between 232 and 250 SAs, an overutilization of an additional 123 FSL positions that are not assigned to the IINI. Currently, the IINI program expends 260 SA resources investigating "305 matters." The FBI's TURK system does not track support personnel or non-FBI task force members. Thus, the total number of personnel investigating this violation on behalf of the FBI exceeds the 260 TURK figure.

The 305 classification pertains only to the investigation of the online sexual exploitation of children.

- 305A - Online E-groups, organizations, and websites that exploit children; and for-profit enterprises that exploit children.
- 305B - Individuals who indicate a willingness to travel interstate for the purpose of engaging in sexual activity with a minor and individuals who entice (or attempts to entice) a minor to travel interstate for the purpose of engaging in sexual activity with that individual.
- 305C - Producers and manufacturers of child pornography and major distributors of child pornography.

Honorable Joseph R. Biden, Jr.

- 305D - Possessors of child pornography.
- 305E - Innocent Images training.

(4) Assuming personnel outside the Innocent Images program must also occasionally work on non-305 cases (e.g., terrorism or other urgent cases), "exclusively dedicated" should be defined as spending 90% or more of time on 305 matters? Please break down these dedicated staff positions by number of agents, analysts, support staff or other function.

Response: All members of the IINI, both Agent and professional support, are exclusively dedicated to 305 matters.

(5) Please provide an estimated number of FTEs in addition to personnel identified above that are working 305 or equivalent cases.

Response: There are no additional personnel, other than previously described, conducting investigations of child pornography.

(6) If any of the assets mentioned above overlap with other important areas related to child protection, such as child prostitution or trafficking (e.g., the Innocence Lost program), please clearly break these down.

Response: The IINI (305 matters) is separate and distinct from other FBI Crimes against Children (CAC) classifications, such as the Innocence Lost project conducted by the Criminal Investigative Division. However, in some instances CAC agents are utilized to support IINI matters, and the SAs record their time utilized on 305 matters which becomes part of the cumulative SA TURK system.

<u>The Scope of the Problem</u>

In order to determine the extent of the problem as it exists today please answer the following:

(7) For the last five-year period for which data is available, please provide an estimate of the total number of child pornography or online child enticement <u>transactions</u> over peer-to-peer networks that the FBI is aware of, broken down by type or source if data is available.

Response: The FBI does not track the number of peer-to-peer transactions over the peer-to-peer backbone. However, the Internet Crimes Against Children (ICAC) program does monitor

Honorable Joseph R. Biden, Jr.

peer-to-peer transactions. According to their data, these transactions are several million in number, and the volume increases daily.

(8) For the last five-year period for which data is available, please provide an estimate of the total number of suspects identified by the FBI engaged in commercial child pornography production, distribution or purchase with the U.S. and worldwide. Indicators should include, but not be limited to, the number of unique credit cards used in commercial child pornography transactions and the number of "members" or subscribers identified participating in child pornography commerce websites or rings.

Response: For the last five-year period, there have been an estimated 25,000 suspects identified by the FBI who have engaged in commercial child pornography. The following are a few examples:

- In the FBI's "Orangebill" investigation, more than 5000 customers were identified who used this company to process credit card transactions specifically to gain access to child pornography websites. Leads were sent throughout the US including which identified 50 U.S. companies that hosted approximately 350 websites related to child pornography. 2000 leads were referred to foreign law enforcement agencies via the FBI Legal Attachés, and 3000 leads were referred to the ICAC Task Forces.

- The FBI identified more than 200 users of the E-gold online currency company who paid into a single E-gold account to gain access to child pornography. To date, multiple additional accounts of this type have been identified.

- Between FY 2002 - 2007, the FBI has been responsible for shutting down at least 6,316 child pornography websites/web hosts.

- From June 2005 to May 2006, the Innocent Images International Task Force Sex Tourism website received 21,490 visitors. The web site received approximately 300 e-mails and a review yielded approximately 15 subjects who expressed an interest in traveling from the United States overseas to engage in sexual activity with underage children. The IINI sent 15 leads to other FBI Divisions for further investigation. Two of those leads have yielded results which led to the search and/or arrest of the subject. E-mails received from foreign countries were referred as leads to those specific countries' law enforcement agencies

Honorable Joseph R. Biden, Jr.

through the IINI International Task Force members. Specifically, leads were forwarded to Australia, the United Kingdom, and Thailand, which resulted in the identification of subjects, the execution of search warrants, and the arrests of subjects.

(9) If data is not available specifically for cases involving commercial production, distribution or downloading, please provide data on the number of suspects identified during this period, both commercial and non-commercial, by type of crime.

Response: Between FY 2001-2007 (as of 06/27/2007), the number of suspects identified and arrested by the FBI for online child exploitation under all 305 classifications is **5,048**. The breakdown per classification is as follows:

- 305A - **1,814**
- 305B - **1,256**
- 305C - **1,257**
- 305D - **721**

(10) Are there any other statistical indicators of the magnitude of sexual exploitation crimes - especially child pornography production, distribution, and possession - that you can provide to assist the U.S. Senate in understanding the size and nature of this problem?

Response: The FBI's Innocent Images grew exponentially between fiscal years 1996 and 2006, as follows:

- 1789% increase in Cases Opened (113 to 2135)
- 878% increase in Informations & Indictments (99 to 968)
- 2174% increase in Arrests, Locates & Summons (68 to 1546)
- 1397% increase in Convictions & Pretrial Diversions (68 to 1018)

Honorable Joseph R. Biden, Jr.

I appreciate your interest in the FBI's fight against child pornography on the Internet and I hope this information will be of assistance to you.

Sincerely yours,

James E. Finch

James E. Finch
Assistant Director
Cyber Division

Ms. WASSERMAN SCHULTZ. You know then, Mr. Mason, that in Mr. Finch's letter, he stated that the Innocent Images Unit currently has 32 staff members, including 13 investigators; is that correct?

Mr. MASON. That is correct.

Ms. WASSERMAN SCHULTZ. Do you know how large the unit was in 2006?

Mr. MASON. I do not.

Ms. WASSERMAN SCHULTZ. Was it smaller or bigger or about the same?

Mr. MASON. It was larger.

Ms. WASSERMAN SCHULTZ. I think the number was closer to 40.

So the number of the agents actually has shrunk since Congressman Barton, when he chaired the Energy and Commerce Committee, since his hearings last year, the number of investigators was actually less this year than it was last year; correct?

Mr. MASON. In the Innocent Images Unit, yes.

Ms. WASSERMAN SCHULTZ. The total budget for that unit is about $30 million?

Mr. MASON. No, ma'am. Are you talking annually?

Ms. WASSERMAN SCHULTZ. I am.

Mr. MASON. No, it is not $30 million. If you are talking about appropriated money, it is around—it is closer to $6 million.

Ms. WASSERMAN SCHULTZ. But total funds is $30 million?

Mr. MASON. I am not sure what you are making reference to.

Ms. WASSERMAN SCHULTZ. What I am making reference to is Mr. Finch also stated in his letter to Senator Biden that approximately $3.8 million was transferred from Innocent Images to IC3, which is the Internet Crimes Complaint Center.

Mr. MASON. That is correct.

Ms. WASSERMAN SCHULTZ. What is IC3?

Mr. MASON. It is a location we have in West Virginia where we collect Internet complaints, Internet crime complaints. It is a place to aggregate it because the average Internet fraud amounts to about $75, so we were looking for a way to aggregate all of those complaints to find out when in fact we had a problem.

Ms. WASSERMAN SCHULTZ. They investigate fraud and white collar crime; correct?

Mr. MASON. That is correct.

Ms. WASSERMAN SCHULTZ. Why is so much of Innocent Images being sent to an agency that has nothing to do with child protection?

Mr. WEEKS. Well, in fact, it does, and in fact over a thousand complaints last year came in to IC3 through the Internet Crime Complaint Center.

Ms. WASSERMAN SCHULTZ. Child protection complaints came into IC3?

Mr. MASON. No. Complaints of suspected child molestation. And so the fact of the matter is, the average American doesn't understand necessarily that it is for white collar crime only. They only know it is an Internet Crime Complaint Center, and they make calls of all natures, of all natures to the Internet, to IC3.

Ms. WASSERMAN SCHULTZ. But the majority of the resources should be with the Innocent Images program and not diverted to

an agency that is dedicated to white collar crime and Internet fraud; wouldn't you agree?

Mr. MASON. That didn't just go to IC3. It went to that and to our Cyber Fusion Center. It was split between the two. We see that as a force multiplier, so we do not see it as a diversion away—against Crimes Against Children but rather as yet another type of force multiplier that helps us to identify even more perpetrators of crimes against children.

Ms. WASSERMAN SCHULTZ. You are aware that we are investigating less than 2 percent of the activity?

Mr. MASON. I am.

Ms. WASSERMAN SCHULTZ. Particularly because you compared the activities to speeders in your comments earlier.

Mr. MASON. Only as a scope issue.

Ms. WASSERMAN SCHULTZ. I think it was an unfortunate analogy, which you acknowledged.

Has your department, your division, or any entity in the Department of Justice asked for more money in the President's budget request to come back to cyber crime?

Mr. MASON. We have not asked for more money, but we have indicated in 2008 that none of the money for Innocent Images will be diverted anywhere else.

Ms. WASSERMAN SCHULTZ. That is comforting. It would be good if the U.S. Department of Justice refocused their priorities on making sure that we up the percentage of crimes that we can, against children, that we can investigate beyond 2 percent.

Ms. SÁNCHEZ. The time has expired.

If there is sufficient interest, if there are other Members who would like an additional 5 minutes for questions, since there are so few of us remaining.

Ms. WASSERMAN SCHULTZ. I don't need 5 minutes, but I would like to ask Mr. Weeks one question.

Ms. SÁNCHEZ. Without objection, the gentlewoman would be granted 2 additional minutes.

Ms. WASSERMAN SCHULTZ. Thank you.

You talked about a need for accountability. How does a special counsel at the Department of Justice who would be dedicated to coordinating all of the activity do what you were describing in terms of achieving that accountability? This would be a special counsel at the Department of Justice for child exploitation.

Mr. WEEKS. My personal opinion is that, rather than a special counsel, we probably need a czar. If there is anything stronger than a czar, we need that.

There are so many efforts going on right now within the Department of Justice. Just within the Department of Justice, you have got the ICAC program. You have got the FBI. You have got to CEOS, the Child Exploitation Obscenity Section. You have got Project Safe Childhood. You have got the U.S. Attorneys program.

There is an urgent need for coordination, planning. And with that will come inevitably some elimination of duplicated efforts.

I don't think anybody up here would believe for a second that we have to worry right now about waste or lack of efficiency because these folks are doing incredible work with very little money.

But the point is a special counsel would enable the Department of Justice to do exactly what you have been calling for, which is to refocus this effort and do it in a deliberate and efficient way.

Ms. SÁNCHEZ. At this time, I would recognize Mr. Forbes for 5 minutes of questioning.

Mr. FORBES. Thank you.

It is always interesting to me when we talk about accountability, we held a hearing down in Louisiana. We found out 12 percent of the people arrested ever actually went to jail. Part of that was judges, and part of it was prosecutors.

And the difference that Mr. Weeks didn't point out is, when you have judges, you have a record there that you can look at, a transcript, and you compare the sentence to the record.

When you are dealing with prosecutors, you don't have that record. You can't disclose whether witnesses were willing to testify, whether there were evidentiary problems, all of which prosecutors have to take into play.

Mr. Rothenberg, we know that the Justice Department's proposed crime bill included a provision to include a mandatory minimum for possession of child pornography.

Will you explain why that is needed?

Mr. ROTHENBERG. We believe, and we have seen in the attitude of a number of judges, child porn is not treated as seriously as it should be. As I said and as other witnesses have said, the demand for child pornography is what drives all of these crimes against children and especially over the Internet. In fact, even the young lady, Alicia, who testified earlier today so movingly commented that the man who kidnapped her, took photos and shared them with his friends, obviously, those people were participating in the victimization of her even though they were, so to speak, only looking at photos.

And we do have a problem, as my testimony states, in slightly more than one-quarter of all child pornography offenses, the guidelines—the judges are not following the guidelines that would apply to these offenders who possess child pornography, and we believe that by establishing a 2-year mandatory minimum, we will be establishing at least a floor that anybody who possesses child pornography will go to jail for 2 years, and we believe that would send a signal to the judges, first of all.

It would also send a signal, express ours and Congress's opinion about the severity of the crime, and it would be very useful for the prosecutor to have.

There have been cases where an offender in Chicago who was a drug offender, and he had been sentenced to home confinement. And he spent his time downloading hundreds of images of children being sexually assaulted. And the judge at the district court level sentenced him to 1 day of prison (and supervised release) but 1 day in prison.

We appealed that, and it was reversed in a very eloquent opinion by Judge Posner in the Seventh Circuit.

But that is the attitude some judges have. And by establishing a mandatory minimum, we can prevent that.

Mr. FORBES. Mr. Ryan, I want to compliment AOL for retention of records, and I want to ask you, what is the process for AOL to

retain subscriber records and then provide these records to law enforcement via subpoena? How long does AOL contain those records, and how cumbersome, and is it necessary to retain them any longer?

Mr. RYAN. We found our existing retention scheme for our records has been very effective in our partnership with law enforcement coupled with the active use of the preservation requests. We received over 2,000 preservation requests last year, and recently, we tallied over 80 percent from the States that are actively engaged, primarily the ICAC task forces that issued preservation requests followed up with further legal process, typically search warrants.

That signifies to us that that is an active investigation leading to prosecution. And the fact that we have testified in a number of those cases has demonstrated that that tool is extremely effective.

Retention can be misleading because there are no uniform standards of what records are kept among various companies.

That is due to the different architecture of various networks and the various business models.

So we have found that works effectively for AOL. That may not be as effective for one of our colleagues.

So we focus on what works best and most effectively for us, and we think the key is an active partnership with law enforcement because this data, no matter how long it is kept, these are real-time cases, the response has to be typically within 24 to 48 hours to get to the bottom of the case.

So staffing is actually—we find more critical than the availability of records.

Mr. FORBES. Ms. Collins, will you submit for the record how—just an explanation for us of how NIC networks with ISPs, the financial institutions, law enforcement agencies to investigate child pornography sites, and what additional resources we need to get the job done?

Ms. COLLINS. Approximately 40 percent of the reports we receive each week actually come from the service providers. Law enforcement really loves the reports that we get from companies such as AOL, Yahoo and so forth, and the companies have been very good about complying with the Federal law mandating that they report child pornography.

Unfortunately, in order for them to make a tip to the CyberTip line, they need to make a report with us so we know who the person is. There is no mandate that the companies actually register with us. The contents of reports, when we have a new ISP calling—actually, I have staff right now in San Jose, California, registering new ISPs at a conference out there. We have registered about 18 out there alone. We have to convince them of what they should be reporting. We have to kind of call upon their good nature in trying to do the right thing in order to get the appropriate content.

Companies such as Yahoo and AOL have been wonderful, but we have been working with them for many years. It would be very useful to have an established content of reports to be provided in a cyber tip line as well as some overarching maintenance of records and retention.

But law enforcement, we are making hundreds of referrals every week. They are not able to get to these reports in a few days.

So we ask that possibly the electronic service provider have more consistency in how long they maintain this data to provide to law enforcement with the legal process that they need.

Ms. SÁNCHEZ. Mr. Keller is recognized for 5 minutes.

Mr. KELLER. Let me go back to you, Ms. Collins, on behalf of the National Center for Missing and Exploited Children.

If there are parents and teachers as well as teenagers watching your testimony today, do you have any tips or proactive steps to protect against child predators that you can direct them to, maybe a Web site link about, these are the five things that every parent or teacher should know?

Ms. COLLINS. I think that it goes to something that you stated earlier about the child, whether it be the child as the first or the last line of defense for themselves.

I think that there are remarkable programs out there of online safety. We used to have many of these tips listed on our Web site at cybertipline.com, but we really need to be able or to empower these children to be able to recognize the warning signs. And I think that it is also important for parents to, when they hear the topic of Internet predation, to be able to keep some perspective of it that not every child is of equal risk of being approached by a predator, but there are some significant risks of encountering a bad person. That may be chatting with people they don't know online, talking about sexually explicit topics, sending photographs online. All of these will raise the risk of a child of finding somebody who wants to perpetrate against them.

Mr. FORBES. And those tips can be find on cybertipline.com?

Ms. COLLINS. I would also like to recommend that they go to our Web site, which is netsmarts411.org. They can ask any question that they wish, and our analysts will respond in a very clear cut English nontechnological answer of what it is, whether they want to know how to delete a MySpace page; how do I make my child's social networking page private? They can get the answers from that group.

Mr. KELLER. I am going to start with you on my next question that is the issue of recidivism. For those listening, a fancy way of saying people get out of jail and do it again.

Do you have any statistics when it comes to sex crimes, child molesters, what the recidivism rate is?

Ms. COLLINS. I do not have those numbers for you.

Mr. KELLER. If anybody has any recidivism statistics, if you can raise your hand, I will call on you.

Mr. Weeks.

Mr. WEEKS. I will offer this. We deal with this issue in a lot of the State legislatures where we are working on legislation. Today we heard some pretty outrageous statistics about low recidivism rates for sex offenders.

We have always told our volunteers and our people that you will never win that fight.

Mr. KELLER. Do you have a recidivism——

Mr. WEEKS. There was one in Canada that was done recently that was very good. Essentially, you have this problem, though.

Mr. KELLER. I just need the number because I have other questions.

The reason that is a significant question, we have heard that it is two-pronged, prevention and enforcement. And if you could talk about a kid who is engaged in shoplifting or vandalism, I would totally agree with it. But I think some of these people can't be fixed, frankly. And I think looking them up is the only way to go.

So, in Florida, we have something called the Jimmy Ryce Act that, after their term is over, we still keep them civilly confined, and thank God we do, because they are going to do it again; and that is why this issue of recidivism is really key to look at because some of these folks are just messed up and are unfixable through any form of rehab.

Ms. WASSERMAN SCHULTZ. Will the gentleman yield?

We also passed the Federal version of the Jimmy Ryce Act and the Adam Walsh Act as well. I am hopeful, and you were strongly supportive of it, and my good friend from Florida, I am really hopeful that other States will take the urging that Congress made in passing that and adopt their own civil confinement laws.

Ms. SÁNCHEZ. The time of the gentleman has expired.

Mr. ROTHENBERG. I wanted to reassure the Congresswoman that the Bureau of Prisons is enforcing the authority that you gave us last year. We have certified several dozen defendants who are currently incarcerated for civil confinement. And it has been challenged, and we are defending our authority to do that very vigorously.

Ms. WASSERMAN SCHULTZ. Madam Chair, if you are about to adjourn, can I ask the indulgence of the Committee and ask unanimous consent for 2 of my 3 additional minutes?

Ms. SÁNCHEZ. I will recognize myself for 5 minutes and then yield to the gentlewoman from Florida.

Ms. WASSERMAN SCHULTZ. Thank you very much.

Ms. Collins, can you tell me on the CyberTip line leads, how many of those does NCMEC send out to the ICACs each year?

Ms. COLLINS. Last year, received about 76,000 leads through the CyberTip line. I do not have that number for you. I can get that to you when I get back. I have that at my office. I can submit that to you.

But the vast majority of the leads that we do send out to local, State and Federal law enforcement, I would say approximately 70, 75 percent are going to the ICAC task force.

Ms. WASSERMAN SCHULTZ. Is it thousands?

Ms. COLLINS. Absolutely.

Ms. WASSERMAN SCHULTZ. How many leads does, Mr. Waters, does the ICAC send out?

Mr. WATERS. We set up the system so that each State can query those dynamically and query those, pull those leads directly. Wyoming, being the State with the lowest population, has roughly 2,000 leads a year, and it runs the gamut from there.

Ms. WASSERMAN SCHULTZ. So if Wyoming has the smallest population and arguably the smallest number of leads, this is hundreds of thousands of leads we could be dealing with.

Is there any difference between the kind of referrals coming from the NCMEC and those coming from the ICAC data, that network, that either of you are familiar with?

Ms. COLLINS. Sure. The reports we are receiving is a combination of what is coming in from electronic service providers as what is coming in from the public.

It can be a parent who said that they found that their child is communicating with a stranger online. It could be somebody who encountered child pornography online.

Agent Waters can correct me if I am wrong, but primarily, the ICAC data network is providing information out to law enforcement regarding individuals using peer-to-peer technology to trade images and videos of child pornography.

Ms. WASSERMAN SCHULTZ. Mr. Waters, did you want to answer?

Mr. WATERS. That is the primary distinction.

One of the advantages that we have from those individuals that we can triage that data so that we can categorize threat levels. Not only do we see who is trading, but we see the volume and the time frame they are trading, the level of sadomasochism against the child. So we can select the best image.

Ms. WASSERMAN SCHULTZ. So your process is just more formalized and scientific as opposed to more informal referral?

Mr. WATERS. Well, because we know where we are going to be looking at the beginning of each day, we know how to look. But the CyberTip line is receiving information from all types of folks that come across this material. So it runs the gamut of what they run into.

Ms. COLLINS. It really does run the gamut. We have over 20 analysts in our CyberTip line that have a tremendous amount of value before we refer these leads up to law enforcement.

Because we get so many leads from the ISPs and from the electronic service providers that provide us with the images, we need to rely very closely on our relationship with the ICAC task forces because we are not a law enforcement agency that can mail CDs of child pornography. So we allow law enforcement to secure encrypted access into our system.

Ms. SÁNCHEZ. I want to thank our witnesses for their testimony. The issues of misuse of the Internet for the commission of sex crimes against children is one of the—is one of manifest importance for every American, and it is a difficult problem for which there is not one easy solution.

Nonetheless, I want to commend all of our witnesses for their commitment to addressing this problem. We have heard some very good ideas today that hopefully will give Congress guidance as we proceed to move forward in trying to tackle this very difficult issue.

Without objection, Members will have 5 legislative days to submit any additional written questions for our analysts which we will forward to you and ask that you answer as promptly as you can so that they can be made part of the record.

And without objection, the record will remain open for 5 legislative days for the submission of any other additional materials.

And with that, this hearing is adjourned.

[Whereupon, at 5:30 p.m., the Committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE LAMAR SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND RANKING MEMBER, COMMITTEE ON THE JUDICIARY

Thank you, Mr. Chairman.

The hearing today is on an important topic—protecting our children from sexual exploitation on the Internet.

We all agree that we must protect America's children from sex offenders. We also agree that law enforcement agencies need additional resources to bring child predators to justice.

Resources, however, are not enough. If Congress is serious about combating this heinous crime, then we must provide law enforcement personnel with the tools needed to stop sexual attacks on children that are broadcast over the Internet.

Sexual predators use the same Internet technology that has revolutionized our way of life to stalk our children. Our criminal laws must keep pace with our technology.

The FBI estimates that as many as 50,000 child predators are online at any time searching for their next victim.

Today, one in five American children between the ages of 10 and 17 will be sexually solicited online during their lifetime.

Just last year, Congress enacted the Adam Walsh Child Protection and Safety Act, which included new tools to go after sexual predators on the Internet. Yet, within months, sex offenders found a new virtual playground—social networking websites.

These websites, mostly used by college and high school students to communicate with friends, are now being used by pedophiles to lure unsuspecting children.

Typically, convicted child sex offenders are prohibited from any contact with children. Social networking sites can unwittingly provide the perfect cloak of anonymity to get around this restriction. Congress must stop child predators from using these sites.

First, we should require sex offenders to report all email addresses.

Second, law enforcement agents need immediate access to Internet subscriber information. Before law enforcement officials can shut down a child pornography site, they must first identify the operator and users of the site.

Unfortunately, many Internet Service Providers (ISPs) keep these records for as little as 24 to 72 hours or less. This short retention period may prevent law enforcement officials from catching these pedophiles. The failure of the ISPs to maintain these essential records can mean the difference between life and death for a child.

Law enforcement officials have discovered websites depicting the live sexual assault of young children as it is happening. Child pornography consists of more than pictures of children in suggestive poses. It is also the real-time rape, abuse and molestation of innocent children.

Some ISPs retain subscriber information for up to 90 days. Some do not retain such information for any significant time period. Record retention will help law enforcement officials rescue children who are being abused in real-time.

In a perfect world, cooperation between law enforcement agencies and the ISPs would not require a mandate from Congress.

I hope that a solution can be reached without Congress intervening. I am, however, committed to resolving this issue through a legislative proposal, if necessary.

Another important tool to combat the child pornography industry is to cut it off at its source—money. In recent years, Internet child pornography has evolved from peer-to-peer sharing among pedophiles to a global commercial enterprise worth billions of dollars annually.

Website operators offer "subscriptions" to known child pornography sites that can be purchased using a major credit card or through an emerging tool known as virtual money.

Virtual money, unlike traditional credit cards, is essentially anonymous. It is now the payment method of choice for Internet child pornography. Subscribers can provide fictitious personal information (or no personal information). No credit card or Social Security number is required making them virtually untraceable.

Virtual money presents yet another loophole of anonymity for sex offenders. It leaves law enforcement little hope of identifying these predators. I am committed to closing this loophole.

I welcome our witnesses and thank you for joining us today. I yield back the balance of my time.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND MEMBER, COMMITTEE ON THE JUDICIARY

Mr. Chairman, I thank you for holding this very important hearing on "Sex Crimes and the Internet." When crimes are needlessly being perpetrated against citizens of this country, we as Members of this body have a duty to use whatever measures necessary to curtail such criminal behavior and ensure that we provide the most effective measures possible to be implemented and enforced to ensure the safety of all members of this society.

I am pleased to welcome our witnesses who have gathered here today to give us guidance and insights in our efforts to create innovative solutions at the federal level that will address the incredible challenges that we face in our attempt to curtail sex crimes against children on the internet: Honorable Earl Pomeroy, Representative from North Dakota; the Honorable Marilyn Musgrave, Representative, 4th District of Colorado; The Honorable Debbie Wasserman Schultz, Representative 20th District of Florida; the Honorable Nick Lampson, Representative, 22nd District of Texas; the Honorable Christopher Carney, Representative, 10th District of Pennsylvania; the Honorable Cathy McMorris Rodgers, Representative, 5th District of Washington.

I also welcome our second panel of witnesses: Mr. Michael Mason; Mr. Flint Waters; Mr. John Ryan; Mr. Grier Weeks; Mr. Laurence Rothenberg; Mr. Michelle Collins; and Mr. Elizabeth Banker. I hope that your testimony here today will prove fruitful in guiding this Committee to craft creative and effective legislation to help eliminate such intolerable acts perpetrated against innocent children.

Mr. Chairman, the purpose of this hearing is to discuss issues and strategies to combat the use of the internet to facilitate the commission of sex crimes against children. It is an opportunity for our witnesses to discuss several pending Congressional legislative proposals, alternative approaches to stemming sex crimes against children over the internet, and give guidance to this Committee as to what may be the most efficient and effective means to eliminate sex crimes against our children via the internet.

Mr. Chairman, there are a number of categories of crimes involving sexual exploitation of children and minors that are committed through the use of the internet. They include: the use of the internet to disseminate images of child pornography and sexual exploitation of children; the use of the internet by adult sexual predators to infiltrate "chat rooms" and other social networking sites in order to identify underage persons for purposes of arranging sexual encounters with minors.

Unfortunately, the internet provides a market for the distribution of child pornography and other images of sexual exploitation of children. According to a 2006 report by The National Center for Missing and Exploited Children (NCMEC), its Cyber Tipline received reports about 62,265 incidents of child pornography, 1087 cases of child prostitution, 564 cases of child sex tourism, 2,145 incidents of child sexual molestation, and 6,334 cases of online enticement for sexual acts. In 2006, child pornography was estimated to be a $20 billion industry.

Even more disturbing is the statistical evidence that demonstrates a correlation between the possession of child pornography and child molestation. According to the Director of the Sex Offender Treatment Program, Butner Federal Correctional Institution, who testified in 2006 as to his findings related to the treatment of 155 child pornography offenders, both groups of Internet child pornography offenders treated in the SOTP included a significant proportion (i.e., 80% to 85%) of offenders who perpetrated contact sexual crimes. The Director found that: at the time of sentencing, 115 (74%) subjects had no documented hands-on victims; forty (26%) had

known histories of abusing a child via a hands-on sexual act; the number of victims known at the time of sentencing by the 155 subjects was 75; following treatment, the inmates disclosed perpetrating contact sexual crimes against another 1,702 victims; and eighty-five percent of the inmates were in fact contact sexual offenders, compared to only 26 percent known at the time of sentencing.

Mr. Chairman, there is also evidence that not only does child pornography inherently involve the commission of sex crimes against children, but predators, on occasion, affirmatively use child pornography as part of their process of "grooming" minors to engage in sexual relations. The Unit Chief for the FBI's Crimes Against Children Unit testified in hearings held before this Committee in 2002, that child pornography is used by molesters to:

1. Demonstrate sex acts to children. Offenders commonly use pornography to teach or five instructions to naive children about how to [engage in various sex acts];
2. Lower the sexual inhibitions of children. Some children naturally fear sexual activities. Some offenders show pictures of other children engaging in sexual activities to overcome these fears, indicating to their intended victims that it is all right [sic] to have sex with an adult because lots of other boys and girls do the same thing.
3. Desensitize children to sex. Offenders commonly show child pornography to their intended victims to expose them to sexual acts before they are naturally curious about such activities.
4. Sexually arouse children. Offenders commonly use pornographic images of other children to arouse victims, particularly those in adolescence.

Another problem has arisen in connection with sexual predators' accessing various commercial "social networking" web sites. These sites, such as "My Space" or "Facebook" establish on-line "communities" based on common interests or affiliations. Individuals can post personal information about themselves and their interests, and form on-line relationships with others arising from such common interests. Unfortunately, these "on-line communities" have provided opportunities for on-line predators to locate and identify targets for sexual exploitation.

For example, a study funded by Congress through a grant to the National Center for Missing and Exploited Children found that of 1,500 youths surveyed about their internet activity: 1 in 7 received sexual solicitations; 1 in 3 had been exposed to unwanted sexual material; 1 in 11 had been harassed; 1 in 3 communicated with someone they did not know in person; and approximately 1 in 9 formed close relationships with someone they met online.

We must eliminate predators who prey on and commit crimes against children as well as the vehicles they use to commit such crimes. We need to continue to seek solutions that will put in place effective guidelines for combating, preventing and eliminating sex crimes on the internet against children in all corners of the United States. I look forward to hearing from our witnesses today in our attempt to gain some guidance on this very serious matter.

Thank you, Mr. Chairman. I yield back the balance of my time.

PREPARED STATEMENT OF THE HONORABLE STEVE COHEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE, AND MEMBER, COMMITTEE ON THE JUDICIARY

The growth of the Internet has created vast opportunities for increased connectivity among ordinary people all around the world. Unfortunately, while most of this rise in connectivity has been for the better, the Internet's growth has also opened the door to the facilitation of sex crimes against children, whether through the online dissemination of child pornography images or the use of online chat rooms and social networking sites by sexual predators to lure minors. I look forward to considering our witnesses' proposed solutions to this problem.

PREPARED STATEMENT OF HEMANSHU NIGAM, CHIEF SECURITY OFFICER, FOX INTERACTIVE MEDIA AND MYSPACE

Statement of Hemanshu Nigam
Chief Security Officer
Fox Interactive Media | MySpace

United States House of Representatives
Committee on the Judiciary

Hearing on Sex Crimes and the Internet

October 17, 2007

Dear Chairman Conyers and Ranking Member Smith:

On behalf of Fox Interactive Media and MySpace, I am writing to express our strong support for H.R. 719, The KIDS Act of 2007. I would also like to thank Congressmen Pomeroy, Weiner, Chabot, the late Representative Paul Gillmor, and the other 70 plus co-sponsors of this legislation for their leadership on this issue.

Currently, convicted sex offenders are required to register their physical address, and those who do not do so can be prosecuted and returned to jail. We now know that is not enough. As people across America increasingly use the Internet, the social activity on online communities has begun to mirror the offline world in a variety of ways. As a result, convicted sex offenders must be required to register their online addresses and other online identifiers in addition to their physical address. The KIDS Act of 2007 would require such registration, and is therefore a critical piece of legislation that will help keep youth across America safe, not only in the physical world, but also in the online world.

MySpace is an online community. On MySpace people can share interests with a network of their friends, and others who have common interests. Over 200 million MySpace profiles have been created, and we are one of the most highly trafficked websites in the US. We are committed to making our corner of the Internet a safer and better lit neighborhood so that all users can feel, and actually be, safer when accessing their MySpace pages. We have implemented a wide range of safety features, particularly to protect our younger users.

The safety team at MySpace works to protect our users and to keep potential predators out of our community. To better identify and remove these unwanted visitors to our site, we partnered with Sentinel Tech Corporation to develop a searchable database called

Sentinel SAFE, which contains information on the estimated 600,000 registered sex offenders currently in the U.S. This database brings together more than 50 state and local sexual offender registries for the first time ever. By cross- checking the information aggregated in the sex offender registries against our user profiles, we can help keep predators off our site.

The KIDS Act of 2007 will build on the MySpace email verification system and Sentinel SAFE to better allow us to quickly identify registered sex offenders and remove them from our site. Those who do not follow the law and fail to register, and then use that online address, will get a ticket straight to jail, just as they do in the physical world when they do not register their physical address.

I want to praise you Mr. Chairman and Ranking Member Smith for holding this hearing – you are important leaders in the fight to make the online world even safer. We must work together to keep virtual communities brightly lit, just as we strive to do with the streets of our towns and cities. With your leadership, we will win our collective fight against predators on the Internet, and make younger users all across the country, safer and more secure online.

○